WILLINGNESS TO SHARE INFORMATION VIA MOBILE APPLICATION: THE RISK-BENEFIT PERSPECTIVE

Jyväskylä University
School of Business and Economics

Master's Thesis

2022

Author: Mari Paalimäki
Subject: Marketing
Supervisor: Heikki Karjaluoto

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

ABSTRACT

Author
Mari Paalimäki

Title
Willingness to share information via mobile application: the risk-benefit perspective.

Subject
Marketing

Type of work
Master's Thesis

Date
12.9.2022

Number of pages
51

Increased time spent online, and the increased use of mobile devices and applications have raised consumer privacy concerns. With advanced technology enables efficient data collection through mobile devices, thus consumers are demanding more control for information sharing. Major technology companies have announced that they will stop third-party data collection and are already offering consumers ways to block data collection. This has significant implications for the effectiveness of digital marketing, as third-party information has been used to optimize digital marketing. Therefore, companies should focus on first-party data collection to ensure that digital marketing can implement effectively in the future.

This study examines mobile app users' decision-making in information sharing from a risk-benefit perspective and test the moderating effect of technology anxiety. In addition, the study examines whether users' willingness to share information affects their acceptance of in-app messages. The study was implemented as an experimental study, where the impact of the app's data processing notifications on the privacy risk and personalization experienced by the user was tested. The respondents were randomly divided into four different groups, which were treated with a low or high level of privacy risk and a low or high level of personalization, depending on the group. After treatment, each respondent answered the same online questionnaire. A total of 400 respondents answered the survey.

The results of the study confirm the importance of trust in the willingness to share information. In addition, the results suggest that personalization strengthens trust, increases the users' willingness to share information, and increases the intention to accept in-app messages. In addition, the research results suggest that privacy risk notifications regarding data processing increased users' privacy concerns, providing a new perspective on the kind of information may reduce users' trust in the app and thus reduces the willingness to share information.

Key words
Willingness to share information, privacy, personalization, trust, mobile app

Place of storage
Jyväskylä University Library

TIIVISTELMÄ

Tekijä
Mari Paalimäki

Työn nimi
Halukkuus jakaa tietoa mobiilisovelluksen kautta: riski – hyöty näkökulma.

Oppiaine	Työn laji
Markkinointi	Pro-gradu tutkielma
Päivämäärä	Sivumäärä
12.9.2022	51

Verkossa vietetyn ajan lisääntyminen ja erityisesti mobiililaitteiden ja sovellusten käytön yleistyminen on lisännyt kuluttajien yksityisyyteen liittyviä huolia. Kuluttajat vaativat yhä enemmän päätäntävaltaa henkilökohtaisten tietojen jakamisen osalta. Suuret teknologiayhtiöt ovat vastanneet kuluttajien tarpeisiin tarjoamalla verkkoalustojensa käyttäjille tapoja estää tiedonkeruu. Lisäksi teknologiayhtiöt ovat ilmoittaneet lopettavansa kolmannen osapuolen tietojen keräämisen, joita käytetään digitaalisen markkinoinnin optimointiin. Tällä muutoksella on merkittäviä vaikutuksia digitaalisen markkinoinnin tehokkuuteen. Näin ollen yritysten tulee keskittyä ensimmäisen osapuolen tietojen keräämiseen, jotta pystyvät tehokkaaseen digitaaliseen markkinointiin myös tulevaisuudessa.

Tämä tutkimus tutkii mobiilisovelluksen käyttäjien päätöksentekoa tiedon jakamisessa riski – hyöty näkökulmasta ja testaa teknologia-ahdistuksen moderoivaa vaikutusta. Lisäksi tutkimus tutkii käyttäjän tiedonjaon halukkuuden vaikutusta vastaanottaa sovelluksen sisäisiä viestejä. Tutkimus toteutettiin kokeellisena tutkimuksena verkossa, jossa testattiin sovelluksen tietojenkäsittelyä koskevien ilmoitusten vaikutusta käyttäjän kokemaan yksityisyysriskiin ja personointiin. Vastaajat jaettiin satunnaisesti neljään eri ryhmään ja jokainen ryhmä altistettiin ryhmän mukaan matalan tai korkean tason yksityisyysriskille sekä matalan tai korkean tason personoinnille. Altistuksen jälkeen jokainen vastaaja vastasi samoihin kyselylomakkeen kysymyksiin verkossa. Tutkimukseen vastasi yhteensä 400 vastaajaa.

Tutkimuksen tulokset vahvistavat luottamuksen merkityksen mobiilisovelluksen käyttäjien halukkuudessa jakaa tietoa. Lisäksi tulokset viittaavat siihen, että personointi vahvistaa käyttäjien luottamusta, lisää halukkuutta jakaa tietoa, sekä vaikuttaa positiivisesti aikomukseen vastaanottaa sovelluksen sisäisiä viestejä. Tietojenkäsittelyn yksityisyysriskejä koskevat ilmoitukset kuitenkin lisäsivät käyttäjien yksityisyyshuolia. Tämä tulos tuo uudenlaista näkökulmaa siihen, millaisen tiedon esittäminen käyttäjille voi heikentää käyttäjien luottamusta sovellusta kohtaan ja siten vähentää halukkuutta jakaa tietoa sovelluksen kautta.

Asiasanat
Halukkuus jakaa tietoa, yksityisyys, personointi, luottamus, mobiilisovellus

Säilytyspaikka
Jyväskylän yliopiston kirjasto

CONTENTS

LIST OF TABLES AND FIGURES

1 INTRODUCTION

There are nearly 8 billion people in the world, of whom around 67 percent use a mobile device, and the number of users has increased by 95 million between 2021 and 2022 (Kemp, 2022). In addition, the mobile phone is the only digital device which use is currently growing (Kemp, 2022) The average time spend on mobile app is a 4 to 5 hours a day, when internet consumption on all devices is about 7 hours a day and the phenomenon is reflected globally (Sydow, 2021). The Covid-19 pandemic increased internet consumption globally and companies had to find ways to offer products and services online to consumers to cover lost revenues. Thus, pandemic has forced both consumers and companies to embrace the use of digital services and channels for day-to-day operations, and this change will be permanent. By 2030, 90 percent of the world's population will use the Internet and as 5G technology becomes more widespread, faster data transfer will enable more agile use of mobile devices and applications (Kemp, 2022; Kotler et al., 2021).

The consumer market consists of a five different generation with a different kind of needs and purchasing behaviors: baby boomers, generation X, Millennials, generation Z and generation Alpha (Kotler et al., 2021). The younger generations are more willing to shop on mobile devices and share information about themselves, but expect personalization when sharing information with brand. (Kotler et al., 2021; Pentina, Zhang, Bata & Chen, 2016). Thus, the younger generations are growing purchasing power for mobile devices, if brands manage to engage them with personalized content and experiences. However, younger generation download the most ad-blockers for mobile devices, as there are too many poorly targeted ads, and due concerns about online privacy (Baum, 2019). Hence, mobile apps will become an important marketing and communication channel in the near future, but this requires effective and relevant personalization by brands for their target audiences.

There is paradox in privacy and personalization. Companies need customer data to understand customers' preferences and thus be able to provide personalization. (Mandal, 2019; Smith & Zook, 2020). However, At the same time, customers are increasingly concerned about how the data collected from them is used and who has access to it (Mandal, 2019; Morey, Forbath & Schoop, 2015). Majority of consumers have become aware of their privacy rights and want to take control of their own personal information. (Deloitte, 2018). In addition, consumers are more willing to share information with companies they trust and that offer value for the exchange of information (Goldberg, Mangold, Marsh & Sides, 2019). According to Arbanas, Arkenberg, Downs, Jarvis, and Westcott (2021), 62 percent of generation Z and 72 percent of Millennials wants to receive personalization, but less than half of the respondents are willing to share more information to the brands to get more personalized and targeted advertising. However, consumers value different types of data in different ways (Aguirre, Roggeveen, Grewal & Wetzels, 2015) Consumers value most information that allows firms to profile consumers and is resold to third parties, thus by sharing such information, consumers demand benefits in return (Fehrenbach & Herrando, 2021; Morey et al., 2015).

Since 2018 the General Data Privacy Regulations (GDPR) has been the law in the European Union that protects individuals' rights over how the companies collects,

uses, and stores personal information for marketing and customer resource management purposes (Smith et al., 2020). GDPR requires companies to ask for consumers' permission to collect the data, collected data must be justified, and consumers have right to change their minds and delete they data if they want to (European Union, 2016). Increased privacy demand of consumers has led big technology companies to create own solutions to meet consumers' data protection needs. For example, Apple (Newman, 2021), Google (Temkin, 2021) and Mozilla (Wood, 2019) have announced that they will end of the third-party cookie tracking on they own platforms. The change will have a significant impact on digital marketing optimization and performance for both businesses and consumers. According to Struik (2021), companies with first-party customer data and trust, will succeed in digital marketing in the future. Hence, collecting first-party data will be a top priority for companies to manage customer relationships in the future.

1.1 The aim of the study

The study aims to understand more of information sharing decision via mobile application. This study explore how perceived privacy risk and perceived personalization affects user's willingness to share personal information. In addition, the aim is to find out whether the user's willingness to share information affects the intention of mobile app users to accept in-app messages from the app provider. The study is based on earlier research article on; customer perceived value, satisfaction, and loyalty and the role of willingness to share information (Leppäniemi, Karjaluoto & Saarijärvi, 2017). This paper studied the effects of perceived value and satisfaction on customers' willingness to share information with a retailer in offline context. Previous studies have indicated that perceived value has a positive effect on willingness to share information (Jacobson, Gruzd & Hernandez-Garcia, 2019; Leppäniemi et al., 2017; Xu, Teo, Tan & Agarwal, 2009). This study examines the mobile app user's willingness to share information through the app using a risk-benefit assessment, where the benefits of perceived personalization may create value for the user and thus increase the willingness to share information.

The topic of the study is highly relevant for many reasons. First, according to Marketing Science Institute (2020), increased online time has raised consumers privacy concerns and emphasizes that trust and value-exchange are currently key factors to study ensuring customer satisfaction throughout the customer journey. Second, as mentioned above, the time spent on mobile devices will increase significantly in the future with 5G technology, thus it's relevant to address the mobile context in this study. According to the Moorman (2021), 25 percent of B2B and B2C companies use mobile applications to online sale and most companies believe that mobile application is a key piece of customer acquisition as well as customer retention in the future.

Third, due to increasing data privacy regulations and consumer privacy demands, the lack of third-party data is a relatively new issue for digital marketing. The lack of third-party data creates both opportunities and challenges for companies to collect data to optimize marketing actions and to communicate with customers. Mobile marketing can add positive brand messaging through location-based personalization, creating value for both parties (Dwivedi et al., 2021). Hence, A mobile app can be a

channel through which a company can develop customer relationships, communicate with customers through in-app messages and increase the willingness to share information. Companies need to focus on providing value to consumers thus they are willing to share data for personalization. In addition, companies need to get their customers to accept in-app messages to communicate effectively with customers, According to Goldfarb and Tucker (2013), high ethical practices for data privacy can create a competitive advantage for companies. Thus, privacy management with transparency of personal data processing practises can build trust and increase customers' willingness to share information via mobile app. The research questions of this study are:

1. How the mobile app user makes the decision to share information with the mobile app provider?

2. Is the mobile app user's willingness to share information connected to the intention to accept in-app messages from the app provider?

1.2 Structure of the study

The study begins with introduction, where the reader is introduced to the topic of the study and where the topicality and importance of the research is justified. This will be followed by literature review. The literature review chapter discuss the key concepts used in the research and the relationships between the concepts, reflecting previous academic studies. After the literature review, the data collection methods and the research results are presented. At the end of the study, the theoretical and practical conclusions of the research results are discussed, as well as the limitations of the study and future research agendas are presented.

2 LITERATURE REVIEW

First, it's necessary clarify the difference between the terms *data* and *information* and the use of the terms in this study. According to Turilli and Floridi (2009), *data* is generated by the interaction between the software and the mobile device, where the software, such as an application, collects data from the mobile device. Hence, data consist of insignificant numbers, values, and characters, thus its use is irrelevant. However, when the data is processed with the data analysis tools, the collected data becomes essential structured *information,* where values and context can be combined into useful information (Turilli et al., 2009). Thus, the information cannot exist without the data because it's produced through the processing of data. According to European Union GDPR law (Art. 4(2), 2016), the concept of *data processing* consists of all activities related to personal data including data collection, data mining, data use, storage, sharing and deletion. In addition, European Union GDPR law (Art. 4(1), 2016) defines the concept of *personal data* to include all data relating to person such as name, ID numbers in online and offline environment, location data and all factors that enable the person to be identified. In this study the terms *personal data* and *personal information* are used as synonyms based on the GDPR law definitions and refers to the user's name, ID number, location and all the information that can be used to identify an individual using collected data via mobile devices.

When an individual shares personal information online, it may put the individual in a situation where personal information can be misused or resold by a third party. (Malhotra, Kim & Agarwal, 2004). Currently data breaches are unfortunately common and increased online presence makes consumers more vulnerable and cautious about sharing information. Hence, this negatively effects on companies marketing communications strategies, thus customers are not willing to share information that companies need for offering personalization online (Hofacker, Malthouse & Sultan, 2016). In addition, personal information has a monetary value to businesses (Miller, Lim & Scott, 2020). Consumers are aware of that fact and thus want something valuable in return for the exchange of information to compensate for the privacy risk.

2.1 The role of in-app marketing in information collection

Mobile devices play a major role in marketing communication at all stages of the customer journey (Marketo, 2022; Rowles, 2017). Mobile app marketing is one of the digital marketing strategies that can be used to target marketing messages to users and thus provide personalization through the app (AMA, 2019; Marketo, 2022). In addition, the mobile app marketing tools enables effective ways to communicate with the app users, and thus increase customer database (Smith et al., 2020; AMA, 2019; Marketo, 2022). Mobile devices are everywhere with consumers, making mobile a highly effective marketing channel to reach target customers in real time, in the right location (Bauer & Strauss, 2016; Rowles, 2017). According to Chiang and Chen (2017), location-based mobile marketing will be one of the most important digital marketing tools in the near future. However, the use of location-based in-app marketing is still limited

because in-app marketing creates tensions between the user and the app provider due to privacy concerns (Gu, Xu, Xu, Zhang & Ling, 2017).

Mobile applications can have access to user's personal information and location via mobile phones' ID number (Meng, Ding, Chung, Han & Lee, 2016; Nath, 2015). In addition, location-based mobile marketing targets users based on personalization criteria such as personal information, online activity behaviour, and location information (Meng et al., 2016; Nath, 2015). As previously mentioned, big technology companies have made changes based on consumer requirements to improve data control and allow the users to choose whether to allow the app to track the mobile activity and/or location. Hence, the success of location-based mobile app marketing is strongly linked to users' assessment of the balance between perceived benefits and perceived privacy risk (Shankar, 2016; Wang & Lin, 2017).

Cheung and To (2017) explored the effect of trust on the mobile app user's attitudes towards in-app advertising, and found that trust plays a significant role in user's attitudes towards in-app advertising. In addition, Rialti, Filieri, Zollo, Bazi, and Ciappei (2022) studied how user's attitudes affect the user's purchase intentions in mobile application, and found that attitudes impact on user's purchase intention. Moreover, Rialti et al. (2022) found that the effectiveness of advertising has a positive impact on the user's in-app purchase intention. However, more understanding of user behavior at different stages of customer journey of app use and adoption is needed (Dinsmore, Swani, Goodrich & Konus, 2021; Stocchi, Pourazad, Michaelidou, Tanusondjaja, & Harrigan, 2021).

Stocchi et al. (2021) provide the customer journey framework for studying the mobile app adoption and use through three stages. First, through *pre-adoption stage*, which is related to attitudes, individual and technical characteristics that impact on user's decision-making (Stocchi et al., 2021). Second, through *intention to use stage* which is related to user's experiences and factors that predict decision to use app, and the last, through *post- adoption stage* that include factors of ongoing use of app and app engagement (Stocchi et al., 2021). This study focuses on understand more of users' decisions to use mobile app and sharing information through risk-benefit assessment. In addition, this study focuses on post-adoption stage decision-making to accept in-app messages which is related to continue app use.

In general, mobile apps aims to provide benefits to users thus that they will find the app useful and download it. However, the efficient collection of information through a mobile app raises privacy concerns among users. Wottrich, van Reijmersdal, and Smit (2018) studied the decision-making process when downloading a mobile app, and found that the value provided by the app plays a key role for user when making decisions about sharing information through the app. In addition, Keith, Thompson, Hale, Lowry, and Greer (2013) studied the decision making of privacy risks and information sharing from the perspective of risk-benefit assessment. They found that the greater benefits provided by the app led users to share more private information (Keith et al., 2013). Moreover, Acquisti et al. (2015) mention that users value benefits that can be perceived immediately more than benefits that can be perceived later. Thus, users perceive the benefits of the app provide as more important than the benefits of privacy, as privacy benefit only become apparent once it has already been lost. Hence, the benefits of real-time location-based in-app messages are beneficial and valuable for users. In addition, in-app messages offer companies an important opportunity to provide added value to users.

In this study, in-app messages are related to advertising messages and notification that the app sends to the user via the mobile app. Personalized real-time in-app messages are the most effective way to generate value for the app user and increase the app engagement (American Marketing Association, 2021; Kupietzky, 2021; Wohllebe, Hübner, Radtke & Podruzsik, 2021). Wohllebe et al. (2021) studied the effect of the in-app notifications frequency in retail mobile app, and found that irrelevant and depersonalized messages reduce user's willingness to receive messages, and the willingness to open them. In addition, American Marketing Association (2021) mention that at best, the in-app messages have seven-time higher click-through rate compared to email messages. Hence, it's important to understand the factors that impact on the app user's willingness to share information to the personalization actions and intention to accept in-app messages.

2.2 Food delivery applications

Food delivery mobile applications are related to location-based service applications that offer the benefits of ordering food from local restaurants or grocery stores delivered to a user-defined location (Chakraborty, Kayal, Mehta, Nunkoo & Rana, 2022; Ray & Bala, 2021). Food delivery apps include independent restaurant apps and apps that connect different restaurants and grocery stores on a single platform (Chakraborty et al., 2022). In terms of food delivery apps, previous academic research has focused on factors that influence use intentions (Ray et al, 2021; Ray, Dhir, Bala & Kaur, 2019) and continuance of use (Lee, Sung & Jeon, 2019).

Ray et al. (2020) studied the factors that influence the intention to use food delivery apps, and found trust and perceived monetary benefits to be significant factors in the users' intention to use the app. In addition, Ray et al. (2020) mention that food delivery apps should focus more of providing benefits and privacy for users to increase trust and usage intention. Moreover, Ray et al. (2019) found that ease of use is one of the important factors influencing users' intentions to use food delivery apps. In addition, Su, Nguyen, Nguyen, Luu & Nguyen-Phuoc (2022) found that the link between ease of use and trust also affects customer loyalty in food delivery applications. In addition, Lee et al. (2019) studied the factors influencing the continuance of use of food delivery apps and found the usefulness of the app to be a significant driver of continuance of use. Moreover, Lee et al. (2019) mention that the usability of the information provided by the application in particular creates benefits for users and encourages them to continue using the application. Hence, the use of food apps depends a lot on the user's trust in the app provider and the app's ability to deliver benefits to the user. As with all mobile apps, the use of food delivery apps raises privacy concerns that can negatively affect trust.

The use of location-based food delivery apps requires users to share personal information. However, little academic research has been done on users' decisions to share information in food delivery apps. This study uses a fictitious food delivery app to study the decision-making of app users to share personal information through risk-benefit perspective. Food delivery apps are inherently suited to be studied from a risk-benefit perspective, as food delivery apps offer significant benefits, but at the same time they require the disclosure of private information in exchange for benefits.

2.3 Privacy concerns in information sharing

Several studies have found that privacy concerns have a negative impact on online consumers' intention to share personal information (Culnan, 2000; Jai & King, 2015; Karwatzki, Dytynko, Trenz & Veit, 2017; Li, Sarathy & Xu, 2011; Zhao, Lu & Gupta, 2012). The term *privacy* is defined as the right of individuals to control the collection and use of their personal information (Chellappa & Sin, 2005; Smith, Milberg & Burke, 1996). Thus, privacy is related to an individual's power to control personal information at all stages of data processing practises. Privacy risks are related to privacy concerns, but privacy concerns can be more multidimensional than privacy risks (Dinev et al., 2006; Xu et al., 2009). Privacy risks represent the user's unique concerns about losing privacy in exchange of personal information to benefits (Dinev et al., 2006; Keith, et al., 2013; Xu et al., 2009). However, privacy concerns are strongly linked to privacy risks (Zhou, 2012), thus this study refers to both of the concepts when discussed about privacy risks. Malhotra, Kim & Agarwal (2004) present Internet user's information privacy concerns, IUIPC - model which can be used to understand online privacy factors through three different dimensions: information collection, control of the collected information, and awareness of information protection practices (illustrated in Figure 1).

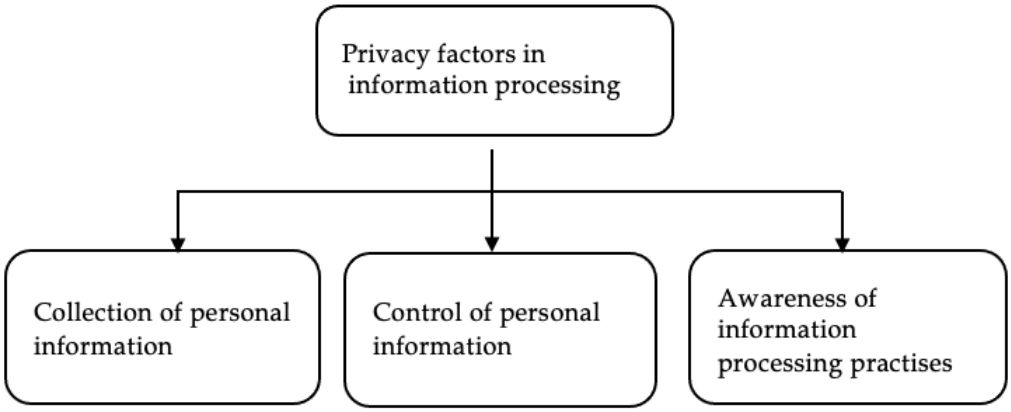

FIGURE 1 Privacy factors in information processing (Malhotra et al., 2004)

The information collection - dimension is related to value-exchange of sharing information (Malhotra et al., 2004). Thus, from the perspective of mobile app user, sharing information includes concerns about the receiving real value from exchange of shared information. Dimension of control of the collected information is related to the risk-benefit evaluation of shared information (Malhotra et al., 2004). The mobile app user evaluates the benefits and privacy risks of the sharing information, and if the benefits are valuable to user, the privacy concerns may have less impact on decision to share information. Hence, the user has the power to control the risks and benefits associated with sharing information. Moreover, the awareness of information protection practices - dimension is related to consumers' understanding of information privacy practises (Malhotra et al., 2004). In other words, the understanding of information collection, what information is collected and why, who is collecting, and how collected information is used, stored, and deleted.

Privacy factors in information processing can be used to observe the factors that may influence a mobile app user's decision making about sharing information. Hence, the privacy factors should be considered when the aim is to create an online environment where the user has the opportunity to influence the sharing of their own information. However, transparent, and comprehensible information about individual's possibilities to influence their own privacy protection can increase the individual's need for privacy (Acquisti, Brandimarte & Loewenstein, 2015; Tsai, Egelman, Cranol & Acquisti 2011). Thus, the lack of information about data processing may increase privacy concerns, but at the same time transparency of data processing may also increase the demand for privacy.

According to GDPR (Art. 13, (1,2), 2016), companies that operate in European Union must provide an online privacy policy statement that include company's data processing practices. Unfortunately, privacy protection policy statements are often difficult to understand (Acquisti et al., 2015). Xu, Dinev, Smith, and Hart, (2011) discovered the relationship between privacy concerns and privacy policy statement. They found that the perceived effectiveness of privacy policy statements is associated with perceived privacy risks (Xu et al., 2011). In addition, Balapour, Nikkhah, and Sabherwal (2020) found that comprehensible privacy policy statement and the perceptions of perceived security of mobile application users have a positive connection. Moreover, Tsai et al. (2011) mention that privacy information has an impact on users' decision-making online. Hence, privacy policy statements and notifications may have an impact on the user's perceived privacy risks and thus decision-making process of sharing information. However, privacy policy statements that are obscure do not serve the user's needs in the decision - making but rather create an information asymmetry between the service provider and the user (Acquisti et al., 2015; McDonald & Cranor, 2008). Moreover, users may not even understand the privacy risks associated with using online platforms, and privacy policy statements that are difficult to understand doesn't have a wanted impact on awareness of privacy risk (McDonald et al., 2008).

Information is collected using a variety of advanced technologies and consumers may not even understand when they should make privacy decisions. *Transparency* refers to access to information that can be used by the user as part of the decision-making process, with the aim of reducing information asymmetry and thus increasing trust between parties (Cambridge Dictionary, 2022; Turilli et al., 2009). The information about privacy choices should be presented more transparent and comprehensible to increase users' awareness of the implications of their own privacy protection choices and privacy risks. According to Acquisti and Grossklags (2005), consumer attitudes, beliefs of ability to protect own information, and knowledge of the privacy risks impact on privacy decisions. Moreover, control of personal information and existing trust are key factors in reducing privacy concerns (Acquisti et al., 2015; Xu et al., 2009). Thus, transparent and comprehensible information about the data processing and implications of privacy decisions-making may enable the feeling of control over the shared information, and thus increase trust. However, Karwatzki et al. (2017) mention that provide transparent information may not directly affect the user's willingness to share personal information, but privacy risks such as privacy loss may play a greater role in information sharing.

Previous studies have found that perceived privacy risks have a negative effect on trust and the app user's willingness to share information via mobile app (Martin & Murphy, 2017; Okazaki, Eisend, Plangger, de Ruyter & Grewald, 2020; Wang, Duong,

& Chen, 2016; Wang et al., 2017). Existing trust decrease privacy concerns, thus higher trust is associated with lower privacy risk and increase willingness to share information (Dinev et al., 2006; McKnight & Chervany, 2002). Aiken and Bous (2006) emphasize that possibility of personal privacy plays a key role in user's trust and willingness to share information. In addition, providing comprehensible information to the user has been shown to increase the trust between the service provider and the user (Fang, Chiu & Wang, 2011; Wang et al., 2017). Moreover, Dinev et al. (2013) mention that the lack of information control is negatively related to perceived privacy, which in turn increase perceived privacy risks. Thus, uncertainty about data processing may cause privacy risks, such as misuse of shared information or privacy loss, and thus negatively affect trust in the app provider. Based on the above literature, the following hypotheses are proposed:

H1. Perceived privacy risk is negatively related to trust.

H2. Perceived privacy risk is negatively related to willingness to share information.

Privacy concerns negatively affect the intention to use mobile app (Stocchi, Michaelidou & Micevski, 2019) and accepting location-based mobile marketing messages (Gutierrez, O'Leary, Rana, Dwivedi & Calle, 2019; Heo & Chang, 2018). The mobile device is connected with the individual through device ID and thus the mobile app provider can track individual's online activity and collect information about the user (Meng et al., 2016). However, the user has the control to decide whether to share information with app provider, and whether to receive in-app messages or not. Hence, it can be hypothesized that if the user perceives privacy risks when using the mobile app, such as misuse or loss of personal data to a third party, the user does not give permission to the app provider to track online activity and to send in-app messages based on it. Thus, the following hypothesis is proposed:

H3. Perceived privacy risk is negatively related to intention to accept in-app messages.

2.4 Information sharing for personalization

Personalization is defined as a way of managing customer relationships by using collected information to serve an individual or a group according to preferences and thus generating value (Fan & Pool, 2006). Mobile devices provide opportunity to collect information about consumer and thus build more deeply understanding of consumer's behaviour and even predict individual behavior patterns (Smith et al., 2020). According to Chellappa et al. (2015), possibility to personalization depend on the company's ability to collect customer information and customer's willingness to share personal information with the company. Moreover, customer satisfaction, loyalty and customer retention are strongly related to the ability to produce personalization (Ball, Coelho & Vilares, 2006; Chellappa et al., 2015; Fang, 2019).
Personalization is one of the most important aspects of a company's customer relationship management, as it allows customer profiling, facilitates targeting, and creates product and service differentiation (Chellappa et al., 2015). In addition, data-driven

personalization delivers more relevant marketing communications to customers, which simplifies decision-making and encourages participation in personalization (Chellappa et al., 2015; Kotler et al., 2021). Moreover, Karwatzki et al. (2017) mentions that the benefits observed through personalization may increase the consumer's willingness to share information. Hence, personalization can create benefits for both the business and the consumer. However, sharing information is highly dependent on consumer's willingness to share information.

Prior studies have indicated that perceived personalization is positively related to consumer's willingness to share information (Karwatzki et al., 2017; Wang et al., 2016; Zhao et al., 2012). Consumers demand high personalized experiences, but are aware of the risks involved in sharing personal information online (Arbanas et al., 2021), and evaluate risks and benefits of sharing decision. *Privacy calculus theory* can be used to explain the behaviour of individual in a situation where the cost of sharing information is compered to perceived benefits (Culnan et al., 1999; Dinev et al., 2006; Keith et al., 2013; Xu et al., 2009). Privacy calculus theory can be presented as a decision-making process (see Figure 2) in which the user evaluates the risk-benefit balance and makes decision about sharing information based on that assessment (Barth et al., 2017; Xu et al., 2009). In general, risks can be i.e., time-related, financial, or psychological, but in this study the focus is on privacy risks, which are strongly related to personalization through intention to share personal information (Acquisti et al., 2015; Lee, Tsao & Chang, 2015). Based on privacy calculus theory, consumers share information in return for economic or social benefit if the benefit outweighs the risks (Culnan & Bies, 2003; Culnan et al., 1999; Pentina et al., 2016). Thus, when users perceive personalization as beneficial, the risk of privacy loss may be acceptable if economic or social value is sufficiently valuable for individual.

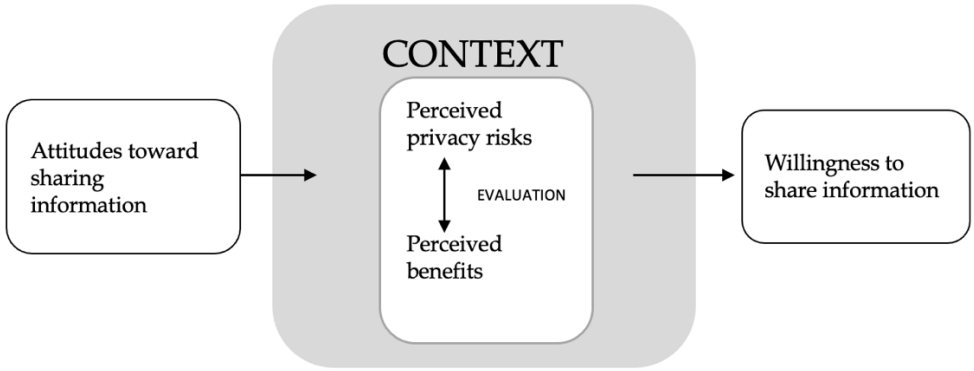

FIGURE 2 Risk-benefits evaluation model (Barth et al., 2017)

The context where the privacy risk - benefit assessment is performed has a significant impact in terms of the decision to share information (Keith et al., 2013). In the context of mobile app, personalization is based on user's preferences, online activity, and location information (Ozturk, Nusair, Okumus & Singh, 2017; Xu et al., 2009). In addition, information-based personalization through a mobile app can create value for the user by relevant marketing messages (Xu et al., 2009). Xu et al. (2009) identified three different value types that generates benefits for mobile user's: time-dependent value, position-dependent value, and user-dependent value. They divided these value types in two categories that generate benefits; to personalization, which enables create value

via tailored experiences and offers, and to location-based benefits that enables to create value in real-time based on user's location (Xu et al., 2009). Thus, mobile devices are an effective way to generate value for users in real-time regardless of user's location and thus encourage users to share information for personalization.

For this very reason, the use of mobile devices and especially sharing information via mobile is strongly associated with privacy concerns and negative attitude on sharing information (Lee et al., 2015). Keith et al. (2013) mention that context-specific privacy risks may have a greater impact on the willingness to share information than perceived benefits. However, it's been noted that there may occur inconsistency between user attitude towards privacy and actual behaviour (Acquisti et al., 2015). Wang et al. (2016) studied information disclose with privacy-calculus theory. Based on risk – benefit evaluation they found that mobile app users value more benefits than risks when sharing personal information with the app provider (Wang et al., 2016). The app user may strongly value privacy but still share information to benefit from it, for example getting personal discounts or valuable information. Phenomenon is called *personalization - privacy paradox* (Awad & Krishnan, 2006; Karwatzki et al., 2017; Pentina et al., 2016; Chellappa et al. 2005), which combines these two concepts when studying information sharing via mobile devices.

According to Acquisti et al. (2015), adopted culture, social expectations, motivation, and past experiences guide individuals in evaluating privacy risks in different context and situations. In addition, individual's privacy preferences can vary by context, situation, attitudes as well as the type of data (Acquisti et al., 2015; Treiblmaier, 2007). Hence, it is difficult to define individuals' attitudes towards privacy in information sharing, but by understanding the decision-making process, it is possible to find factors that may influence individual's attitudes and decision to share information. Xu (2006) studied the effect of personalization on consumer attitudes towards mobile advertising and found a strong connection between personalization and attitudes, which affects consumer's behavior. Hence, the perceived personalization may be the key factor when it comes to shaping consumer attitudes toward information sharing and accepting in-app messages.

However, when consumer value privacy, it negatively affects willingness to be part of personalization (Awad et al., 2006; Karwatzki et al., 2017, Xu et al., 2011), which makes it difficult for companies to provide benefits to consumer. Giving a control over the sharing of personal information may reduce consumer's perceived privacy risks and thus lowers the threshold for being part of the personalization. However, it should be noted that increasing general understanding of privacy issues may also increase concerns and increase in the number of people who value privacy more (Acquisti et al., 2015).

The effect of benefits on consumer trust has been studied and a positive connection has been found between them (Kim, Ferrin & Rao, 2008; Komiak & Benbasat, 2006; Ozturk et al., 2017; Su et al., 2022). Kim et al. (2008) tested a trust-based decision-making model and found that perceived risks, perceived benefits, and trust can affect making decisions. In addition, Kim et al. (2008) noticed that the role of trust extends from reducing privacy concerns to the intention to decide. Moreover, Ozturk et al. (2017) studied the loyalty of mobile hotel booking users with relationships between personalization, trust, and risk. They found that although sharing information for personalization causes negative attitudes and privacy risks among users, personalized benefits reduce risks and enhance trust in the service provider (Ozturk et al., 2017). In addition,

Su et al. (2022) studied factors which influence on user's trust in mobile food delivery app. They found a relationship between personalization and trust, but also between trust and user's loyalty, which suggests that trust affects the user's behavioural intention (Su et al., 2022). Hence, it can be assumed that perceived personalization has a positive effect on trust and thus on the user's willingness to share information with the app provider and receive in-app messages. Based on the above literature, the following hypotheses are proposed:

H4. Perceived personalization is positively related to trust.

H5. Perceived personalization is positively related to willingness to share information.

H6. Perceived personalization is positively related to intention to accept in-app messages.

2.5 The role of trust in information sharing

The concept of trust has been studied in the internal context of organizations (Mayer et al., 1995; McAllister, 1995; Schoorman, Mayer & Davis, 2007). Mayer et al. (1995) developed *interactive model of organizational trust*, which can be used to understand the formation of trust between two parties. Mayer et al. (1995) defines the concept of *trust* as placing yourself in a vulnerable position and taking the risk of the other party's actions. In addition, trust has been studied in the context of e-commerce (e.g., Awad & Ragowsky, 2008; Kim, Ferrin & Rao, 2008; Sullivan & Kim, 2018). Sullivan et al. (2018) defines *trust* in e-commerce as the consumer's expectations and assessments of the trustworthiness of the provider and the reliability of the functionality and security of the website.

Trust between consumer and service provider in e-commerce has been studied mostly with *technology acceptance model*, where trust is built through generated value by perceived usefulness and ease-of-use (e.g., Awad et al., 2008; Ajzen, 1991; Gefen et al., 2003). In addition, trust has been studied with *theory of reasoned action* where trust is observed with the relationship between attitudes, intentions, and behaviour (e.g., Kim, Ferrin & Rao, 2009; McKnight et al., 2002; Zhang, Cheung & Lee, 2014). Moreover, Kim et al. (2009) used *extend value framework* to study risk-benefit evaluation in consumer decision-making process and found a strong relationship between the risk-benefit evaluation and trust in the purchase decision-making.

Previous studies that discuss trust in mobile context are also mainly based on *technology acceptance model* factors i.e., perceived usefulness and easy-of-use (e.g., Stocchi, Michaelidou & Micevski, 2019; Su et al., 2022) or the *privacy-calculus theory* (Kang et al., 2019; Ozturk et al., 2017; Wang et al., 2016). User's attitudes and trust have been shown to have a significant relationship (Wang, Genc & Peng, 2020). In addition, trust has been shown to have a positive effect on the user's intention to download and use mobile services (Chin, Harris & Brookshire, 2018; Gupta, Chopra, Tanwar & Manjhi, 2021; Luceri, Bijmolt, Bellini & Aiolfi, 2022; Wang, Shen & Su, 2013; Kang & Namkung, 2019). Moreover, a positive relationship has been found between trust and intention to use location-based mobile applications (Heo et al., 2018; Wang et al., 2017). Thus, user's

attitudes, trust and intention to use mobile services are connected. Furthermore, the quality of the information and the functionality of the service have a significant connection to the user's trust (Su et al., 2022; Wang et al., 2017). Hence, trust plays a significant role in information sharing in the mobile app context, as it affects the intentions to adopt and use app, which in turn makes information sharing possible.

Prior studies have found a positive link between trust and willingness to share information in online (Komiak et al., 2006; Malhotra et al., 2004; Schoenbachler & Gordon, 2002). Komiak et al. (2006) developed *trust-based adoption model*, which provides a framework to understand how trust may increase consumers' intention to share information. The trust-based adoption model consists of three dimensions: cognitive trust, emotional trust, and intention to use. Cognitive trust is based on beliefs of trust and is formed when user has identified the rational reason to trust (Komiak et al., 2006). In addition, Komiak et al. (2006) emphasize that cognitive trust has an impact on emotional trust, which is based on attitudes of trust and evaluation of feeling of trust, and hence form intention to use online services.

In this study, the trust between the mobile app user and the app provider is examined the combination of interactive model of organization trust (Mayer et al., 1995), and trust-based adoption model (Komiak et al., 2006). The models in question support each other and the interactive organizational trust model complements the trust-based model with the risk perspective in trust formation, which occur in sharing information as privacy risks in mobile context. Next, the formation of trust between the mobile app user and the app provider is discussed with the dimensions of these two models.

Trust is a key factor in information sharing between *the trustor*, i.e., the app user who is willing to share information, and *the trustee*, i.e., the app provider, who is collecting the information and providing personalized benefits based on collected data (Malhotra et al., 2004). *Trust* can be defined as decision to trust the other party is based on the app user's expectations and assessments of the app provider, which always involves risk-taking related to the actions of the app provider (Mayer et al., 1995; Sullivan et al., 2018). Hence, the app user is willing to take the risk to trust the app provider although the user can't fully ensure that the app provider is acting in an acceptable manner. Evaluation process of trustworthiness present trust formation between the trustor and the trustee through perceived trustworthiness factors (see Figure 3).

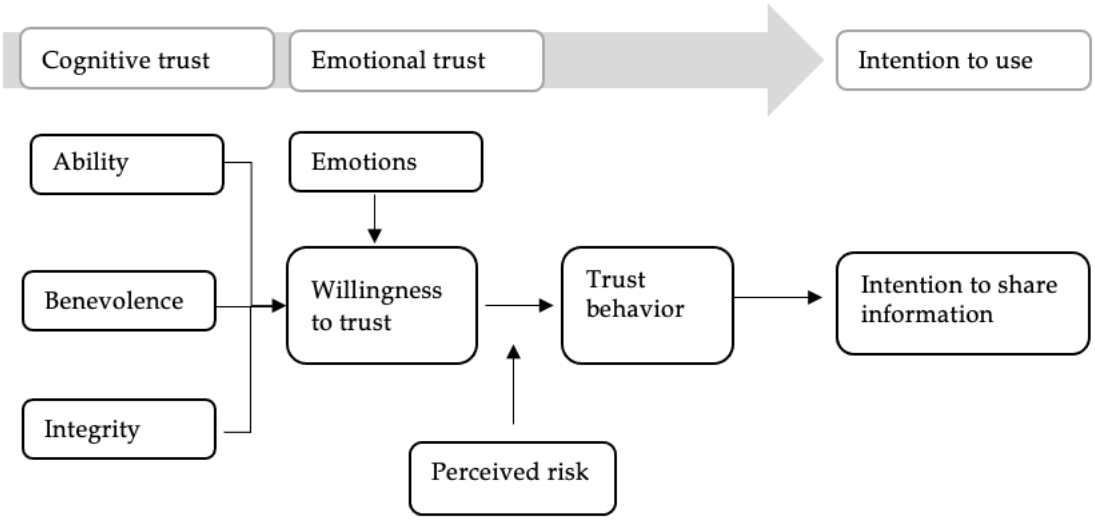

FIGURE 3 Evaluation process of trustworthiness with perceived trust factors (Mayer et al., 1995)

The *trustworthiness* of trustee can be defined as a motivation to lie, thus if the trustor beliefs that the trustee has some reason to lie, trustworthiness decreases (Mayer et al., 1995; Schoorman et al., 2007). Cognitive factors that are related to trust beliefs and affect trustee's trustworthiness are as the user's perceptions of ability to influence, the beliefs of the app provider's benevolence to do good without self-interest and the perceptions of the app provider's integrity. (Mayer et al., 1995; Schoorman et al., 2007). These cognitive factors are determined by the user's principles and which the app provider must follow to be able to build a trust-based relationship with user (Komiak et al., 2006; Mayer et al., 1995; Schoorman et al., 2007). Therefore, if the app provider is only committed to making monetary profit in collecting the personal information and does not care the privacy concerns of the app user, the principles accepted by the parties will differ and the app provider's trustworthiness decreases.

In addition, trust is related to emotional factors that influence on trust behavior jointly with cognitive elements (Andersen & Kumar, 2006; Komiak et al., 2006; Mayer et al., 1995; Schoorman et al., 2007). However, vulnerability is related with emotional trustworthiness as attitudes and emotions may change in time as the user evaluate the app provider's trustworthiness (Akrout, Diallo, Akrout & Chandon, 2016; Schoorman et al., 2007). Therefore, negative emotions, especially in the early stages of building trust-based relationship, affect the level of trust negatively (Andersen et al., 2006). Hence, when negative emotions arise, it is important to find the reason and address it with the parties, thus the level of trust can be managed, and the relationship may even be further strengthened (Andersen et al., 2006; Schoorman et al., 2007).

The trustor (i.e., the app user) evaluates the trustworthiness of the trustee (i.e., the app provider) and assessing the level of risk in trust relationship and then decide whether to take a risk and share personal information with the trustee (Mayer et al., 1995; Schoorman et al., 2007). Hence, in building trust-based relationships, first comes the willingness to trust and after the actual behavioural trust that involves the risk-taking in trust such as privacy loss, and after that intention to share information. The risk level evaluation is related to the user's personal factors, past experiences, and the situational factors, and if the level of trust is higher than the perceived level of risk, the trustor will trust relationship with the app provider, and vice versa (Mayer et al., 1995). Thus, trust is influenced by cognitive and emotional factors. In addition, when evaluating the risks and benefits of a trust relationship, emotional factors play a significant role in increasing the level of trust and strengthening the relationship.

Trust reflects the level of risk that a user is willing to take when sharing information (Malhotra et al., 2004). Thus, by reducing privacy risks with transparent data practices, the app provider can build trust and improve customer relationships in the long run (Bleier & Eisenbeiss, 2015; Milne & Boza, 1999; Schoorman et al., 2007). In general, the imbalance of power between the parties affects the imbalance in perception of risk, thus the party with less power of control perceive more risks, which affects trust (Mayer et al., 1995; Schoorman et al., 2007). Information asymmetry in data processing practices between the mobile app user and the app provider can increase the user's risk, which can reduce trust between parties.

However, the app provider must be able to demonstrate the capability to act as expected by the app user in all dimensions (ability, benevolence, integrity, and emotions), thus the app user can make the decision to trust on both cognitive and emotional level (Komiak et al., 2006; Mayer et al., 1995). Hence, e.g., transparency of data practices is not enough to convince user to trust app provider, but e.g., the app provider

must show the ability to show benevolence and integrity in actions if the user expects that. Hence, trust has a key role in information sharing, because without the app user's trust towards the app provider, the user will most likely not even download the app, in which case the app usage and information sharing will not take place. Based on the above literature the following hypotheses are proposed:

H7. Trust is positively related to willingness to share information.

H8. Willingness to share information is positively related to intention to accept in-app messages.

2.6 The moderating effect of technology anxiety

Technology anxiety is related to individual's concerns and experiences, when using of technology-related devices, such as a mobile phone (Meuter, Ostrom, Bitner & Roundtree, 2003). In addition, Meuter et al. (2003) emphasize that technology anxiety is specifically related to individual's ability and willingness to use technology. Thus. it is appropriate to explore the moderating effect of technology anxiety on the impact of privacy risks and personalization in sharing information through a mobile app and accepting in-app messages. Especially in the mobile context, a significant amount of technology anxiety can occur. Technology is evolving rapidly, and this can cause users to feel anxious about using new technology and distrust technology-related devices, or even discourage users from adopting new technology (Gelbrich & Sattler, 2014; Yang & Forney, 2013). In addition, some previous studies have discussed the concept of computer anxiety (e.g., Lee, Choi & Kang, 2009; Sievert, Albritton, Roper & Clayton, 1988), but the concept of technology anxiety better describes today's various technological devices and services.

Previous studies have explored the relationship between technology anxiety to individual attitudes and behavioural intentions (Curran & Meuter, 2007; Gelbrich et al., 2014; Meuter et al., 2003; Venkatesh, 2000). Meuter et al. (2003) explored the use of self-service technologies and found that technology anxiety reduces the intention to use technology-related services. In addition, Meuter et al. (2003) noticed that self-service technologies provide to user benefits with timesaving, effective, high-quality, easy-to-use functions that are always available to users. However, Gelbrich et al. (2014) found that technology anxiety has a greater effect on attitudes than the ease of use of technologies. Curran et al. (2007) studied the factors that influence the user's decision to adopt new technologies and found that attitudes in general towards technology and specific brands affect the technology adoption and use. In addition, Curran, Meuter, and Surprenant (2003) discovered that users who often use technologies, have more positive attitudes towards technology providers, while for users who use technology less frequently, attitudes are influenced by the general attitude towards technology.

Moreover, Kang et al. (2019) tested the moderating effect of technology anxiety on users' behavior toward personalized services in a mobile application context. They found that users with high level of technology anxiety are mostly unaware of benefits that technology-related services can offer (Kang et al., 2019). Thus, users who experience way less technology anxiety benefit from personalization significantly more.

Hence, technology anxiety includes the user's concern about their own abilities to use technology and it has a negative effect on the willingness to adopt new technologies and ability to be part of personalization. Technology anxiety can moderate perceived privacy risks, moderate perceived benefits, and thus affect user's trust towards the application provider and technology in general. Therefore, technology anxiety can affect a user's intention to adopt and use a mobile app and receive personal benefits. Based on the above literature the following hypotheses are proposed and presented in the research model (see Figure 4) with other hypotheses of this research:

H9a. Technology anxiety moderates the negative relationship between perceived privacy risk and trust. Specifically, technology anxiety enhances the negative link between perceived privacy risk and trust.

H9b. Technology anxiety moderates the negative relationship between perceived privacy risk and willingness to share information. Specifically, technology anxiety enhances the negative link between perceived privacy risk and willingness to share information.

H9c. Technology anxiety moderates the negative relationship between perceived privacy risk and intention to accept in-app messages. Specifically, technology anxiety enhances the negative link between perceived privacy risk and intention to accept in-app messages.

H9d. Technology anxiety moderates the positive relationship between perceived personalization and trust. Specifically, technology anxiety weakens the positive link between perceived personalization and trust.

H9e. Technology anxiety moderates the positive relationship between perceived personalization and willingness to share information. Specifically, technology anxiety weakens the positive link between perceived personalization and willingness to share information.

H9f. Technology anxiety moderates the positive relationship between perceived personalization and intention to accept in-app messages. Specifically, technology anxiety weakens the positive link between perceived personalization and intention to accept in-app messages.

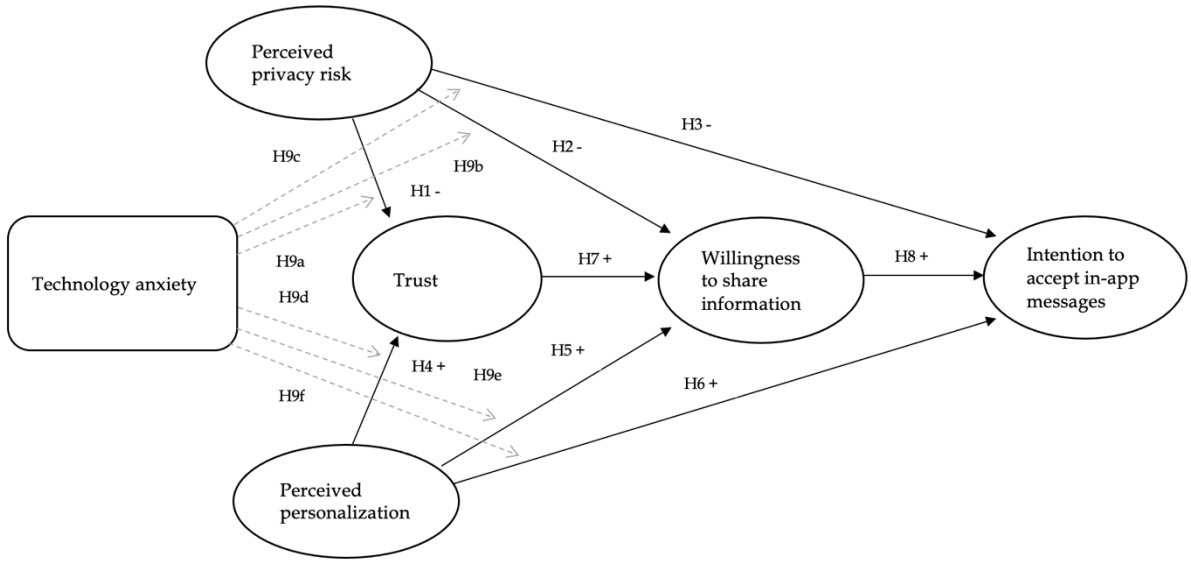

FIGURE 4 Research model.

3 DATA AND METHODOLOGY

3.1 Research design

Similar to other studies on mobile application privacy issues (e.g., Betzing, Tietz, vom Brocke & Becker, 2019; Harbach, Hettig, Weber & Smith, 2014; Hsieh & Li, 2022), this study was conducted in online – based experimental study where participants were treated with different mobile screen scenarios before answering the online survey questions. The experiment was implicated with a fictitious food and grocery delivery mobile application scenarios, which were used to test the user's intentions to share information with that application. The study is designed so that the independent variables group the setup into four different groups that manipulate the signal strength of the independent variables with different treatments, and we are interested on the averages of these different groups (Metsämuuronen, 2005). Independent variables, perceived personalization and perceived privacy risk, forms four different test groups based on the strength of manipulation signal (see Figure 5). The group 1 measured the impact of low perceived personalization and high privacy risk on the dependent variables, the group 2 measured the impact of high perceived personalization and high perceived privacy risk on the dependent variables, the group 3 measured impact on low perceived personalization and low perceived privacy risk on the dependent variables, and the group 4 measured impact on high perceived personalization and low perceived privacy risk to dependent variables.

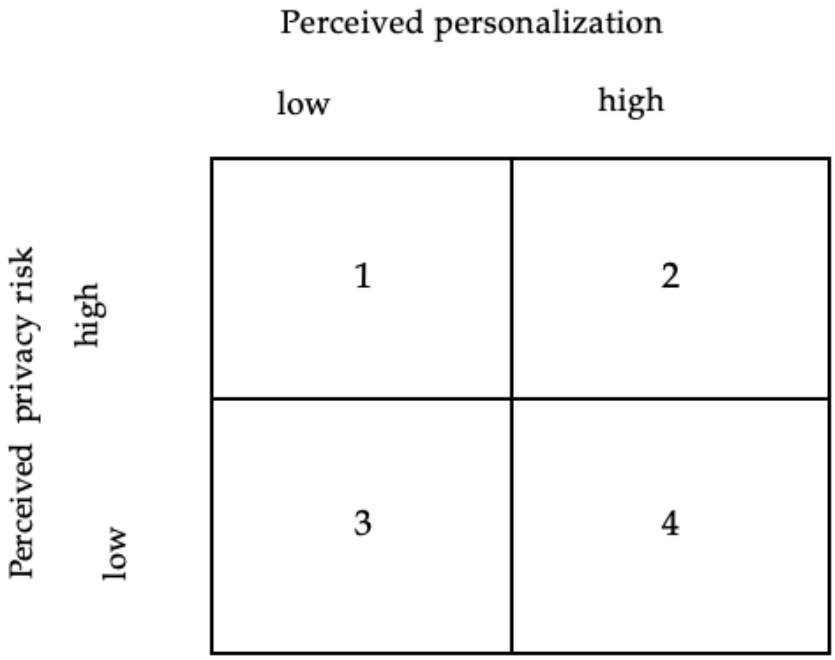

FIGURE 5 Treatment test groups.

Study participants were presented with preliminary information about the app and after that, participants were randomly divided into four different groups and different

groups were exposed to different treatments according to the group. Before taking the survey, participants saw the following preliminary information about the mobile app:

> "You are downloading a free mobile app that provides affordable shipping services for your restaurant orders and your grocery store orders made through the app in your local area. You can use the app anywhere by sharing your location with the app provider to discover your local restaurants and grocery stores. You can also receive personalized offers as notifications directly to your mobile phone if you accept that the app is collecting data from your order transactions and if you allow the app to send notifications based on your online activity. The app provider is a global provider of digital platform economy. "

Test group 1 measured low perceived personalization and high perceived privacy risk; thus, test group 1 served as the control group of the experiment and was not exposed to any treatment and participants just responded the survey after reading the preliminary information about the mobile application. Test group 2 measured of high perceived personalization and high perceived privacy risk and was exposed to the treatment of high perceived personalization (see Table 1) after which participants responded to the questionnaire. Test group 3 measured low perceived personalization and low perceived privacy risk and was exposed to the treatment of low perceived privacy risk (see Table 1) after which participants responded to the survey. Test group 4 measured high perceived personalization and low perceived privacy risk and was exposed to the treatment of high perceived personalization as well as treatment of low perceived privacy risk, after which participants responded to the survey.

TABLE 1 Content of independent variables exposed to treatment.

Independent variables	Low	High
Perceived personalization	* No treatment.	Content of mobile screen 1: "Why we want to track your online activity? We want to collect data from your online activity to provide you with a more valuable and personalized app experiences based on your preferences." Content of mobile screen 2: "We like to know your preferences so that we can offer more beneficial offers, products, and services to you. You can customize your app experience and add, change, or delete your preferences in the app settings." Content of mobile screen 3: "Why we ask you to share your location with us? We would like to send you real-time ads and notifications based on your location so you can benefit of our offers anywhere."

(continues)

TABLE 1 (continues)

Perceived privacy risk	Content of mobile screen 1: "We respect our customers privacy and the data we collect is accessible only those involved in our company. No third-party operators are involved in the processing of the customer data we collect." Content of mobile screen 2: "We provide more options to choose what information you want to share with us, and you can change your choices anytime in the app settings." Content of mobile screen 3: "We want to give you the control of your own data. You can see the profile we build on your online activity, and you change your preferences or delete information whenever you like."	*No treatment.

The treatments for the experiment were designed to demonstrate to the participants the use of the information collected via mobile application in a transparent manner. The content of the treatments was designed using data transparency factors (Malhotra et al., 2004), and the aim of the treatments was to show the app users why the app provider wants to collect information about the users, how the app provider uses the collected information and how the mobile app users can control the information they share via the app. As previously mentioned, test group 2 was exposed to the treatment of high perceived personalization, thus group 2 respondents were shown mobile screens (see Figure 6) before the questionnaire that provide transparent information about why the app wants to track users' online activity and location information and how the users can benefit from it. Test group 3 was exposed to the treatment of low perceived privacy risk, thus group 3 respondents were shown mobile screens (see Figure 7) before the questionnaire that provide transparent information about who is allowed to process the collected data, about the options of app users to choose what information they want to share with the app provider and about the possibility to see the profile that the app provider built from user's online activity based on collected data and the user's ability to change or delete personal preference information. Test group 4 was exposed to both high perceived personalization treatment and low perceived privacy risk treatment before the questionnaire.

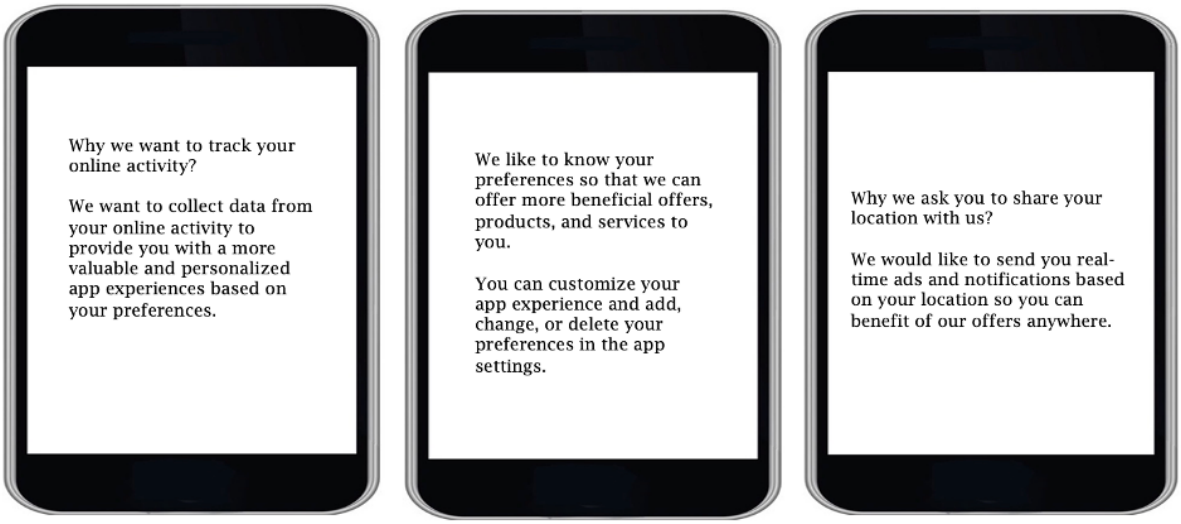

FIGURE 6 Treatment of high perceived personalization.

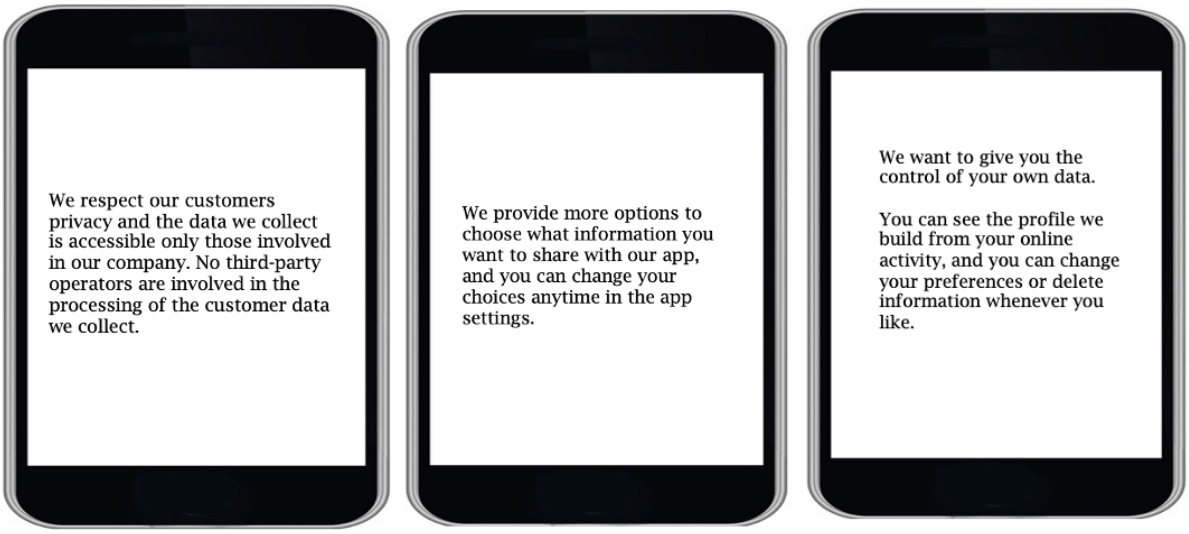

FIGURE 7 Treatment of low perceived privacy risk.

3.2 Data collection method

The research design and structured questionnaire were pre-tested before the data collection in May 2022, and the purpose was to test the functionality of the experimental study as well as the signal strength of the treatments. In the pre-test, manipulation check variables were added to the questionnaire to assess the performance of the experiment. Test group 2 was asked to evaluate with 7-point Likert scale, to what extent mobile screen notifications (see Figure 6) reflect a high level of personalization when using the mobile app. Test group 3 was asked to evaluate with 7-point Likert scale, to what extend mobile screen notifications (see Figure 7) reflect a high level of data privacy when using the app (note the reverse layout). To find out if there were any dif-

ferences between the groups, the means of the two independent variables were compared using the Mann-Whitney U-test, because the variables were not normally distributed, which can be explained by the small sample size, n = 49. Independent variable perceived privacy risk U-test statistic was 18.500 and sig. <0.001, thus groups are different from each other. Independent variable perceived personalization U-test statistic was 175.500 and sig. was 0.011, thus groups are different from each other, but not as significantly as in the case of perceived privacy risk. Based on Mann-Whitney U-test result to the content of high perceived personalization treatment was made a few word changes to make the differences between high and low treatments more pronounced. In addition, one pair of online survey items was replaced because no covariation was found between the items.

The sample was collected in June 2022 with a questionnaire that was built in Qualtrics software and conducted via online survey. Among the sample, there was one respondent who did not accept the privacy notice at the beginning of the survey, thus one respondent was removed from the total respondents. Hence, a final total 400 individuals responded to the survey A total of 100 individuals responded to group 1, which is 24.9 percent of all respondents, and the total of 99 individuals responded to group 2, which is 24.7 percent of all respondents. In addition, a total of 101 individuals responded to group 3, which is 25.2 percent of all respondents, and to the group 4 total of 100 individuals responded, which is 25.2 percent of all respondents. Thus, each group was answered by approximately the same number of respondents.

3.3 Research variables

All measures used in this study were adapted from existing scales and all the construct items are measured using 7-points Likert (see Appendix 1). Both perceived personalization and perceived privacy risk constructs were measured with three items adapted from Wang et al. (2016), and trust construct was measured with four items adapted from Sutanto et al. (2013). Willingness to share information was measured with two items adapted from Leppäniemi et al. (2017), and intention to accept in-app messages construct was measured with two items from Heo et al. (2018), which were modified to reflect the purpose of this study. The moderating variable – Technology anxiety construct was measured with three items adapted from Meuter et al. (2003).

4 RESULTS

The results of the study are presented in this chapter. Descriptive statistics to describe respondents' profile and experimental research manipulation check were performed by using SPSS 28.0. In addition, a two-step approach examination of conceptual framework was conducted by using Smart PLS (v. 3.3.9). First, confirmatory factor analysis (CFA) was run to confirm convergent and discriminant validity of the scales, after which the hypotheses were tested and analyzed by running the structural model. CFA is one of factor analysis methods of structural equation modeling, which can be used to define the variation between latent variables, the number of factors, which explains the correlation between observed variables, i.e., the variation between the variables, as well as the relationships between them (Birks & Wills, 2013; Brown, 2013; Malhotra). According to Brown (2013), the structural equation model consists of two models, the first one is measurement model which defines the relationship between factors and indicators, and validity and reliability of model, and the second one is structural model which can be used to test hypotheses and determine factor relationships. The results of the models are discussed below.

4.1 Profile of respondents

Table 2 present the respondents demographic and of the 400 respondents in the sample 50.7 percent were male (n = 203) and 49.3 percent were female (n = 197). In terms of age distribution, 10.8 percent (n = 43) of the respondents were 18-25 years old, 41.3 percent (n = 165) were 26-34 years old, 29.5 percent (n = 118) were 35 - 44 years old, 14 percent (n = 56) were 45 - 54 years old, and 4.5 percent (n = 18) were 55 years old or more. The income level of the respondents is distributed like 4.3 percent of total respondents (n = 17) earn less than US$ 10,000 a year, 29.8 percent of total respondents (n = 119) earn US$ 10,000 – 39,999 a year, and 57.8 percent of total respondents (n = 231) have annual earnings between US$ 40,000 – 79,000. Further, 8.3 percent of total respondents (n = 33) earn more than US$ 80,000 a year.

TABLE 2 Demographic profile of respondents.

Demographics and characteristics	n	(%)	Group 1 (n)	Group 2 (n)	Group 3 (n)	Group 4 (n)
Total	400	100	100	99	101	100
Gender						
Male	203	50.7	49	54	50	50
Female	197	49.3	51	45	51	50
Age						
18-25	43	10.8	12	8	13	10
26-34	165	41.3	41	41	36	47
35-44	118	29.5	27	35	33	23
45-54	56	14.0	16	13	16	11
55 or more	18	4.5	4	2	3	9

(continues)

TABLE 2 (continues)

Income (annual)						
<US$ 10,000	17	4.3	6	5	4	2
US$ 10,000 – 24,999	47	11.8	9	15	12	11
US$ 25,000 – 39,999	72	18.0	20	15	21	16
US$ 40,000 – 59,999	133	33.3	29	35	36	33
US$ 60,000 -79,999	98	24.5	28	27	20	23
>US$ 80,000	33	8.3	8	2	8	15
Educational level						
Less than High School	1	0.3	-	-	1	-
High School	45	11.3	12	10	13	10
Bachelor's Degree	220	55.0	60	55	53	52
Master's Degree	134	33.5	28	34	34	38
Mobile application usage (Hours per day)						
< 1 hour	11	2.8	4	3	2	2
1-2 hours	95	23.8	23	26	27	19
3-4 hours	163	40.8	47	34	37	45
5-6 hours	86	21.5	18	26	22	20
> 6 hours	45	11.3	8	10	13	14

The level of education is distributed among the respondents like 55 percent have a bachelor's degree (n = 220) and 33.5 percent of respondents have a master's degree (n = 134). The rest of the respondents have a high school (11.25 percent, n = 45) or lower education level (0.25 percent, n = 1). For frequency of mobile application usage distribution, only 2.8 percent of respondents (n = 11) use mobile applications less than 1 hour per day, 23.8 percent of total respondents (n = 95) use mobile apps 1 - 2 hours per day and 40.8 percent (n = 163) use mobile apps 3 - 4 hours per day. Moreover, 21.5 percent (n = 86) use mobile apps 5 - 6 hours per day and 11.3 percent of total respondents (n = 45) use mobile apps more than 6 hour per day. Hence, the profiles of the respondents seem to be distributed in such a way that they can represent a larger population when analyzing the results.

4.2 Manipulation check with the independent samples t-test

The success of the manipulation is examined by comparing the mean values between the groups, and thus finding out how the manipulation of the independent variables affected the mean values of the test groups. In the experiment there was two independent variables, perceived personalization and perceived privacy risk that were manipulated with high and low level of manipulation. The analysis of the differences between the manipulation level (low, high) of two independent groups was carried out with an independent samples t-test using SPSS software. First, it was determined how the level of perceived personalization manipulation affected the mean values by comparing the answers of the respondents who participated in the low perceived personalization manipulation group (n= 201, group 1 and group 3) and the high perceived

personalization manipulation group (n = 199, group 2 and group 4). For the manipulation of the variable perceived personalization the aim was to get a higher mean value for the high manipulation group than lower manipulation group. As presented in the Table 3, the mean values differ between the groups of low (2.00) and high (3.01) level of manipulation, T-value is -9.975 and p-value is <0.001, thus the manipulation level groups differ statistically significantly from each other.

TABLE 3 Independent samples t-test results.

Independent variable	T-value	df	*p*-value	Level of manipulation	n	Mean	SDV
Perceived personalization	-9.975	398	<0.001***	Low	201	2.00	1.002
				High	199	3.01	1.003
Perceived privacy risk	39.900	398	0.000***	Low	201	3.50	0.501
				High	199	1.50	0.501

Second, the aim was determining how the level of perceived privacy risk manipulation affected the mean values by comparing the answers of the respondents who participated in the low perceived privacy risk manipulation group (n = 201, group 3 and group 4) and the high perceived privacy risk manipulation group (n = 199, group 1 and group 2). The mean values differ between the groups of low (3.5) and high (1.5) manipulation, T-value is 39.900 and p-value is 0.001, thus the manipulation level groups differ statistically significantly from each other. Therefore, it can be concluded that the manipulation was successful for both independent variables. However, it should be noted that for the variable perceived privacy risk, the aim was to get a higher mean value for the group of high level of manipulation, but the result was the opposite.

4.3 Measurement model

The measurement model is the first step in two-stage structural equation modeling (SEM) to estimate constructs (or factors) validity and reliability of the constructs (see Table 4). Confirmatory factor analysis CFA was used to estimate the loadings of factors that were selected based on theory and to see if they were loaded as expected. (Malhotra et al., 2013). Thus, the CFA was used to confirm or refute the theory-based concept of which factors explain the variability of variables and to measure internal validity and reliability of the model. According to Garson (2016), the values of the factor loadings vary between -1 and 1, and the closer the factor loading is to value 1 the stronger the factor can explain the variation of the observed variable. In addition, factors with loadings of 0.7 or higher are reliable to explain the variation between the factor and variables (Hulland, 1999). As presented in the Table 4, standardized factor loadings ranged from 0.743 to 0.916, all factor loadings were significant and exceeded

0.7. All factor loadings are presented also in the Figure 8, with constructs. The reliability of constructs can be measured with Cronbach's alpha value and composite reliability value, which should be ≥0.7 (Hair, Wolfinbarger, Money, Samouel & Page, 2015). As presented in the Table 4, Cronbach's alpha values are ≥ 0.7, thus it indicates that the measurement method is reliable. According to Hair, Sarsted, Ringle, and Mena (2011b), Cronbach's alpha measures all indicators at once, thus it is not the most reliable measure in structural equation modeling to measure reliability. Composite reliability measures items according to their individual reliability (Hair et al., 2011b), and the value vary between 0 to 1 (Garson, 2016), and values should be ≥0.7 (Malhotra et al., 2013). As presented in the Table 4, composite reliabilities of constructs vary between 0.866 – 0.920, which exceeded the criteria of ≥0.7.

TABLE 4 Reliability and validity analysis.

Construct (Cronbach's alpha)	Standardized factor loadings	Composite reliabilities	AVE
Perceived personalization (0.767)		0.866	0.684
PP_item1	0.848		
PP_item2	0.743		
PP_item3	0.884		
Perceived privacy risk (0.863)		0.915	0.783
PPR_item1	0.893		
PPR_item2	0.853		
PPR_item3	0.908		
Trust (0.867)		0.909	0.714
TR_item1	0.845		
TR_item2	0.862		
TR_item3	0.852		
TR_item4	0.820		
Willingness to share information (0.785)		0.903	0.823
WSI_item1	0.916		
WSI_item2	0.898		
Intention to accept in-app messages (0.783)		0.902	0.821
INT_item1	0.914		
INT_item2	0.899		
Technology anxiety (0.871)		0.920	0.793
TA_item1	0.895		
TA_item2	0.863		
TA_item3	0.913		

Notes: PP: Perceived personalization, PPR: Perceived privacy risk, TR: Trust, WSI: Willingness to share information, INT: Intention to accept in-app messages, TA: Technology anxiety.

However, composite reliability values that are >0.9 may indicate that the items are too similar to each other or represent the desired dimension and just correlate well with each other. (Garson, 2016). Hence, the convergent validity of the model should be specified, which can be used to define that the indicators of the constructs are strongly

connected to each other and therefore reflect the same construct (Brow, 2013). The average variance extracted (AVE) measures the amount of variance that is captured by the construct in relation to the amount of variance due to measurement error and the value should be higher than 0.5 (Fornell & Larcker, 1981). As presented in the Table 4, AVE of constructs range from 0.689 to 0.823 which exceeded the criteria of >0.5, thus for each construct, the construct and its indicators are strongly connected.

Discriminant validity can be used to define that the different variables do not correlate with each other, i.e., variables are divergent from each other (Brown, 2013: Hair et al., 2015), and discriminant validity is achieved if the square root of the average variance extracted (√AVE) is higher than all other constructs correlations (Malhotra et al., 2013). Fornell – Larcker discriminant validity criterion is presented in the Table 5, and as it can be seen the √AVE are higher than other constructs correlations; PP √AVE =0.827, PPR √AVE =0.885, TR √AVE =0.845, WSI √AVE=0.907, INT √AVE =0.906, and TA √AVE =0.891. Based on the results of measurement model it can be asserted that validity is achieved.

TABLE 5 Fornell – Larcker Discriminant validity Criterion.

Measure	PP	PPR	TR	WSI	INT	TA
Perceived personalization	0.827					
Perceived privacy risk	0.260	0.885				
Trust	0.511	0.307	0.845			
Willingness to share information	0.459	0.221	0.767	0.907		
Intention to accept in-app messages	0.450	0.273	0.762	0.837	0.906	
Technology anxiety	0.112	0.707	0.446	0.375	0.418	0.891

Notes: PP: Perceived personalization, PPR: Perceived privacy risk, TR: Trust, WSI: Willingness to share information, INT: Intention to accept in-app messages, TA: Technology anxiety.

4.4 Structural model

After it has been established that the measurement model is valid and reliable, the structural model should be evaluated. The structural model is the second step in two-stage structural equation modeling (SEM) to examine the strength of the relationships between the constructs and testing hypothesized relationships (Brown, 2013; Hair et al., 2015; Malhotra et al., 2013). It is relevant to check the multicollinearity of the model, i.e., that the indicators of the model do not correlate with too many other indicators and thus affect hypothesis testing results negatively (Hair, Risher, Sarstedt & Ringle, 2019; Hair, Sarstedt, Hopkins & Kuppelwieser, 2014). Variance Inflation Factor (VIF) values should be under 3 (Hair et al, 2019; Hair et al., 2011b), and as presented in the Table 6, collinearity is in optimal level as the VIF values vary between 1.321 and 2.966, thus the values are less than 3.

Table 6 Collinearity.

Indicator	VIF-value
PPR_item1	2.229
PPR_item2	2.108
PPR_item3	2.312
PP_item1	1.886
PP_item2	1.321
PP_item3	1.936
TR_item1	2.098
TR_item2	2.398
TR_item3	2.153
TR_item4	2.096
WSI_item1	1.718
WSI_item2	1.718
INT_item1	1.705
INT_item2	1705
TA_item1	2.183
TA_item2	2.240
TA_item3	2.966

Path coefficients (β) are measured to estimate the hypothesized paths of the model. Path coefficient value range is -1 to 1 and the value closer to 1 predicts a stronger positive connection between the constructs and the value closer to -1 predicts a stronger negative connection between the constructs, while the value closer to zero predicts a weaker connection between the constructs (Garson, 2016; Hair et al., 2019;). The model's hypothesized path coefficients are presented in the Table 7., and as can be seen, the values vary between -0.198 and 0.744 and the values predict the direction of the final results. However, path coefficient significance must be measured with bootstrapping procedure which provides t-values that can be used to confirm significance of the hypotheses (Hair et al., 2015; Hair, Ringle & Sarstedt, 2011a). According to Garson (2016), t-values must be $\geq$1.96 to reach the 0.05 significance level. As presented in the Table 7, t-values exceed the criteria $\geq$1.96 for H_1, H_4, H_5, H_6, H_7, H_8, H_{9a}, H_{9b} and H_{9c}, thus these hypotheses are empirically supported. In addition, the path analysis coefficients are presented in the Figure 8.

In the evaluation of the structural model R^2-values (coefficient of determination values) explain how well independent variables explain the dependent variables and values vary between 1 and 0 and the aim is to reach the highest possible values (Hair et al., 2014, Hair et al., 2015). According to Hair et al. (2011a), if the R^2 value is $\geq$ 0.75, the effect is strong and if the R^2 value is around 0.5 the effect is moderate, while if the R^2 value is around 0.25, the effect is very weak. As can be seen from the Table 8, Trust (TR) R^2 -value is 0.433 which means that 43.3 percent of the variance in trust variable is explained by the independent variables perceived personalization (PP) and perceived privacy risk (PPR) which is fairly moderate effect. In addition, Willingness to share information (WSI) R^2-value is 0.604, thus the model explains 60.4 percent of the variance of the WSI variable which is moderate effect. Moreover, as presented in the Table 8, intention to accept the in-app messages (INT) R^2-value is 0.720, thus model explain 72 percent of the variance of INT variable which is close to strong effect.

TABLE 7 Structural model results.

Hypothesized path		Path Coefficient β	t-value	p-value	Result
H_1	PPR → TR	-0.198	2.424	0.016*	Supported
H_2	PPR → WSI	-0.126	1.786	0.075	Not supported
H_3	PPR → INT	-0.014	0.267	0.789	Not supported
H_4	PP → TR	0.503	9.237	0.000**	Supported
H_5	PP → WSI	0.132	2.783	0.006**	Supported
H_6	PP → INT	0.097	2.116	0.035*	Supported
H_7	TR → WSI	0.671	10.788	0.000**	Supported
H_8	WSI → INT	0.744	15.496	0.000**	Supported
H_{9a}	TA → PPR →TR	0.248	4.783	0.000**	Supported
H_{9b}	TA → PPR →WSI	0.144	3.022	0.03*	Supported
H_{9c}	TA → PPR → INT	0.130	3.310	0.001**	Supported
H_{9d}	TA → PP → TR	-0.034	0.092	0.927	Not supported
H_{9e}	TA → PP → WSI	0.024	0.150	0.881	Not supported
H_{9f}	TA → PP → INT	0.057	1.359	0.175	Not supported

Notes: *p≤0.05, **p≤0.01

TABLE 8 R^2-values.

Dependent variable	R^2-value	Effect
TR	0.433	fairly moderate
WSI	0.604	moderate
INT	0.720	close to strong

As presented in the Table 7, perceived privacy risk PPR (β = -0.198, p = 0.016) and perceived personalization PP (β = 0.503, p = 0.000) both have significant effect on mobile app user's trust, thus H_1 and H_4 are supported. As mentioned above, the R^2 of the TR variable is 0.433, thus about 43 percent of its variation is explained by the PPR and PP variables. In addition, perceived personalization (β = 0.132, p = 0.006) have a positive effect on app user's willingness to share information via mobile app, thus H_5 is supported. The R^2 of the WSI variable is 0.604 i.e., about 60 percent of its variation is explained by the PPR, PP, and TR variables. Moreover, H_6 is supported, thus perceived personalization (β = 0.097, p = 0.035) have a positive effect on app user's intention to accept in-app messages, and the R^2 of the INT variable is 0.720 i.e., 72 percent of its variation is explained by the PPR, PP, TR, and WSI variables.

However, there is no direct statistical relationship between perceived privacy risk (β = - 0,126, p = 0.075) and willingness to share information (p > 0.05). Similarly, there is no direct statistical relationship between perceived privacy risk (β = - 0.014, p = 0.789) and app user's intention to accept in-app messages (p > 0.05). Thus, H_2 and H_3 are not supported. Trust (β = 0.671, p = 0.000) has a significant positive effect on the app user's willingness to share information, and there is also a very strong positive relationship between the app user's willingness to share information (β = 0.744, p = 0.000) and intention to accept in-app messages. Thus, H_7 and H_8 are supported.

Technology anxiety (β = 0.248, p = 0.000) has a positive moderating effect on the relationship between perceived privacy risk and trust. Thus, H_{9a} is supported. Hence, the technology anxiety strengthens the negative link between perceived privacy risk and trust. The higher the user's technological anxiety level, the stronger the perceived

privacy risk will negatively affect the user's trust. In addition, technology anxiety (β = 0.144, p = 0.03) has a positive moderating effect on the relationship between perceived privacy risk willingness to share information. Hence, the technology anxiety strengthens the link between perceived privacy risk and willingness to share information. Similarly, technology anxiety (β = 0.130, p = 0.001) has a positive moderating effect on the relationship between perceived privacy risk and intention to accept in-app messages. Thus, the technology anxiety strengthens the link between perceived privacy risk and intention to accept in-app messages. Hence, H_{9b} and H_{9c} are supported. However, as confirmed above, there is not a statistical support for relationship between perceived privacy risk and willingness to share information, thus it can only be stated that technology anxiety may affect indirectly between these two variables. Likewise, as there is not a statistical support for relationship between perceived privacy risk and intention to accept in-app messages, it can be stated that technology anxiety may affect indirectly between these two variables.

As presented in the Table 7, there is no support on H_{9d} as technology anxiety (β = -0.034, p = 0.927) has not a negative moderating effect on the relationship between perceived personalization and trust. In addition, technology anxiety (β = 0.024, p = 0.881) has not a negative moderating effect on the relationship between perceived personalization and willingness to share information. Hence, H_{9e} is not supported. Moreover, technology anxiety (β = 0.057, p = 0.175) has not a negative moderating effect on the relationship between perceived personalization and intention to accept in-app messages. The results of the structural model are presented in the Table 7 above.

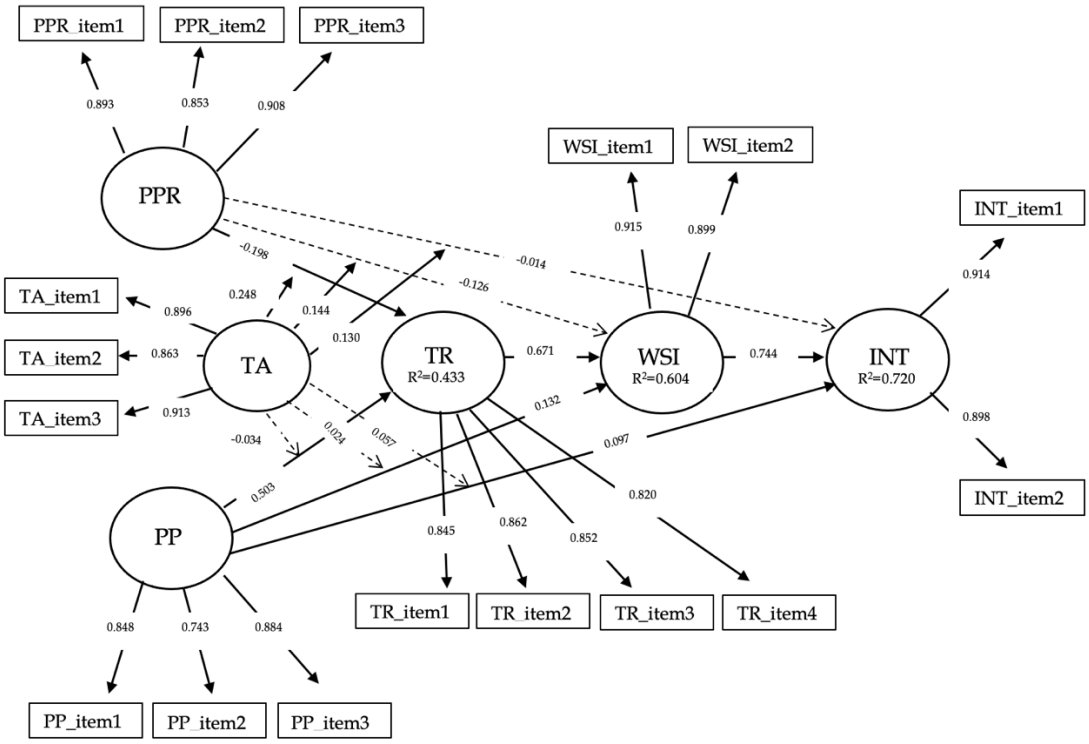

FIGURE 8 Path analysis coefficient.

5 DISCUSSION

In this study the focus was on understanding more of information sharing decision via mobile application and how perceived privacy risk and perceived personalization effects the app user's willingness to share personal information. In addition, the study focus was to determine whether there is a link between user's willingness to share information and intention to accept in-app messages from the app provider. Increased time spent online and especially on mobile devices have raised consumer privacy concerns about data misuse, which in turn has increased mistrust of data collection and consumer's demand of control over the sharing personal information. Therefore, major technology companies have taken steps to provide consumers with options for more privacy online presence. These changes will allow consumers to minimize third-party data collection and prevent tracking of online activity. In the future, the first-party data will play a significant role in companies' ability to provide personalized services for the customers and thus generate value and satisfaction This study provides evidence on how perceived privacy risk and perceived personalization affect a mobile app user's decision to share personal information via a mobile app. Despite the fact that the topic is highly topical, there is a little academic research into it from this point of view. Mobile apps provide an effective direct channel to collect first-party data if the user is willing to share it with the app provider.

5.1 Theoretical implications

This study verifies several pieces of literature on privacy risks and personalization in mobile device and makes contributions to the literature of the decision-making process when it comes to sharing personal information via mobile app. First, the study confirms that trust is significant positive element on user's willingness to share information through the mobile app. This finding is in line with previous studies that have shown a positive connection between trust and willingness to share information (Komiak et al, 2006; Malhotra et al., 2004; Schoenbachler et al., 2002). In addition, prior studies have found that trust plays a key role in intention to download the mobile app (Chin et al., 2018; Gupta et al., 2021; Kang et al., 2019). Thus, the result of this study confirms the notion that the significant role of trust continues even in the phase of adopting and using the mobile app, where the app requests permission to collect information. The result is a notable addition to the mobile app literature, as it increases the understanding of the importance of the trust existence in information sharing via mobile app. The user has the option to choose whether to share information with the app, thus downloading the app does not guarantee the user's willingness to share personal information. Hence, the result indicates that during the mobile app adoption and use phases the user must have trust toward the app provider in order to be ready to share information through the app.

Second, this study found a significant negative connection between the perceived privacy risk and trust. The result support the previous studies that have discovered that privacy risk negatively influences trust in mobile app context (Okazaki et al., 2020; Wang et al., 2016; Wang et al., 2017). Lack of awareness of the use of the collected data

or concern about misuse of the personal information may cause perceived privacy risks to the app user, which negatively affects trust toward the app and decrease the willingness of share information (Dinev et al., 2006; Malhotra et al, 2004). Transparent discussion about data processing in mobile app might be one way to decrease privacy risks and increase trust (Acquisti et al., 2015; Xu et al., 2009). However, the results of this study did not support the expectations that perceived privacy risk and willingness to share information are directly connected. This result is surprising since many prior studies have shown the connection (e.g., Jai et al., 2015; Karwatzki et al., 2017; Li et al., 2011; Zhao et al., 2012). In addition, the results of this study did not support the expectation that perceived privacy risk and intention to accept in-app messages would have a direct connection. Similarly, this finding is unexpected, as prior studies have shown the negative connection between privacy risks and the app use (Heo et al., 2018; Stocchi et al., 2019). These results may even strengthen the important role of trust in information sharing through the mobile app and thus accepting in-app messages from the app provider. This assumption supports the findings of previous studies that trust is a significant determinant of intention to use an application (Heo et al., 2018; Wang et al., 2017).

Third, the results of this study suggest that presenting transparent information about data processing to the mobile app user may increase the perceived privacy risks. This result was surprising addition to the research results and challenges expectations that transparency about data processing after downloading the app would be the effective way to reduce the app user's privacy risks and increase trust. However, the finding is in line with few previous studies that discuss that transparent privacy information can increase the value of privacy (Acquisti et al., 2015; Tsai et al., 2011). The results of this study shows that the groups that were exposed with low perceived privacy risk notifications, perceived significantly more privacy risks than the groups that did not see any notifications related to privacy risks. Thus, it can be assumed that providing information about data processing after downloading an application may raise more privacy concerns for the user than in a situation where no information is provided. In addition, privacy notices that are difficult to understand can increase the privacy risks for the user (Acquisti et al., 2015; McDonald et al., 2008). The finding is a significant observation to previous literature on mobile app privacy issues, as the discussion is currently heavily focused on the fact that users may experience less privacy concerns through transparent information. However, this assumption requires further research.

Fourth, the results confirm that perceived personalization is positively related to trust. The result confirms the findings of previous studies that personalization and trust have a positive connection in mobile app context (Ozturk et al., 2017; Su et al., 2022). Through the perceived personalization, the app user creates a perception of the app provider's ability to offer valuable service. In addition, if the service meets the user's expectations, then the user's trust towards the app provider increases. Moreover, the results confirm that perceived personalization has a positive effect on the willingness to share information. This finding support previous studies that confirm the positive relationship between personalization and willingness to share information (Karwatzki et al., 2017; Wang et al., 2016; Zhao et al., 2012). Users value the perceived benefits of personalization relatively more compared to the risks in mobile apps (Wang et al., 2016). In addition, the perceived benefits of personalization generate value to the user (Chellappa et al., 2015), which reduces perceived risks, and thus increase trust to

the app provider (Ozturk et al., 2017). Hence, the mobile app users are willing to share information with the app provider in exchange for personalized benefits that provide value, which in turn strengthen the trust with app provider.

Moreover, the results confirm that perceived personalization has a positive effect on intentions to accept in-app messages. This finding confirms that personalized, time- and location-relevant in-app messages are more likely to be received as they provide value to the app user (Wohllebe et al., 2021). Hence, properly implemented personalization that generate value for the user may influence the user's intention to share information, and thus intention to accept in-app messages. In addition, this finding strengthens the importance of information sharing and personalization in the effectiveness of in -app messages.

Fifth, the results support that willingness to share information and intention to accept in-app messages have a significant positive relationship. The result supports a few previous studies that have found similar results (Gutierrez et al., 2019; Heo et al., 2018). This finding is a notable addition to the mobile app literature, as there has been relatively little research on the acceptance aspect of in-app messages. The finding suggests that the app user's willingness to share information may predict the intention to receive in-app messages and vice versa. Thus, decision-making related to information sharing also may affect directly on effectiveness of the in-app marketing actions. In addition, it is important to note the role of trust and personalization in the acceptance of in-app messages, as the results suggest that both trust and the real benefits of the messages have a positive effect on user's intention to accept in-app messages.

Sixth, the results of the study confirms that technology anxiety strengthens the negative effect of perceived privacy risk on trust. Thus, the more technology anxiety the app user experiences, the more strongly the perceived privacy risks negatively affect trust. This finding is notable addition to the mobile app literature as it increases the understanding of factors that influence of trust in mobile app context. Technology anxiety is strongly related to the user's own ability and willingness to use technology (Meuter et al., 2003). Previous studies have shown that the technology anxiety affects user attitudes (Gelbrich et al., 2014) and attitudes towards technology in general can affect the use of technology (Curran et al., 2007). Based on the result of this study, the user's negative beliefs toward technology and inability to use technology strengthens the negative impact of the perceived privacy risks on trust.

Seventh, the results confirms that technology anxiety strengthens the negative impact of perceived privacy risk on willingness to share information. Thus, the higher the user’s technology anxiety level, the stronger negative effect of perceived privacy risks on the user’s willingness to share information. This finding is significant addition to the mobile app literature as the result is one of the first to confirm a strengthening effect of technology anxiety between perceived privacy risks and willingness to share information. In addition, the result of this study confirms that technology anxiety strengthens the negative impact of perceived privacy risks to intention to accept in-app messages. Similarity, this finding is a significant addition to the mobile app literature, as it is one of the first to find a strengthening effect of technology anxiety on between perceived privacy risks and the intention to accept in-app messages.

However, this study did not find a direct statistical relationship between the perceived privacy risk and willingness to share information. Hence, in this study the strengthening effect of technology anxiety effect on willingness to share information

effect indirectly via trust. Similarity, this study did not find a direct statistical relationship between the perceived privacy risk and intention to accept in-app messages. Thus, in this study the strengthening effect of technology anxiety effect on intention to accept in-app messages effect indirectly via trust and willingness to share information. These findings strengthen the role of trust in the mobile app user's decision-making process to share information and intention accept in-app messages. However, trust should be reflected as the user's trust in their own abilities to use the mobile app, and as trust towards the app provider. In addition, the mobile app user who experience high level technology anxiety do not even realize the benefits of personalization (Kang et al., 2019), which may also strengthen negative attitudes towards information sharing. Hence, the anxiety of technology weakens the mobile app user's willingness to share information and thus the intention to accept in-app messages.

However, the results do not support expectation of the negative moderating effect of technology anxiety between the perceived personalization and trust. Similarly, the results do not support expectation of the negative moderating effect of technology anxiety between perceived personalization and willingness to share information, nor between perceived personalization and intention to receive in-app messages. These results may indicate that mobile app users who perceive the benefits of personalization do not experience high level technology anxiety. This assumption is in line with previous finding that mobile app users who experience way less technology anxiety, will benefit from personalization significantly more than user's who experience high level of technology anxiety (Kang et al., 2019).

5.2 Practical implications

Based on the theoretical contributions addressed above this study offers practical implications for information collection in a mobile app. As third-party data collection becomes more difficult, companies must focus on first-party data collection in order to offer personalization and thus create value to customers. The mobile app offers an efficient channel to collect first-party customer data. In addition, the app provides effective channel to deliver value by personalized messages to user based on user location in real time. However, it requires the user's permission. The theoretical contributions of the research show that users value the benefits, which can positively affect the users' trust in the app provider and thus the willingness to share information. However, perceived privacy risks may limit users from fully utilizing the benefits offered by the app, which in turn may weaken trust towards the app. In addition, the high level of technology anxiety experienced by the user strengthens the negative effect of perceived privacy risks on trust, which reduces the user's willingness to be part of personalization. Hence, it is important to emphasize the benefits of the app, thus that the user can use this information in making a decision to share personal information with the app provider.

In addition, emphasizing the benefits of the mobile app can positively influence the granting of permission to send in-app messages. With in-app messages, companies can encourage users to continue using the app and create value through optimized personalization, which further strengthens trust. This may create a positive cycle in which both parties would benefit. If the user understands how using the app can create

benefits, the user may be more willing to share information via app. In addition, the app provider receives information about the user and thus is able to offer personalization, which increase trust. Hence, it is important to understand the role of in-app messages in providing benefits to the user, and thus building trust in sharing information. In addition, the importance of in-app messages in developing customer relationships and strengthening customer loyalty should be taken into account.

Presenting transparent information about data processing may increase app user's privacy concerns. Transparent information can cause a negative reaction when adopting the app and prevent the user to share information via the app. In addition, if user experience high technology anxiety and the inability to understand the data processing of the app, it further strengthens the negative reaction. Hence, presenting transparent information about data processing is not necessarily the best way to build trust with the app user. In addition, the privacy notions that are difficult to understand may also increase user's privacy concerns or evoke technology anxiety. The challenge is to find a way to inform users about data processing in an understandable way, thus it does not cause concerns about privacy risks. However, companies must act in information collection in accordance with general good ethical practices and collect only the kind of information that is necessary to provide a high-quality service to users.

In addition, the individual's ability to use the technology has an effect on adopting the app. Technology anxiety strengthens the negative impact of the privacy risks experienced by the individual on trust. Hence, the app provider should guide the user in using the app, thus that the user is able to use the functions of the application according to own preferences. This can increase the user's trust in the app and enhance the willingness to share information. The app users want to benefit from the information they share, and by emphasizing information about the benefits of the app with comprehensible and guiding way, the user's willingness to share information can be increased. As the user learns to use the app according to their preferences, their attitudes towards the application may become more positive. As a result, the user may be more willing to be part of the personalization and to share information and receive in-app messages.

5.3 Limitations and future research

As with the any empirical study, this study has some limitations that should be considered when interpreting the results. First, the research set-up is designed in such a way that it is assumed that the mobile app user experience privacy risks. The privacy risk notifications presented in the experiment were divided into high- and low-level treatments, but the high-level treatment did not include the notification, because it was assumed that privacy risks are experienced in any case, and thus it was expected that the notification of the data processing would reduce the perceived privacy risks through the low-level treatment. However, this research design yielded unexpected results, as the hypothesized low-level treatment actually increased privacy risks, even though the assumption was the opposite. Thus, the result may be due to the research setting in question, where the information presented to the user reminds of privacy issues related to information sharing and may thus increase privacy-related concerns.

In the future studies, this phenomenon could be investigated further in order to increase the understanding of whether information about data processing causes even more concerns for the app user, and how transparency in data processing should be presented to the user in order to reduce privacy concerns.

Second, the results of the study may be affected by the nature of the fictitious mobile app used in this study. The operation of the fictitious mobile app was based on providing affordable transport services for restaurant orders and grocery shopping. Thus, it can be expected that in most cases the app is downloaded in order to receive benefits and offers from local restaurants and grocery stores which requires information sharing and may increase intention to accept in-app messages. In other words, the app used in the experiment emphasizes the perceived benefits that the app offers, this may have an impact on the results. However, applications are mostly downloaded to receive benefits, so by emphasizing the benefits after downloading the application, it is possible to increase the user's trust in the application. Future studies could also explore the willingness to share information in different application contexts, such as surveillance applications, where individuals do not benefit from information sharing, but only a specific party benefit.

REFERENCES

Acquisti, A. & Grossklags, J. 2005. Privacy and rationality in individual decision making. IEEE Security & Privacy 3 (1), 26-33.

Acquisti, A., Brandimarte, L. & Loewenstein, G. 2015. Privacy and human behavior in the age of information. Science. American Association for the Advancement of Science 347 (6221), 509-514.

Aguirre, E., Roggeveen, A. L., Grewal, D. & Wetzels, M. 2015. The personalization-privacy paradox: implications for new media. Journal of Consumer Marketing 33 (2) 98-110.

Ajzen, I. 1991. The theory of planned behavior. Organizational Behavior and Human Decision Processes 50 (2), 179-211.

Akrout, H., Diallo, M. F., Akrout, W. & Chandon, J. 2016. Affective trust in buyer-seller relationships: A two-dimensional scale. The Journal of Business & Industrial Marketing 31 (2), 260-273.

American Marketing Association. 2019. Mobile marketing. American marketing association webpage. Available: <URL: https://www.ama.org/topics/mobile-marketing/>

American Marketing Association. 2021. 5 ways to improve mobile app engagement. Available: <URL: https://www.ama.org/2021/06/09/5-ways-to-improve-mobile-app-engagement/>

Andersen, P. H. & Kumar, R. 2006. Emotions, trust, and relationship development in business relationships: a conceptual model for buyer–seller dyads. Industrial Marketing Management 35 (4), 522-535.

Arbanas, J., Arkenberg, C., Downs, K., Jarvis, D. & Westcott, K. 2021. Digital media trends, 15th edition: courting the consumer in a world of choice. Deloitte. Available: <URL: https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html>

Awad, N. F. & Krishnan, M. S. 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly 30 (1), 13-28.

Awad, N. F. & Ragowsky, A. 2008. Establishing trust in electronic commerce through online word of mouth: an examination across genders. Journal of Management Information Systems 24 (4), 101-121.

Balapour, A., Nikkhah, H. R. & Sabherwal, R. 2020. Mobile application security: role of perceived privacy as the predictor of security perceptions. International Journal of Information Management 52, 102063.

Ball, D., Coelho, P. S. & Vilares, M. J. 2006. Service personalization and loyalty. The Journal of Services Marketing 20 (6), 391-403.

Barth, S. & de Jong, M. D. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review. Telematics and Informatics 34 (7), 1038-1058.

Bauer, C. & Strauss, C. 2016. Location-based advertising on mobile devices: a literature review and analysis. Management Review Quarterly 66 (3), 159-194.

Baum, D. 2019. Ad blocking trends 2020. Impact plus. Available: <URL: https://www.impactplus.com/blog/ad-blocker-trends-for-2019>

Betzing, J. H., Tietz, M., vom Brocke, J. & Becker, J. 2019. The impact of transparency on mobile privacy decision making. Electronic Markets 30 (3), 607-625.
Bleier, A. & Eisenbeiss, M. 2015. The importance of trust for personalized online advertising. Journal of Retailing 91 (3), 390-409.
Bruner, G. C. & Kumar, A. 2007. Attitude toward location-based advertising. Journal on Interactive Advertising 7 (2), 3-15.
Cambridge Dictionary. "Privacy" meaning in business English. https://dictionary.cambridge.org/dictionary/english/privacy Visited 25.1.2022.
Chakraborty, D., Kayal, G., Mehta, P., Nunkoo, R. & Rana, N. P. 2022. Consumers' usage of food delivery app: a theory of consumption values. Journal of Hospitality Marketing & Management 31 (5), 601-619.
Chellappa, R. K. & Sin, R. G. 2005. Personalization versus privacy: an empirical examination of the online consumer's dilemma. Information Technology and Management 6 (2), 181-202.
Chiang, L. P., & Chen, C. H. 2017. Evaluating antecedents and consequences of location-based services. International Journal of Electronic Commerce Studies 8 (1), 47-76.
Chin, A. G., Harris, M. A. & Brookshire, R. 2018. A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. International Journal of Information Management 39, 49-59.
Culnan, M. 2000. Protecting privacy online: is self-regulation working? Journal of Public Policy & Marketing 19 (1), 20–26.
Culnan, M. J. & Armstrong, P. K. 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 10 (1), 104-115.
Culnan, M. J. & Bies, R. J. 2003. Consumer privacy: balancing economic and justice considerations. Journal of Social Issues 59 (2), 323-342.
Curran, J. M. & Meuter, M. L. 2007. Encouraging existing customers to switch to self-service technologies: put a little fun in their lives. Journal of Marketing Theory and Practice 15 (4), 283-298.
Curran, J. M., Meuter, M. L. & Surprenant, C. F. 2003. Intentions to use self-service technologies: a confluence of multiple attitudes. Journal of Service Research 5 (3), 209-224.
Deloitte. 2018. A new era for privacy: GDPR six months on. Deloitte. Available: <URL: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf>
Dinev, T. & Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. Information Systems Research 17 (1), 61-80.
Dinsmore, J., Swani, K., Goodrich, K. & Konus, U. 2021. Introduction: advancing understanding of mobile applications in marketing. Journal of Business Research 126, 361-362.
Dwivedi, Y. K., Ismagilova, E., Hughes, L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, A. P., Rowley, J., Salo, J., Tran G. A. & Wang, Y. 2021. Setting the future of digital and social media marketing research: perspectives and research propositions. International Journal of Information Management, 59, 102168.
European Union (2016). Regulation 2016/679 of the European parliament and the Council of the European Union. Available: <URL: https://gdpr-info.eu/>

Fan, H. & Poole, M. S. 2006. What is personalization? Perspectives on the design and implementation of personalization in information systems. Journal of Organizational Computing and Electronic Commerce 16 (3), 179-202.

Fang, Y., Chiu, C. & Wang, E. T. G. 2011. Understanding customers' satisfaction and repurchase intentions an integration of IS success model, trust, and justice. Internet Research 21 (4), 479-503.

Fang, Y. 2019. An app a day keeps a customer connected: explicating loyalty to brands and branded applications through the lens of affordance and service-dominant logic. Information & Management 56 (3), 377-391.

Fehrenbach, D. & Herrando, C. 2021. The effect of customer-perceived value when paying for a product with personal data: a real life experimental study. Journal of Business Research 137, 222-232.

Fornell, C. & Larcker, D. F. 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 18 (1), 39.

Garson, D. G. 2016. Partial Least Squares: regression & structural equation models. Statistical Associates Publishing. Available: <URL: https://www.smartpls.com/resources/ebook_on_pls-sem.pdf >

Gefen, D., Karahanna, E. & Straub, D. 2003. Trust and TAM in online shopping: an integrated model. MIS Quarterly 27 (1), 51-90.

Gelbrich, K. & Sattler, B. 2014. Anxiety, crowding, and time pressure in public self-service technology acceptance. The Journal of Services Marketing 28 (1), 82-94.

Goldberg, R., Mangold, M, Marsh, M. & Sides R. 2019. Consumer privacy in retail: the next regulatory and competitive frontier. Deloitte. Available: <URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-retail-privacy-survey-2019.pdf >

Goldfarb, A., Tucker, C., 2013. Why managing consumer privacy can be an opportunity. MIT Sloan Management review. Available: <URL: https://sloanreview.mit.edu/article/why-managing-consumer-privacy-can-be-an-opportunity/>

Gu, J., Xu, Y., Xu, H., Zhang, C. & Ling, H. 2017. Privacy concerns for mobile app download: an elaboration likelihood model perspective. Decision Support Systems, 95, 19-28.

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K. & Calle, T. 2019. Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: identifying intrusiveness as the critical risk factor. Computers in Human Behavior 95, 295-306.

Gupta, S., Chopra, R., Tanwar, S. & Manjhi, S. K. 2021. Consumer trust in mobile food delivery apps: exploring the antecedents and consequences. International Journal of Mobile Human Computer Interaction 13 (1), 33-55.

Hair, J. F., Ringle, C. M. & Sarstedt, M. 2011a. PLS-SEM: indeed, a silver bullet. Journal of Marketing Theory and Practice 19 (2), 139-152.

Hair, J. F., Risher, J. J., Sarstedt, M. & Ringle, C. M. 2019. When to use and how to report the results of PLS-SEM. European Business Review 31 (1), 2-24.

Hair, J. F., Sarstedt, M., Ringle, C. M. & Mena, J. A. 2011b. An assessment of the use of partial least squares structural equation modeling in marketing research. Journal of the Academy of Marketing Science 40 (3), 414-433.

Hair, J. F., Wolfinbarger, M., Money, A. H., Samouel, P. & Page, M. J. 2015. The essentials of business research methods. Third edition. Routledge.
Hair, F. Jr, Sarstedt, M., Hopkins, L. & G. Kuppelwieser, V. 2014. Partial least squares structural equation modeling (PLS-SEM): an emerging tool in business research. European Business Review 26 (2), 106–121.
Harbach, M., Hettig, M., Weber, S. & Smith, M. 2014. Using personal examples to improve risk communication for security & privacy decisions. Conference on Human Factors in Computing Systems 26.4.2014, Toronto, Ontario, Canada.
Heo, J. & Chang, C. 2018. Factors influencing intention to accept location-based mobile advertising among young mobile user segments: a social exchange perspective. International Journal of Mobile Communications, 16 (6), 607-623.
Hofacker, C. F., Malthouse, E. C. & Sultan, F. 2016. Big data and consumer behavior: imminent opportunities. The Journal of Consumer Marketing 33 (2), 89-97.
Hsieh, J. & Li, H. 2022. Exploring the fit between mobile application service and application privacy. The Journal of Services Marketing 36 (2), 264-282.
Hulland, J. 1999. Use of partial least squares (PLS) in strategic management research: a review of four recent studies. Strategic Management Journal 20 (2), 195-204.
Jacobson, J., Gruzd, A. & Hernandez-Garcia, A. A. 2019. Social media marketing: who is watching the watchers? Journal of Retailing and Consumer Services 53 (03), 101774.
Kang, J. & Namkung, Y. 2019. The role of personalization on continuance intention in food service mobile apps: a privacy calculus perspective. International Journal of Contemporary Hospitality Management 31 (2), 734-752.
Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. 2017. Beyond the personalization-privacy paradox: privacy valuation, transparency features, and service personalization. Journal of Management Information Systems 34 (2), 369-400.
Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. 2013. Information disclosure on mobile devices: re-examining privacy calculus with actual user behaviour. International Journal of Human-Computer Studies 71 (12), 1163-1173.
Kemp, S. 2022. Digital 2022 global overview report. Datareportal webpage. Available: <URL: https://datareportal.com/reports/digital-2022-global-overview-report >
Kim, D. J., Ferrin, D. L. & Rao, H. R. 2008. A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decision Support Systems 44 (2), 544-564.
Kim, D. J., Ferrin, D. L. & Rao, H. R. 2009. Trust and satisfaction, two stepping stones for successful e-commerce relationships: a longitudinal exploration. Information Systems Research 20 (2), 237-257.
Komiak, S.Y. & Benbasat, I. 2006. The effects of personalization and familiarity on trust and adoption of recommendation agents. MIS (30) 941-960.
Kotler, P., Kartajaya, H. & Setiawan, I. 2021. Marketing 5.0: technology for humanity. Wiley.
Kupietzky, J. 2021. How push notifications drive audience engagement with quick snackable content. American Marketing Association. Available: <URL: https://www.ama.org/marketing-news/how-push-notifications-drive-audience-engagement-with-quick-snackable-content/>
Lee, C., Tsao, C. & Chang, W. 2015. The relationship between attitude toward using and customer satisfaction with mobile application services: An empirical study

from the life insurance industry. Journal of Enterprise Information Management 28 (5), 680-697.
Lee, H., Choi, S. Y. & Kang, Y. S. 2009. Formation of e-satisfaction and repurchase intention: moderating roles of computer self-efficacy and computer anxiety. Expert Systems with Applications 36 (4), 7848-7859.
Lee, S. W., Sung, H. J. & Jeon, H. M. 2019. Determinants of continuous intention on food delivery apps: extending UTAUT2 with information quality. Sustainability 11 (11), 3141.
Leppäniemi, M., Karjaluoto H. & Saarijärvi, H. 2017. Customer perceived value, satisfaction, and loyalty: the role of willingness to share information. International Review of Retail, Distribution and Consumer Research 27 (2), 164 – 188.
Li, H., Sarathy, R. & Xu, H. 2011. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Systems 51 (3), 434-455.
Luceri, B., Bijmolt, T., Bellini, S. & Aiolfi, S. 2022. What drives consumers to shop on mobile devices? Insights from a meta-analysis. Journal of Retailing 98 (1), 178-196.
Malhotra, N. K., Birks, D. F., Wills, P. A. & Wills, P. 2013. Marketing Research (4th ed.). Pearson Education UK.
Malhotra, N. K., Kim, S. S. & Agarwal, J. 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information System Research 15 (4). 336-355.
Mandal, P. C. 2019. Public policy issues in direct and digital marketing – concerns and initiatives: public policy in direct and digital marketing. International Journal of Public Administration in the Digital Age 6 (4), 54-71.
Marketing Science Institute. 2020. Research priorities 2020-2022. Available: <URL: https://www.msi.org/wp-content/uploads/2021/07/MSI-2020-22-Research-Priorities-final.pdf-WORD.pdf>
Marketo. 2021. Mobile marketing new. Marketo webpage. Available: <URL: https://www.marketo.com/mobile-marketing/>
Martin, K. D. & Murphy. P. E. 2017. The role of data privacy in marketing. Journal of the Academy of Marketing Science 45 (2), 135-155.
Mayer, R., Davis, J. & Schoorman, F. 1995. An integrative model of organizational trust. The Academy of Management Review 20 (3), 709-734.
McAllister, D. 1995. Affect-based and cognition-based trust as foundations for interpersonal cooperation in organizations. Academy of Management journal 38 (1), 24-59.
McDonald, A.M. & Cranor, L. F. 2008. The cost of reading privacy policies. Journal of Law and Policy for The Information Society 4 (3), 543-568.
McKnight, D. H. & Chervany, N. L. 2001. What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. International Journal of Electronic Commerce 6 (2), 35-59.
Meng, W., Ding, R., Chung, S. P., Han, S. & Lee, W. 2016. The price of free: privacy leakage in personalized mobile in-app ads. Network and Distributed System security symposium conference. Available: <URL: https://wenke.gtisc.gatech.edu/papers/ndss16_mobile_ad.pdf >

Meuter, M. L., Ostrom, A. L., Bitner, M. J. & Roundtree, R. 2003. The influence of technology anxiety on consumer use and experiences with self-service technologies. Journal of Business Research 56 (11), 899-906.

Miller, J., D., Lim, J. & Scott, D., M. 2020. Data-first marketing. How to complete and win the age of analytics. Wiley.

Milne, G. R. & Boza, M-E. 1999. Trust and concern in consumers' perceptions of marketing information management practices. Journal of Interactive Marketing 13 (1), 5-24.

Moorman, C. 2021. The CMO survey. Managing and measuring marketing spending for growth and return. Available: <URL: https://cmosurvey.org/wp-content/uploads/2021/08/The_CMO_Survey-Highlights_and_Insights_Report-August_2021.pdf>

Morey, T., Forbath, T. & Schoop, A. 2015. Customer data: designing for transparency and trust. Harvard Business Review 93 (5), 96-105.

Nath, S. 2015. Madscope: Characterizing mobile-app target ads. In proceedings of the 13th annual international conference on mobile systems, applications, and services. AMC. Available: <URL: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/main-4.pdf>

Newman, D. 2021. Apple's privacy updates push CMO's into a cookie-less world. Forbes. Available: <URL: https://www.forbes.com/sites/danielnewman/2021/05/19/apples-privacy-updates-push-cmos-into-a-cookie-less-world/?sh=42f40ebb7c3b>

Okazaki, S., Eisend, M., Plangger, K., de Ruyter, K. & Grewal, D. 2020. Understanding the strategic consequences of customer privacy concerns: a meta-analytic review. Journal of Retailing 96 (4), 458-473.

Ozturk, A. B., Nusair, K., Okumus, F. & Singh, D. 2017. Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. Information Systems Frontiers 19 (4), 753-767.

Pentina, I., Zhang, L., Bata, H. & Chen, Y. 2016. Exploring privacy paradox in information-sensitive mobile app adoption: a cross-cultural comparison. Computers in Human Behavior 65, 409-419.

Ray, A. & Bala, P. K. 2021. User generated content for exploring factors affecting intention to use travel and food delivery services. International Journal of Hospitality Management 92, 102730.

Ray, A., Dhir, A., Bala, P. K. & Kaur, P. 2019. Why do people use food delivery apps (FDA)? A uses and gratification theory perspective. Journal of Retailing and Consumer Services 51, 221-230.

Rialti, R., Filieri, R., Zollo, L., Bazi, S. & Ciappei, C. 2022. Assessing the relationship between gamified advertising and in-app purchases: a consumers' benefits-based perspective. International Journal of Advertising 41 (5), 868-891.

Rowles, D. 2017. Mobile marketing. How mobile marketing is revolutionizing marketing communications and advertising. 2nd edition. Kogan Page.

Schoenbachler, D. D. & Gordon, G. 2002. Trust and customer willingness to provide information in database-driven relationship marketing. Journal of Interactive Marketing 16 (3), 2-16.

Schoorman, F. D., Mayer, R. C. & Davis, H. D. 2007. An integrative model of organizational trust: past, present and future. The Academy of Management Review 32 (2), 344-354.

Shankar, V. 2016. Mobile marketing: the way forward. Journal of Interactive Marketing, 34, 1-2.

Sievert, M. E., Albritton, R. L., Roper, P. & Clayton, N. 1988. Investigating computer anxiety in an academic library. Information Technology and Libraries 7 (3), 243-252.

Smith, H., Milburg, S. & Burke, S. 1996. Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly 20 (2), 167-196.

Smith, PR. & Zook, Ze. 2020. Marketing communications: integrating online and offline customer engagement and digital technologies. 7th edition. KoganPage.

Stocchi, L., Michaelidou, N. & Micevski, M. 2019. Drivers and outcomes of branded mobile app usage intention. The Journal of Product & Brand Management 28 (1), 28–49.

Stocchi, L., Pourazad, N., Michaelidou, N., Tanusondjaja, A. & Harrigan, P. 2021. Marketing research on mobile apps: past, present, and future. Journal of the Academy of Marketing Science 50 (2), 195-225.

Struik, N., (2021). First-party data is key in a new era for digital marketing. Deloitte. Available: <URL: https://www2.deloitte.com/nl/nl/pages/customer-and-marketing/articles/first-party-data-is-key-in-a-new-era-for-digital-advertising-c.html>

Su, D. N., Nguyen, N. A. N., Nguyen, L. N. T., Luu, T. T. & Nguyen-Phuoc, D. Q. 2022. Modeling consumers' trust in mobile food delivery apps: perspectives of technology acceptance model, mobile service quality and personalization-privacy theory. Journal of Hospitality Marketing & Management 31 (5), 535-569.

Sullivan, Y. W. & Kim, D. J. 2018. Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments. International Journal of Information Management 39, 199-219.

Sutanto, J. Palme, E., Tan, C. H. & Phang, C. W. 2013. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Quarterly 37 (4), 1141-1164.

Sydow, L. 2021. Consumers in five countries now spend more than 5 hours a day in apps. App annie. App annie webpage. Available: <URL: https://www.appannie.com/en/insights/market-data/consumers-in-five-countries-now-spend-more-than-5-hours-a-day-in-apps/>

Temkin, D. March 3, 2021. Charting a course towards a more privacy-first web. Google ads & commerce blog. https://blog.google/products/ads-commerce/a-more-privacy-first-web/

Treiblmaier, H. (2007). Users' perceptions of benefits and costs of personalization. Proceeding of the International Conference on Information Systems. Montreal, Quebec, Canada. Available: <URL: https://core.ac.uk/download/pdf/301340531.pdf >

Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. 2011. The effect of online privacy information on purchasing behavior: an experimental study. Information Systems Research 22 (2), 254-268.

Turilli, M. Floridi, L. 2009. The ethics of information transparency. Ethics and Information Technology 11 (2), 105-112.

Venkatesh, V. 2000. Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model. Information Systems Research 11 (4), 342-365.

Wang, E. S. & Lin, R. 2017. Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. Behaviour & Information Technology 36 (1), 2–10.

Wang, N., Shen, X. & Sun, Y. 2013. Transition of electronic word-of-mouth services from web to mobile context: a trust transfer perspective. Decision Support Systems, 54 (3), 1394-1403.

Wang, T., Duong, T. D. & Chen, C. C. 2016. Intention to disclose personal information via mobile applications: a privacy calculus perspective. International Journal of Information Management 36 (4), 531-542.

Wang, Y., Genc, E. & Peng, G. 2020. Aiming the mobile targets in a cross-cultural context: effects of trust, privacy concerns, and attitude. International Journal of Human-Computer Interaction 36 (3), 227-238.

Wohllebe, A., Hübner, D., Radtke, U. & Podruzsik, S. 2021. Mobile apps in retail: effect of push notification frequency on app user behavior. Innovative Marketing 17 (2), 102-111.

Wood, M. 2019. Today's Firefox blocks third-party tracking cookies and cryptomining by default. Mozilla blog post. Available: <URL: https://blog.mozilla.org/en/products/firefox/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/>

Wottrich, V. M., van Reijmersdal, E. A. & Smit, E. G. 2018. The privacy trade-off for mobile app downloads: the roles of app value, intrusiveness, and privacy concerns. Decision Support Systems, 106, 44-52.

Xu, D. J. 2006. The Influence of personalization in affecting consumer attitudes toward mobile advertising in China. The Journal of Computer Information Systems, 47 (2), 9–19.

Xu, H., Dinev, T., Smith, J. & Hart, P. 2011. Information privacy concerns: linking individual perceptions with institutional privacy assurances. Journal of The Association for Information Systems 12 (12), 798-824.

Xu, H., Teo, H.H., Tan, B.C. & Agarwal, R. 2009. The role of push-pull technology in privacy calculus: the case of location-based services. Journal of Management Information Systems 26 (3), 135-174.

Yang, K. & Forney, J. C. 2013. The moderating role of consumer technology anxiety in mobile shopping adoption: differential effects of facilitating conditions and social influences. Journal of Electronic Commerce Research 14 (4), 334-347.

Zhang, K. Z., Cheung, C. M. & Lee, M. K. 2014. Examining the moderating effect of inconsistent reviews and its gender differences on consumers' online shopping decision. International Journal of Information Management 34 (2), 89-98.

Zhao, L., Lu, Y. & Gupta, S. 2012. Disclosure intention of location-related information in location-based social network services. International Journal of Electronic Commerce 16 (4), 53–90.

Zhou, T. 2012. Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. Journal of Electronic Commerce Research 13 (2), 135-144.

APPENDIX 1 CONSTRUCT MEASUREMENT ITEMS

Construct Measurements items		
Construct	**Measurement Items**	**Source**
Personalization *7-point scale: from "Strongly disagree" to "Strongly agree"	1. The mobile application provider can send to me personalized deals and/or ads that are tailored based on my online activity. 2. The mobile application provider can send to me relevant promotional information that are tailored based on my preferences and/or personal interest. 3. The mobile application provider can send to me the type of deals and/or ads that I might like.	Wang et al. 2016. Intentions to disclose personal information via mobile application: A privacy calculus perspective. International Journal of Information Management 36, 531-542.
Privacy Risk *7-point scale: from "Strongly disagree" to "Strongly agree"	1. Sharing the mobile application provider with my personal information would involve many unexpected problems. 2. Sharing my personal information to the mobile application provider would be risky. 3. The potential for loss in sharing my personal information to the mobile application provider would be high.	Wang et al. 2016. Intentions to disclose personal information via mobile application: A privacy calculus perspective. International Journal of Information Management 36, 531-542.
Trust *7-point scale: from "Strongly disagree" to "Strongly agree"	1. The mobile application provider would be trustworthy in handling my personal information. 2. The mobile application provider would tell the truth and fulfill promises related to the information I share with the application. 3. I trust that the mobile application provider would keep my best interests in mind when dealing with my personal information. 4. The mobile application provider is in general predictable and consistent regarding the usage of my personal information.	Sutanto et al. 2013. Addressing the Personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Quarterly 37 (4), 1141-1164.

Willingness to share information *7-point scale: from "Strongly disagree" to "Strongly agree"	1. I am willing to share personal information about me to the mobile application provider. 2. I am willing to share information about my location to the mobile application provider.	Leppäniemi et al. 2017. Customer perceived value, satisfaction, and loyalty: the role of willingness to share information. The International Review of Retail, Distribution and Consumer research 27 (2), 164-188.
Intention to accept in-app messages *7-point scale: from "Strongly disagree" to "Strongly agree"	1. I will allow the mobile app provider to send me in-app messages based on the personal information I share. 2. I will allow the mobile app provider to send me in-app messages based on my location.	Heo et al. 2018. Factors influencing intention to accept location-based mobile advertising among young mobile user segments: a social exchange perspective. International Journal of Mobile Communications 16 (6), 607-623.
Technology anxiety *7-point scale: from "Strongly disagree" to "Strongly agree"	1. I feel apprehensive about using new technologies. 2. I have avoided a new technology because it is unfamiliar to me. 3. I hesitate to use a new technology for fear of making mistakes I can't correct.	Meuter et al. 2003. The influence of technology anxiety on consumer use and experiences with self-service technologies. Journal of Business Research 56 (11), 899-906.