VILNIAUS UNIVERSITETO
VERSLO MOKYKLA

VILNIUS UNIVERSITY BUSINESS SCHOOL

DIGITAL MARKETING STUDY PROGRAM

SUVOKIAMO M-KOMERCIJOS PROGRAMĖLIŲ PRIVATUMO POLITIKOS VEIKSMINGUMAS NAUDOTOJŲ NORUI DALYTIS ASMENINE INFORMACIJA	***THE PERCEIVED EFFECTIVENESS OF M-COMMERCE APP PRIVACY POLICIES ON USER WILLINGNESS TO SHARE PERSONAL INFORMATION***

EMİNE ÖZMEN

Master Thesis

Supervisor: Lecturer Gintarė Gulevičiūtė

Vilnius, 2024 m.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

LIST OF APPENDIXES

INTRODUCTION

The relevance of the thesis

According to the statistics providen by Statista (2023), more than 6.8 billion people use smartphones and this usage is expected to increase in the coming years. Mobile app usage is also increasing in conjunction with smartphone usage, and is expected to increase in the near future with no signs of slowing down. According to research by eMarketer (2020), US adults spend 88% of their smartphone use time on mobile apps. Another research conducted by The Manifest (2018), shows that %51 of people check mobile apps on their phone 1 to 10 times a day. The place and importance of mobile apps in our lives has increased and continues to increase.

The issue of privacy has entered our lives with digitalization. In the digitalized world, users' privacy concerns have started to increase. People's information, which is mostly personal, is being collected and stored in more and more digital areas every day. Personal information, previously known only to individuals' close circles, is now stored on phones, tablets, social media, mobile apps, internet providers and more (Isley, 2015). According to the Jupiter Research (2002), users' concerns about their privacy are increasing day by day. In a 2001 survey, 70% of users declared that they were concerned about their online privacy.

One of the most widely used security mechanisms on the web is privacy policies. Privacy policy statements provide users with a detailed explanation of how their personal information will be used. It is important for users to know how their personal data will be used in order to provide consumer confidence. Therefore, privacy policies are one of the easiest ways to provide users with the necessary trust. However, companies that provide privacy policy, websites, mobile application owners and others can make changes to their privacy policies without informing users (Miyazaki and Krishnamurthy, 2002; Peterson et al, 2007).

The fact that there are many and different types of mobile applications makes the market very competitive and dynamic. Privacy policies, with the transparency they provide, can be beneficial in the decision-making process of users who care about their privacy and sharing or storing their data (Peterson et al, 2007). Privacy policies inform users about the privacy statements and practices of providers and form a cornerstone for users by being involved in decision-making processes. For users, privacy policies are the only sources of information that platforms can obtain on how to use their personal data and how to protect their privacy. For this reason, privacy policies are have great importance for users (Jensen et al, 2004).

One of the previous studies about the impact of transparency of mobile privacy policies on consumers' decision making has shown that mobile application privacy policies do not affect the outcome of consumers' decisions, but consumers better understand the scope of the decision they make in the decision-making process (Betzing et al, 2019). According to the another research conducted by Phelps et al, (2001), shows that consumers' privacy concerns are negatively related to the purchasing decision process and it is important to understand the antecedents of privacy concerns and develop policies to mitigate the concerns. Another research conducted by Popova et al, (2012) shows that, security is the most important concept for users. So, privacy policies have an important impact on user trust and privacy concerns. Therefore, the purpose of this study is to investigate the effectiveness of m-commerce apps privacy policies on users' willingness to share personal information.

The problem of the paper is the following: Since the privacy policy is a feature that every m-commerce app has, how does the perceived effectiveness of M-commerce privacy policies impact users' willingness to share personal information, taking into account factors such as trust and privacy concerns?

The aim of the paper is to find out what impact the perceived effectiveness of M-commerce privacy policies will have on users' willingness to share personal information, taking into account the impact of trust and privacy concerns.

Tasks of the research paper:

- To analyze the concept of privacy policies and data privacy
- To investigate the perceived effectiveness of m-commerce app privacy policies on user privacy concerns and trust
- To investigate how perceived effectiveness of m-commerce app privacy policies are affecting the users' willingness to share personal information
- To select an appropriate research model for defining the perceived effectiveness of m-commerce app privacy policies on users' willingness to share personal information
- Select the appropriate methods for data collection and collect the data needed for defining the perceived effectiveness of the mobile app privacy policy on the users'

willingness to share personal information through various methods of data collection, and analyze it

- Based on the findings of the research, present conclusions and provide recommendations about the results of the research.

Research Methods

Quantitative methodology approach **is chosen** for this topic. Empirical data collection method - online questionnaire survey.

Theoretical methods were being applied: **document analysis, narrative analysis.**

Empirical data processing methods also had been used.

The structure of the thesis

The study consists of 3 main parts: The first part is the analysis of the previous literature, the second part is the methodology, and the last part is the interpretation of the research results. The literature analysis part gives an understanding and overview of the privacy policy concept, perceived effectiveness of m-commerce app privacy policies, user privacy concerns, trust and willingness to share personal information. In the methodology part, in order to understand users' perspectives on m-commerce app privacy policies, and their effect on users' willingness to share personal information, a questionnaire (survey) will be conducted as a research model consisting of various questions. Respondents will be selected from adults who use m-commerce apps. In the analysis part, the evaluations and the outputs of the results of the research, and suggestions for future research are presented. Additionally, in this study Chat GPT 3.5 version was used to generate ideas and check the data analysis results.

1. THEORETICAL ANALYSIS OF THE PERCEIVED EFFECTIVENESS OF M-COMMERCE APP PRIVACY POLICIES ON USER WILLINGNESS TO SHARE PERSONAL INFORMATION

1.1. M-commerce apps privacy policies

1.1.1. Definition and components of data privacy

The volume of data produced around the world is increasing at a rapid pace. According to the European Parliamentary Research Service (EPRS) (2023), a total of 33 zettabytes of data were produced in the world in 2018 and this data volume is expected to increase to 175 zettabytes by 2025. To better understanding, one zettabyte is equal to 10^{21} (1,000,000,000,000,000,000,000 bytes) or 1 sextillion bytes and to understand how big this data, 44 Zettabytes can be considered "6.6 stacks of iPads from Earth to the Moon" (Aalst, 2016).

Especially if we take into account that Information Technologies has radically changed our lives in the last 15 years, users can access the internet and the rest of the world anytime, anywhere, using mobile phones, laptops, tablets or any device with internet access. Although this situation makes the lives of users easier, on the other hand, it has also had significant effects on users' privacy (Vimercati et al, 2012). According to the European Union General Data Protection Regulation (2016), “personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” Data such as content shared by users on social media, demographic data, e-mails, medical data, photos and videos, location informations are defined as personal data and being shared, collected and disseminated on the internet more and more every day. Personal data may be collected for different purposes, but sharing this data may put people's privacy at risk (Vimercati et al, 2012). According to the SNIA (2023), data privacy is a field of data protection concerned with the appropriate processing of sensitive and confidential data, including personal data. According to the European Union General Data Protection Regulation (GDPR) (2016), for organizations subject to the GDPR, there are two broad categories: data protection and data privacy. Data protection means keeping data safe from unauthorized access and data privacy means empowering your users to make their own decisions about who can process their data and for what purpose. It is very important to ensure that the privacy of users is protected in accordance with data privacy and data protection conditions. Users' personal data should be kept confidential and not be traceable and easily shareable. Another example of data protection laws is The Personal Data Protection Law of Turkey. It came into force after its publication in the Official Gazette on 7 April 2016. The purpose of The Personal Data Protection Law expressed as “To protect the fundamental rights and freedoms of individuals, especially the privacy of private life, in the processing of personal data and to regulate the obligations of real and legal entities processing personal data and the procedures and principles to be followed.” According to The Personal Data Protection Law, everyone has the right to request the protection of their personal data. Individuals have the right to be informed about the use of their personal data, to access existing data and to request the deletion or editing of this data. Personal data can only be collected and processed with the consent of individuals (Official Gazette, 2016)

In conclusion, As a result, with the increase in the amount of data produced, shared and stored all over the world every second and the access of users and companies to this data gradually, concepts such as "data privacy, personal data, user privacy" have been added to our lives. With the increasing importance of data privacy, companies, governments, institutions and organizations, even the simplest level of websites, have developed regulations on the protection of data privacy, the use and storage of users' personal data. One of the most important examples of this is GDPR and The Personal Data Protection Law of Turkey.

1.1.2. Concepts of mobile app privacy policies

Mobile applications have become an indispensable part of our daily life (Balapour et al, 2020). A study conducted in 2018 showed that individuals in the USA spend an average of three and a half hours a day on mobile devices, and mobile applications account for 90% of internet time on smartphones and 77% on tablets (Wurmser, 2018). Mobile apps, defined as software applications developed for use on tablets and smartphones (Lim et al, 2015), are user-friendly and often free of charge, and they provide a variety of services like dating, payment/finance, social networking, fitness, gaming and etc (Brandtzaeg et al, 2018).

Before today's technology, the personal information of individuals was known by their close circles or acquaintances. However, with today's technology, all this personal information is known and stored by mobile phone service providers, mobile applications, e-mail service providers, social networks, tablets, computers and smart phones. Especially mobile devices are devices that individuals carry with them all the time and have location and personal information. Therefore, this situation is quite worrying in terms of privacy. Privacy policies are special informative texts about a website, application or company that describe how users' data is collected, used, stored and shared (Isley, 2015). Privacy policies inform users about what personal data is collected, how this data will be used, stored and with whom it will be shared. In addition, privacy policies exist to protect companies, application owners, websites rather than informing users. Because privacy policies are legal texts, they can be error-prone and difficult to read (Olurin et al, 2012; Anton et al, 2004).

Mobile applications should request permission to access users' personal data before installation or at runtime (Aydin et al, 2017; Balebako et al, 2015). However, according to the research conducted by Balebako et al. (2015), application providers failed to inform users about their practices to collect and share users' personal data. In various studies conducted a few years ago, it was concluded that although users must give permission before sharing their personal data with mobile applications, they usually do so without knowing the consequences of their decisions (Betzing et al, 2019; Almuhimedi et al, 2015; Lin et al, 2012).

Since data transfers occur in the background in mobile applications and users cannot see it concretely, users cannot fully understand how data is processed, collected and shared (Wetherall et al. 2011). In addition, although users are provided with privacy policies to clearly read and give permission, different studies have shown that privacy texts are ineffective in clearly informing users due to their length and legal language (Betzing et al, 2019; McDonald and Cranor 2008; Schaub et al, 2015; Tsai et al, 2011). According to different studies, it has been shown that concerns about security and privacy risks are among the reasons why users do not install mobile applications on their devices or continue to use them after a while (Balapour et al, 2020; Harris et al, 2016; Levenson, 2016; Shah et al, 2014).

Parallel to the increase in the use of mobile applications, the concerns of users while using these applications are also increasing (Balapour et al, 2020; Harris et al, 2016). Users are concerned about security vulnerabilities of mobile applications, theft of their data and abuse of stolen data. Different types of apps collect different data. For example, mobile payment apps may collect and share information about shopping habits. Dating apps collect, share and publish personal data and user location about their users' sexual orientation or preferences (Farnden, Martini, & Choo, 2015).

According to the research conducted by Harris et al. (2016) found that security concerns have a major impact on users' intentions to using mobile apps. As a result of hackers accessing the accounts of users in the Starbucks mobile application in 2015, many mobile users stopped using the application and removed it from their devices (Sullivan, 2015). Mobile application developers need to develop appropriate security and privacy solutions, taking into account the security and privacy concerns of users. If it is intended for users to continue to use mobile applications with a sense of trust, the main concerns of users should be taken into account and combined security measures and privacy solutions should be offered (Balapour et al, 2020).

Brandtzaeg et al. (2018) stated that there is very few research on:

- individual perceptions of mobile application privacy,
- actual data flows in applications, and
- how such perceptions and data flows relate to actual privacy policies in mobile applications.

Again, Brandtzaeg et al. (2018) conducted a survey in Norway on the analysis of personal data flows in applications and made a content analysis of the privacy policies of 21 free and popular android applications. The results of the research showed that more than half of the users who responded avoid downloading or using the applications to avoid sharing their personal data.

A study conducted by Zang et al, (2015), examined 110 popular, free Android and Apple mobile operating system (iOS) apps. Among these applications, they identified applications that shared personal, behavioral and location data with third parties. They found that a significant number of apps share user data with third parties, and Android and iOS operating systems do not require users to notify users that they are sharing their data. While 73% of Android apps share personal information such as email addresses with third parties, 47% of iOS apps share geographic coordinates and other location data with third parties. Furthermore, with the privacy scandal in 2018 in which the data of Facebook's 87 million users was extracted from a third-party application hosted by Cambridge Analytica, it was revealed that the personal data of individual users was used and shared beyond their control. However, the Cambridge Analytica case is not the only one. Data scandals were mentioned earlier in the article. Companies such as Google, Amazon, Apple, Facebook and more collect, share and use their users' personal information (Brandtzaeg et al, 2018; Esayas, 2017).

In conclusion, mobile applications have started to occupy an important place in our lives in recent years. We frequently use these applications on our mobile phones, tablets and personal computers that we always carry with us. Therefore, we share a lot of personal information with these applications. Our address information, email, demographic informations, what we like and dislike, our preferences, location information, our friends and more. Considering all these, the rapid rise and use of mobile applications raise important questions about privacy. How much of the data we share is used, how much is shared or stored, which of our data is kept securely? All these questions are becoming more important for mobile app users every day.

With the development of new technologies and mobile applications, people's privacy experience is spreading from the physical space to the online space. This makes privacy much more complex in the new technological age. Although privacy policies and brands, websites or mobile applications aim to inform users about the use of personal data, they are not always very successful in this regard. The many scandals we mentioned in the article over the past 10 years are an example of this. Therefore, in parallel with all these, privacy concerns of users are also increasing.

1.1.3. Privacy in mobile commerce (M-commerce)

There are many definitions for mobile commerce. One of them, "M-commerce refers to conducting any transaction, involving the transfer of ownership or rights to use goods and services, which is initiated and/or completed by using mobile access to computer mediated networks with the help of an electronic device." (Khalifa et al, 2012). Mobile commerce can be defined as a process of trading goods or services, and these trade transactions are conducted through wireless handheld devices such as mobile phones, personal digital assistants (PDAs), wireless computers, and others (Jurevičiūtė, 2011; Michael and Salter, 2006).

Today, mobile commerce has become a rapidly growing and developing market with the increase in integration with internet applications (Khalifa et al, 2012). According to Statista (2023) data, as of the last quarter of 2022, mobile commerce spending in the United States accounts for 38 percent of total digital spending. In the UK, on the other hand, around seven out of ten shoppers in 2022 shopped online using their smartphones. On the other hand, 44 percent of South Korean internet users shop on mobile on a weekly basis.

It is possible to rename mobile commerce as mobile e-commerce (Jurevičiūtė, 2011). Because according to Tiwari et al. (2006), “mobile commerce transactions are simply electronic transactions carried out using a mobile device and wireless network." In other words, transactions made with mobile devices with wireless internet access, such as a mobile phone or tablet. With the widespread use of mobile technology and thus mobile device usage, mobile devices have become an enormous storage area for users' personal information (Eastin et al, 2016). The collection of personal data was once the function of governments and government agencies, but today it has become an inevitable part of daily life for users (Lyon, 2001). Although privacy and data use policies (eg GDPR in Europe) aim to protect users today, according to Cleff (2007), the rapidly expanding data ecosystem is the source of users' mobile information privacy concerns.

One way e-businesses build trust with users is to provide a privacy policy to inform users how to use the following elements: data user, data element, purpose of use, terms and obligations. In addition, e-businesses that have access to users' location data should define whether third-party services can access users' data. All these components are crucial points in shaping privacy policies (Vasileiadis, 2013; Steinfield, 2004). There are fewer studies addressing users' privacy concerns regarding the increasing level of personal information shared in mobile contexts (Kim & Han, 2014). Previous research in this area (i.e., Malhotra et al, 2004; Okazaki et al, 2009; Smith et al, 1996) identifies six factors that contribute to users' information privacy concerns in online environments: data collection, location tracking, data control, inappropriate access, unauthorized secondary use, and awareness of these practices. After collecting their personal data, users want to have control over their use and distribution (Malhotra et al, 2004). Therefore, it has been seen that giving importance to privacy regarding the collection, control, access and use of personal data plays a critical role in building trust in online relationships (Smith et al, 1996).

1.1.4. The perceived effectiveness of privacy policies

Users can review the privacy policy of service providers to learn more about their information privacy practices. As mentioned in previous sections, privacy policies provide users with information on how and for what purpose their data will be used, stored and/or shared. Therefore, users can obtain all necessary information about the data they intend to share with the service provider from their privacy policies. Since privacy policies act as an important bridge between the service provider and the user, service providers must provide users with a privacy policy that is well-written, transparent and contains all the necessary information. In addition, the service provider must comply with all statements made by it. (Zhou, 2017) In recent years, studies focusing on the effectiveness of privacy policies have been increasing (Wang & Wang, 2021). Xu et al. (2011) defined privacy policy effectiveness as “the extent to which a consumer believes that the privacy policy posted online can provide accurate and reliable information about the organization's information privacy practices.” Although there are arguments that users generally do not read privacy policies, some studies have shown that privacy policies are still important for users in making privacy decisions (Tsai et al, 2011; Balapour et al, 2020). An effective privacy policy reduces users' privacy risk and privacy concerns (Xu et al., 2011; Mutimukwe et al., 2020; Wang & Wang, 2021).

Liu et al (2018) divided the information privacy practices that service providers offer to the user into some categories in the content of their privacy policies:

1. First Party Collection/Use: How and why a service provider collects user information.
2. Third Party Sharing/Collection: How user information may be shared with or collected by third parties.
3. User Choice/Control: Choices and control options available to users
4. User Access, Edit, & Deletion: If and how users can access, edit, or delete their information.
5. Data Retention: How long user information is stored.
6. Data Security: How user information is protected.
7. Policy Change: If and how users will be informed about changes to the privacy policy.
8. Do Not Track: If and how Do Not Track signals for online tracking and advertising are honored.
9. International & Specific Audiences: Practices that pertain only to a specific group of users (e.g., children, residents of the European Union, or Californians)
10. Other: Additional privacy-related information not covered by the above categories.

Not every privacy policy presented to users is the same. Some are quite restrictive, while others do not offer the user a real and solid privacy guarantee. For example, some privacy policies guarantee that their users will not share their personal information with third parties under any circumstances, while others may share it with third parties. Therefore, this may cause different reactions in the user. On the other hand, the status of the information requested from the user is also important. For example, requesting sensitive personal data may reduce the user's willingness to share personal information. (Peterson et al, 2007). Therefore, privacy policies that have strong content, protect user rights, and take care to protect/storage the user's personal data are more effective. In this case, these policies may have a more positive impact on the user (Papova et al, 2012).

1.2. Privacy concern and Trust in M-commerce

1.2.1. The concept of privacy concern and users' willingness to share personal information

Because the internet is a global phenomenon, online privacy concerns are also becoming a global concern for users. Today, with rapidly increasing technological developments and increasing internet usage, online privacy of users has become a prominent issue especially in e-commerce discussions (Anic et al, 2018). Online users often measure risks before sharing their personal data, such as misuse or sharing. Because they want to have a sense of trust before sharing their personal data with the website or mobile application they will use. Websites and mobile applications collect users' data, track their visits, and offer personalized content tailored to their personal needs. This can be seen as a beneficial practice for both parties: users receive personalized service, while service providers offer content to users according to their wishes. However, collecting all this information may cause privacy concerns for users. For example, websites can track and record every movement of users on the site, and such information is usually collected automatically and without users' consent (Wu et al, 2012).

Different studies show (Dinev and Hart, 2006; Ginosar and Ariel, 2017) that users are increasingly concerned about their online privacy. Therefore, this situation leads users to give different behavioral responses to their concerns. For example, they choose not to use websites or mobile applications that they consider risky, they share fake information while sharing their personal information, or they prefer to use software that increases privacy (Lwin et al., 2007; Anic et al, 2018).

Phelps et al. (2000) study the antecedents and consequences of users' privacy concerns. According to this study, a conceptual model is proposed in which users' privacy concerns are determined by 4 factors:

- the type of personal information requested,
- the amount of information check offered,
- the potential results and benefits offered in shopping; and
- user characteristics

Phelps et al. argue that the consequences of users' general privacy concerns also influence their future behavioral and attitudinal responses.

According to the another research study by Sheehan and Hoy (1999), it was stated that as users' privacy concerns increase online, they are more likely to exhibit the following behaviors:

- provide incomplete information to websites,
- notify Internet Service Providers about unsolicited e-mail,
- request removal from mailing lists, and
- “flame” online entities sending unsolicited e-mail.

It has also been observed that as users' privacy concerns increase, they are less likely to sign up for websites that request personal data.

On the other hand, Smith et al. (1996) elaborated seven major data privacy concerns of customers:

- Data Collection (storage of large amounts of personal customer data),
- Data Combination (combination of customer data from different databases to gain additional information about a customer),
- Internal Secondary Usage (usage of customer data for an unauthorized secondary purpose within the company),
- External Secondary Usage (disclosure of customer data for an unauthorized -secondary purpose outside the company),
- Errors (deliberate or accidental errors in customer data),
- Improper Access (unauthorized views and edits of customer data), and
- Reduced Judgment (automated decision-making based on customer data).

And according to Preibusch (2013), the study of Smith et al (1996) can be described as the first and most influential work in the field of data privacy concerns.

On the other hand, Anic et al, (2018) developed a research framework based on the antecedents and consequences paradigm of data privacy using the work of Li (2011) and Smith et al, (2011). This conceptual framework covers the individual, regulatory and societal antecedents of users' online privacy concerns.

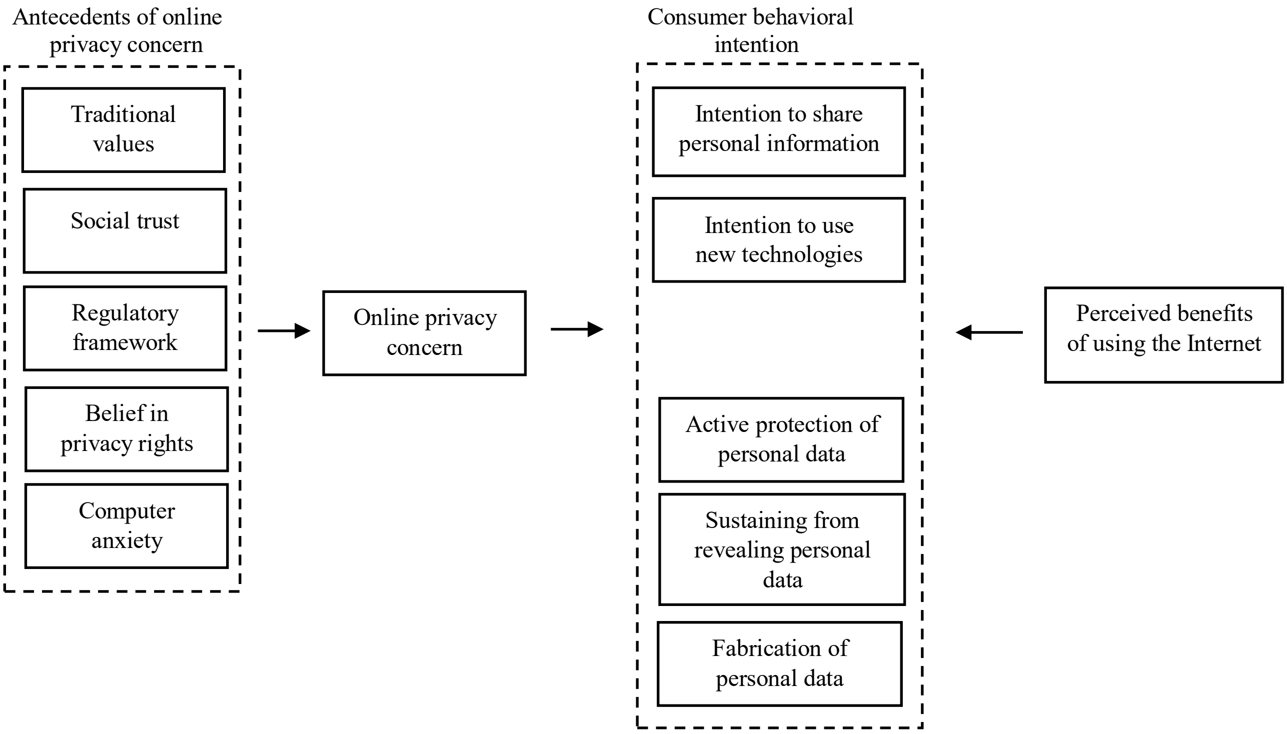

Antecedents of online privacy concern
Traditional values
Social trust
Regulatory framework
Belief in privacy rights
Computer anxiety
Online privacy concern
Consumer behavioral intention
Intention to share personal information
Intention to use new technologies
Active protection of personal data
Sustaining from revealing personal data
Fabrication of personal data
Perceived benefits of using the Internet

Figure 1: *Conceptual framework of antecedents and outcomes of online privacy concern*

Source: Anic et al, (2018)

According to the results of the study of Anic et al, (2018), traditional personal values (VAL) and social trust (ST) of internet users do not have a significant effect on online privacy concerns (OPC). On the other hand, computer anxiety has the biggest impact, followed by the regulatory framework and then belief in privacy right. The study shows that while privacy concerns remain a concern for users, the perceived benefit of using the Internet outweighs users.

In another study conducted by Xu et al (2012), developed the mobile users' information privacy concerns (MUIPC) structure based on the information privacy concerns scale (CFIP) (Smith et al, 1996) and Internet users' information privacy concerns (IUIPC) (Malhotra et al, 2004). The information privacy concern scale (CFIP), developed by Smith et al, (1996), measures individuals' concerns about information privacy practices with 4 subscales: collection, errors, improper access, and unauthorized secondary use. Collection represents the collection of personal data of individuals. Errors and improper access represent companies' errors in protecting data privacy and inappropriate access to the data of these users. Users are concerned about privacy due to errors and inappropriate access. Finally, unauthorized second use represents the use, sale or sharing of users' personal data without their consent (Degirmenci, 2020).

On the other hand, Degirmenci (2020), presented a study examining the impact of previous privacy experience, computer anxiety, perceived control, and app permission concerns on general information privacy concerns of mobile users. It was concluded that the mentioned components have significant effects on the information privacy concerns of the users. One of the findings of the online survey conducted with 775 participants revealed that the current state of application permission requests is problematic and users refuse to disclose their personal information due to concerns about application permission requests.

1.2.2. Privacy awareness

Some users may have different privacy concerns about the same or similar phenomena. This is because the level of privacy awareness that users have is different. As users' internet usage increases, information sharing also increases. Therefore, users acquire information about privacy by reading, seeing, hearing from their close circles, and being exposed directly or indirectly. Thus, users' privacy awareness increases (Balapour et al, 2020). Privacy-conscious people are aware of information and data privacy practices and the use of their personal data by websites or mobile applications (Malhotra et al, 2004). According to Smith et al. (2011) if users are aware of the possibility that websites or mobile applications may collect their personal data without their consent, they have more privacy concerns than users who are not aware of it. Therefore, the privacy awareness of users can affect their attitudes towards mobile applications positively or negatively (Li et al, 2011). Users' perceptions of privacy will affect their behaviors and attitudes such as trust, willingness to use the mobile application, intention to use and intention to disclose information (Dinev et al., 2006; Lowry et al, 2011; Malhotra et al., 2004; Xu et al, 2009).

It is clear that the privacy concerns of users while using websites or mobile applications are effective in sharing their personal data. Users who are concerned about the collection, sharing or disclosure of their personal data do not want to share their information (Wu et al, 2012). For this reason, they may sometimes give up using the mobile application/website or sometimes share false information. At this point, it is of great importance for online or mobile service providers to inform users through privacy policies that they will ensure data security, which data they will collect and for what purpose, and that the collected data will not be shared under user privacy (Balapour et al, 2020).

As a result, it is an undeniable fact that users are concerned about their privacy. If websites or mobile applications request personal data from them, users may be concerned about their privacy and may react in different ways. On the other hand, as mentioned, different studies have found that users' privacy concerns have many different causes and consequences. It has also been observed that users exhibit different attitudes as a result of their privacy concerns for different reasons.

1.2.3. Privacy concerns in M-commerce

In recent years, as the use of mobile applications by users has increased, users' personal data has started to become a fee that they have to pay for using the application. Even if users do not pay for the apps, instead they consciously (or unintentionally) share their personal information, locations, preferences with the apps and pay the mobile app developers by allowing them to access, store and use their personal data. Users accepting permission requests from applications and sharing their personal data has the potential to be a threat to users' privacy. Because the shared information can be used to distinguish users in the case of purchasing services or products, to offer them unsolicited commercial demands, or for fraudulent behavior such as identity theft. For this reason, it would be beneficial for application users to evaluate the cost and benefit of the applications they use (Balapour et al, 2020; Wottrich et al, 2018; Fife et al, 2012).

According to the study conducted by Eastin et al (2016), research findings show that users' concerns about control and unauthorized access to personal information significantly negatively affect m-commerce activities. How US marketers and policy makers address the ownership, collection, use, and sharing of personal data is of great importance to users. Many users struggle with allowing others access to their mobile data, leading to boundary turbulence. On the other hand, the study states that data collection, awareness of collection practices and collecting location information can be seen as more passive dimensions of privacy and do not have a significant impact on consumers' participation in m-commerce. The finding suggests that these particular privacy concerns are not strong predictors of consumers' behavior when it comes to using mobile commerce services. In other words, even if consumers have worries about how their data is collected, how aware they are of the data collection practices, or concerns about sharing their location information, it does not significantly affect their decision to engage in mobile commerce activities. However, informing users about how their data will be handled and seeking clear consent from them may play a role in building trust. By providing transparency and obtaining consent, companies can alleviate some privacy concerns without sacrificing the potential benefits of utilizing big data for business opportunities.

According to the Gurau and Ranchhod (2009), in today's networked society, finding a balance between private and social aspects becomes more complex as information sharing is prevalent. Total privacy control might lead to isolation and missing out on communication benefits. Mobile phones exemplify this situation as they offer personal and social advantages, but they also present privacy challenges. Solutions should be smartly applied to reduce privacy issues while preserving the benefits of mobile communication and computing.

According to Phelps J. et al (2000), information privacy is an utmost security concern. On the other hand, Vasileiadis (2013), argues in his study that some of the users are often concerned with privacy in the context of m-commerce, such as location and personal details. As mobile phones become more common as a portable computing tool, location tracking on mobile devices allows businesses to personalize their offers and ads based on users' preferences and demographics. With this situation, privacy concerns of some users increase and they think that e-businesses do not respect their privacy and use their data for profit. Therefore, it can be concluded that reliability plays a critical role in the context of m-commerce and gaining customer trust is crucial. To build trust with users, e-businesses must provide clear privacy policies that give users control over their location information and usage. Users should have the option to remain anonymous and businesses should protect user data from misuse or unauthorized access.

Another study conducted by Zhang et al. (2015) focuses on users' concerns about information privacy (CFIP) in m-commerce. The research model is based on the APCO model, which examines demographic differences (income, age, education, gender, and experience) and their effects on CFIP. According to the survey results conducted during the research, education level and age significantly affect users' privacy concerns, on the other hand, income level, limited mobile trade experience and gender do not seem to play an important role.

In conclusion, with the increasing use of mobile applications, the privacy concerns of users have been studied in different dimensions. We can talk about the increasing use of mobile applications and a kind of exchange that users make by sharing their personal data to access these applications. Users' concerns about the control and unauthorized access of their personal information negatively affect their m-commerce activities. On the other hand, while the collection of user data and certain privacy concerns regarding mobile applications do not significantly affect users' participation in mobile commerce, informing users about data processing can build trust.

Privacy is a critical concern in mobile commerce, as some users are concerned about sharing their location and personal information with e-businesses. To reduce the privacy concerns of users, businesses and mobile app owners must maintain clear privacy policies, giving users control over their data and the option to remain anonymous. Addressing privacy concerns in m-commerce is a key point for businesses, both users and mobile app owners, and the need for transparent privacy policies to build trust with users should be highlighted.

1.2.4. Importance of Trust

With the increasing amount of data produced and shared worldwide, trust in data privacy is becoming more relevant and important to customers (Berendt et al, 2005; Preibusch et al, 2013; Gimpel et al, 2018). For example, in 2015 the data of 37 million married male and female registered users of the online dating website Ashley Madison were leaked (BBC, 2015), in 2011 Apple was accused of collecting the location data of iPhone and iPad users without their consent (The Guardian, 2011), and Facebook giving the data collected from the profiles of its users to advertising companies (The Telegraph, 2010). Acquisti et al. (2006), defined those as ‘involving misuses of individuals personal information’. As a result, the fact that users' personal identifiable information (PII) is made public, leaked or sold has highlighted the importance of data privacy (Gimpel et al, 2018).

The mention of companies in such data scandals causes economic damage for them as well as damaging their brand image and losing the trust of their customers. On the other hand, they are also at a disadvantage in the competitive market. In companies that gain the trust of their customers in terms of data privacy, customer satisfaction increases and they are in a more advantageous position in the competitive market (Gimpel et al, 2018). For instance, companies such as DuckDuckGo or Silent Circle providing privacy-friendly services. DuckDuckGo, a search engine, doesn’t collect any personal information or behavioral data from users (Tanner 2013). Especially considering that users are more sensitive about theft and leaking of their personal data today, the protection of personal data and data privacy have become very important for companies (Gimpel et al, 2018). In some studies that cited user concerns regarding the protection of personal information, for example Acquisti et al. (2006) mentions the negative impact of the privacy incidents on the market value of the companies. On the other hand, Preibusch et al. (2013) concluded that customers who shop at a privacy-conscious but more expensive online DVD retailer are more satisfied than customers of another cheaper, but less privacy-conscious, online DVD seller.

On the other hand, one way to ensure the trust of users is privacy policies. Users are more likely to trust if they read and understand privacy policies and know for what purpose and with whom they will share their personal data. (Milne & Culnan, 2004) When users perceive that the privacy policy is effective, they also perceive that the online environment in which they are about to transact is safe (Balapour et al, 2020; Wang et al, 2022). Users who feel a sense of trust in the mobile application or website believe there is less uncertainty about the use of the personal information they share (Zimmer et al, 2010). Studies on mobile applications have revealed that companies share and leak users' personal information to unknown targets and third-party ad servers (Brandtzaeg et al, 2018 ; Egele, et al, 2011 ; Enck et al, 2010 ; Zang et al, 2015). states that in online commerce, it is necessary to ensure that users' personal data are well protected and to establish trust between the user and the service provider (Wu et al, 2012).

In conclusion, data privacy, protection of personal data and user privacy issues have also become important for users. Scandals of large companies and brands leaking, selling or sharing users' data have had a negative impact on users. Users began to worry about the purposes for which their personal data would be used, stored or shared. With the increase in users' awareness of data privacy, companies that care about data privacy gain the trust of users, while companies that do not care about them cause users to lose their trust. In addition, it is very important for service providers to provide a privacy policy to protect users' data and to build trust with the user.

1.2.5. Models explaining users' intention to use mobile applications

The Technology Acceptance Model (TAM) by Davis (1989) focuses on user intentions and acceptance of new technology. To the Davis's TAM model, users are influenced by two major factors: perceived usefulness (PU) and perceived ease of use (PEOU). Davis defined perceived usefulness (PU), as 'the degree to which a person believes that using a particular system would enhance his or her job performance' and perceived ease of use (PEOU), defined as “the degree to which a person believes that using a particular system would be free of effort (Davis, 1989).” On the other hand, the classic expectancy theory of motivation, another theory developed by Vroom (1964), is often used to understand the process individuals use when deciding between different behavioral options. According to expectancy theory, individuals are motivated by the desire for an outcome they expect. That is, individuals are likely to choose the effort that will lead to the reward or outcome they desire. (Chiang et al, 2008; Kiatkawsin & Han, 2017; Renko et al, 2012; Chin et al, 2018). Application of Davis's Technology Acceptance Model (TAM) and Vroom's expectancy theory to mobile technology (mTechnology) provide insight into why users decide to use mobile applications (mApps). Two main factors influence users' mApp usage decisions: how useful the mApp is perceived to be and how easy it is to use, both within the context of mTechnology. In addition, when installing the mApp, users have an expectation of the personal benefits they will derive from it, and these expectations of users play an important role in their decision-making processes. Chin et al. (2018) underlines the popularity, perceived value, and effectiveness of mTechnology across diverse demographics. The intense use of mobile devices by users from different demographics shows that they find mobile technologies useful and user-friendly. After the use of mobile devices has become widespread for users, their primary focus is on achieving a desired result: mApp availability on their mobile devices. The resulting benefit can often be described as increased productivity or enjoyment by users. Therefore, it is possible to say that the desire of users for these positive results outweighs their concerns about the potential risks of mobile technology. Users may assume that mobile technologies can provide them with reliable experiences. In essence, applying the TAM and expectancy theories to mTechnology highlights that, perceived usefulness, ease of use, and the user's personal benefit expectation affect the mobile app usage decision.

In order to understand the behavior of users to continue mobile app usage even in case of perceived risk, Shepherd and Kay's (2012) theory of motivated avoidance of sociopolitical information, which is based on system justification theory (Jost & Banaji, 1994) and the subsequent compensatory control theory (Kay et al, 2008). Shepherd and Kay (2012) argue that when people trust an authority to meet their needs and justify this trust by themselves, they tend to avoid information that could undermine or undermine their trust. Motivational avoidance theory can be used to explain why people tend to be complacent about the security of mApps. For example, although users do not have absolute confidence when doing mobile shopping (mShopping), they are also reluctant to completely avoid these transactions due to risk. Therefore, they are willing to trust and believe that mobile shopping applications will ensure their security. For example, when users are mobile shopping, they pay attention to the feedback evaluation scores of the sellers, and when purchasing a product, they are more likely to choose the higher-rated seller rather than the lower-rated seller. Because users choose to rely on vendor feedback from the app they shop with, rather than researching vendors one by one. (Masclet and Pénard, 2012; Yan et al, 2012; Chin et al, 2018).

In a study conducted by Kim and Yoon (2013), Davis's TAM model was used to investigate the factors affecting the use of mobile applications. In the study, various constructs from the TAM model were used to help understand how people perceive and interact with technology: perceived informative usefulness, perceived entertaining usefulness, perceived social usefulness, ease of use, attitude towards app usage, user reviews, and perceived cost-effect. As a result of the study, it was found that perceived informative usefulness, perceived entertaining usefulness, and perceived ease of use had a significant effect on users' attitudes toward using the application. It was founded that when users have positive attitudes towards the application, they are more likely to use the application. Also, user comments played an important role in influencing app usage. In contrast, the study found that the perceived cost-effectiveness of the application did not have a significant impact on users' decision to use the application (Harris et al, 2016).

In conclusion, Davis's TAM model provides a framework for understanding user intentions and acceptance of new technology. On the other hand, Vroom's expectancy theory helps us understand the decision-making processes by taking into account the motivations of individuals to achieve their desired results. The application of these theories to mobile technology helps us understand what factors influence individuals' mobile application installation and usage decisions and provides us with a general framework. Both theories show the importance of personal benefit expectations, which is the common point in the decision-making process of individuals. The use and synthesis of all these theories and models in mobile technology and mobile app installation and usage decisions provides researchers and practitioners with a holistic and valuable perspective on the adoption, installation and use of mobile applications by users.

2. METHODOLOGY OF THE EMPIRICAL RESEARCH ON THE PERCEIVED EFFECTIVENESS OF M-COMMERCE APP PRIVACY POLICIES ON USER WILLINGNESS TO SHARE PERSONAL INFORMATION

2.1 Purpose of the research and research model

The impact of privacy agreements on users' sense of trust and privacy concerns has been widely studied and analyzed by various researchers. As discussed in the literature review section of the research, the content and scope of privacy agreements may have an impact on users' privacy concerns and sense of trust, as well as indirectly have different effects on their willingness to share personal information (Anic et al, 2018; Papova et al, 2012; Mothersbaugh et al. al, 2012; Degirmenci, 2020; Zimmer et al, 2010; Castañeda & Montoro, 2007). However, in the existing literature on the subject, generally the privacy policies of websites and their effects on users have been examined, and research on the mobile application dimension has been limited (Popova et al. 2012; Phelps et al, 2000; Al-Jabri et al, 2019). Therefore, a limited perspective Due to its angle, the author's aim is to expand the current research and enable different factors to be investigated.

Various studies have shown that users are concerned about privacy in online activities. Moreover, almost one-fifth of users have been found to use a secondary email address to avoid giving out their real information online (Phelps et al., 2001). Companies collect and use customers' personal information through registration forms, order forms and/or cookies (Liu, Marchewka and Ku, 2004). Privacy concerns can lead to reluctance to share personal information online and even to users rejecting e-commerce activities (Popova et al, 2012).

The main purpose of the research is to investigate what role privacy policies, users' privacy concerns, the trust they feel or do not feel, have in sharing their personal information with the mobile application and to what extent they affect it. The aim of the author is to find out how the perceived effectiveness of the privacy agreements that users encounter before shopping from mobile commerce applications affect their sense of trust and privacy concerns, taking into account their awareness, and the possibility of sharing their personal information accordingly.

In the presented model, perceived effectiveness of privacy policies and privacy awareness are considered as independent variables. Trust and privacy concerns play a mediating role in measuring the impact of privacy policies on users' willingness to share their personal information. Since users' willingness to share their personal information may vary depending on trust and privacy concerns, users' willingness to share their personal information was treated as a dependent variable. In the end, since users' privacy awareness indirectly affects their willingness to share information, the role of privacy awareness on privacy concerns is discussed.

The presented model is a modification of the Popova et al. (2012), Lauer & Deng, (2007) and Wang & Wang (2021) models which were combined and has been changed based on the addition to the research. In this model, Shepherd and Kay (2012)'s theory of motivated avoidance of sociopolitical information was used while discussing the relationship between trust, privacy concern and willingness to share personal information.

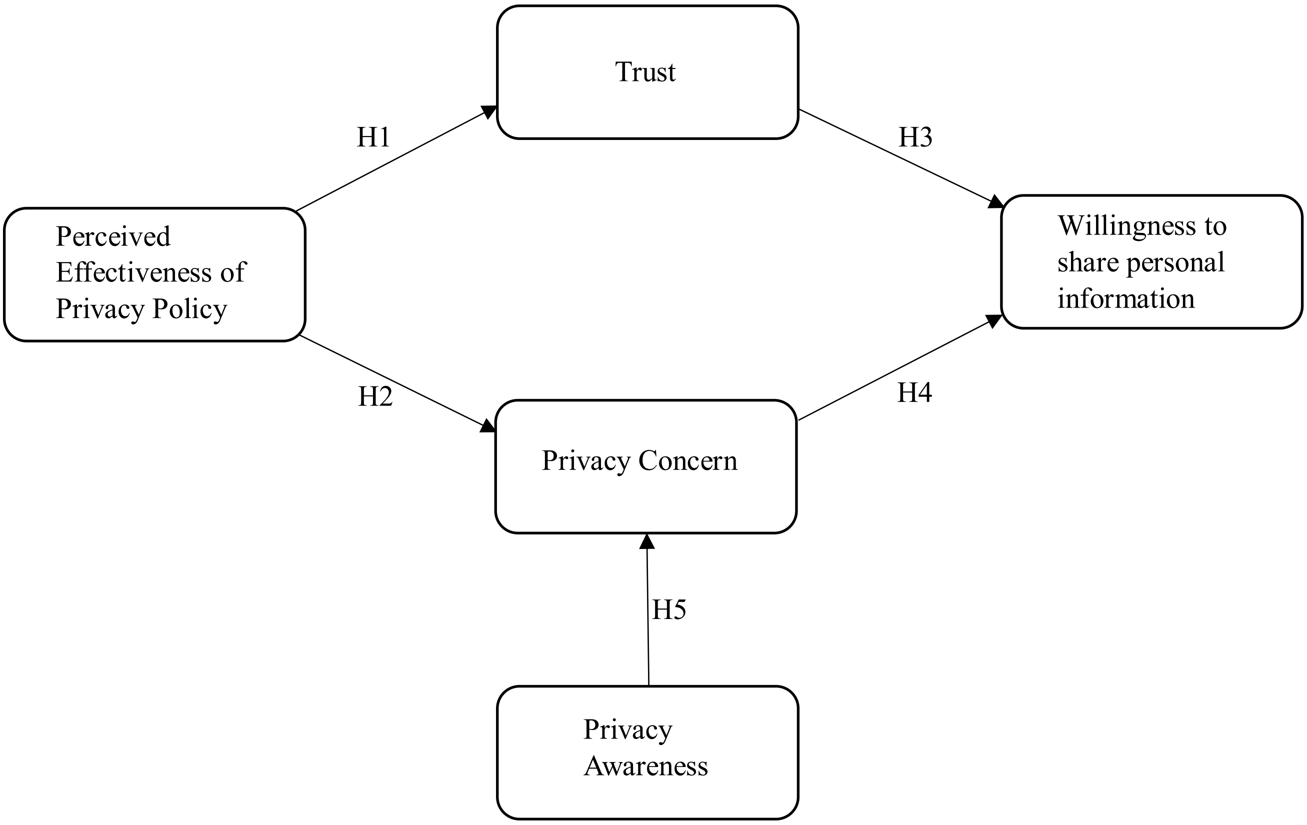

Trust
H1
H3
Perceived Effectiveness of Privacy Policy
Willingness to share personal information
H2
H4
Privacy Concern
H5
Privacy Awareness

Figure 2: *Research model, developed by the author*

Five hypotheses were developed and proposed to measure the interaction of the variables presented in the figure above. It is important to examine the interconnections of various factors that will ultimately influence users' willingness to share personal information. In addition, this research aims to benefit science by examining the relationships between variables, and will also contribute to service providers and companies understanding customers' attitudes about privacy.

One way to increase user trust is to have a privacy policy (Wang et al, 2022) Privacy policies explain how and for what purposes users' data will be used and inform them about the security tools and protection systems of service providers. Therefore, it helps users decide whether to share their personal data (Papova et al, 2012). Some studies argue that privacy policies should be informative and strong texts and should give users assurance in sharing their personal information (Dinev & Hart, 2006; Milne & Boza, 2000). It has been revealed that users perceive mobile applications as secure when they perceive that their privacy policies are highly effective (Balapour et al, 2020). Companies' strong and consistent privacy policies and practices can infer to users that they want to do business fairly with them and create trust in the user. (Lauer & Deng, 2007). Thus, H1 is formed:

H1: The perceived effectiveness of privacy policy has positive impact on trust.

Users' willingness to share personal information is closely related to concerns over privacy. Some studies reveal that users are concerned about losing control over how their personal information is processed and have high levels of privacy concerns (Papova et al, 2012). Research suggests that providing understandable privacy policies is effective in creating a trustworthy online environment and may reduce users' privacy concerns (Milne & Culnan, 2004; Aljukhadar et al., 2010; Bansalet al., 2008). Privacy policies explain how personal data of users is collected and stored or inform about its use. This may help alleviate users' privacy concerns (Zhou, 2017). Research has shown that most users feel less concerned if they encounter a privacy agreement (Earp and Baumer, 2001). Thus, H2 is formed:

H2: As perceived effectiveness of privacy policy increases, privacy concern decreases.

According to research, it is more difficult to develop and maintain trust online than offline because online service providers are more likely to engage in unethical behavior (Zimmer et al, 2010). Extended privacy calculus model (Dinev and Hart, 2006) shows a positive relationships between trust and users' willingness to share personal information. With trust, users' perceived risk decreases and thus they become more willing to share personal information and purchase (Popova et al, 2012; Castañeda & Montoro, 2007). Thus, H3 is formed:

H3: As the trust increases, the willingness to share personal information also increases.

Based on Min and Kim (2015), we can conclude that the desire to share personal data includes sharing on social networking sites, personal sharing on the internet, personal image sharing, location sharing, credit card and address information shared in online shopping, and more. Users' willingness to provide their personal information online is closely related to their concerns about their privacy. (Popova et al, 2012) The consequences of privacy concerns have been examined in different ways in the literature. Some studies have concluded that privacy concerns have a negative impact on information sharing. (Min and Kim, 2015; Kehr et al, 2015; Anic et al, 2018; Popova et al, 2012; Mothersbaugh et al, 2012) Thus, H4 is formed:

H4: As the privacy concern increases, the willingness to share personal information decreases.

According to Hong and Thong (2013), privacy concerns are a multidimensional structure consisting of users' awareness of privacy practices, service providers' information management styles, and the interaction between the user and the third party. Privacy awareness reflects the extent to which an individual is aware of the privacy practices of institutions, organizations and service providers (Malhotra et al. 2004; Phelps et al. 2000). According to some studies, privacy concerns are triggered when users realize that their personal information is being used and/or collected without their permission. (Cespedes and Smith 1993). Users tend to be less concerned when asked for permission to have their information collected and used. (Nowak and Phelps 1995; Smith et al, 2011). Thus, H5 is formed:

H5: As the privacy awareness increases, privacy concern also increases.

2.2. Research design, instrument and scales, sampling method

The purpose of this research is to examine the effect of the effectiveness of the privacy policies of mobile commerce applications on the privacy concerns and sense of trust of users, and therefore on their willingness to share personal information. Based on previous research to determine the impact of the effectiveness of m-commerce privacy policies on the user, the author of the studies used a quantitative research method (Aïmeur et al., 2009; Harris et al., 2016; Tay et al., 2021; Wang et al., 2014 ; Lwin et al., 2007). For this reason, the quantitative research method was chosen by the author of this study in order to conduct an effective research based on previous studies.

The primary data collection tool for this study was chosen as an online questionnaire conducted using the quantitative research method. The author of this study will use an electronic type of online questionnaire. The developed online questionnaire was shared with random participants living in Lithuania using social media platforms and e-mail. The online questionnaire was chosen as the most acceptable alternative for this study because it was planned to collect minimum 146 responses and then analyze the resulting data using the SPSS program.

Research instruments and scales

The main idea of the study is to find out the effect of the effectiveness of M-commerce app privacy policies on the user's willingness to share personal information. Since the research needs to reach definitive results, no specific brand is mentioned in this study. Because users' decisions and behaviors may change depending on the familiar brand they see. A survey in the form of a questionnaire is adopted as a research technique for this study, and it contains a variety of questions.The questionnaire consists of two parts. At the very beginning of the questionnaire, the participant was asked to answer demographic questions and a screening question before proceeding further. As a screening question, participants were asked whether they had a mobile device with internet access. These questions aimed to immediately determine whether the user's answers would be suitable for the purpose of the study. The second part of the research survey consisted of 18 closed-ended questions in order to facilitate the participant's evaluation of the expressions closest to him/her. For this study, questions were evaluated on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The questions were asked sequentially so that the user could fully understand the logic of the survey and the rationale of the research. The first question measures the effectiveness of M-commerce privacy policy in the eyes of users. The four-point structure was adapted from Zhao et al., (2012) and Xu et al., 2011. The second question was adapted as a three-point construct from Pavlou, (2003) and Wu et al., (2012) to measure the user's sense of trust. The third question was designed to evaluate users' privacy concerns. A four-point structure was adapted from Dinev & Hart, (2006) and Anic et al, (2018). The fourth question was prepared to understand the users' extent of privacy awareness. The five-point structure was adapted from Earp & Anton, (2005) and Xu et al., (2011) and Malhotra et al., (2004). The fifth question was prepared to measure users' willingness to share their personal information with the application. Two-point structure adapted from Wu et al, (2012).

Demographic questions	**1. What is your gender?** • Female • Male • Prefer Not to Say
	2. Please, indicate your age in years • 18-24 years old • 25-34 years old • 35-44 years old • 45+ years old

Table 1. *Demographic questions, developed by author*

Screening Question
3. Do you have a mobile device with internet access? • Yes • No

Table 2. *Screening question, developed by author*

Variable	Description	Measurement 5-point Likert type Scale	References
Perceived Effectiveness of Privacy Policy	1. I am confident that this privacy policy of the mobile commerce app genuinely reflect their commitment to safeguarding my personal information. 2. With this privacy policy, I believe that my personal information will be kept private and confidential by mobile commerce app 3. I believe that these mobile commerce applications` privacy policies are an effective way to demonstrate their commitment to privacy 4. The privacy policy provided by the mobile app, clearly and completely describes how users' privacy would be protected and used by it.	1 - Strongly Disagree 2 - Disagree 3 - Neither Agree nor Disagree 4 - Agree 5 - Strongly Agree	(Zhao et al., 2012 and Xu et al., 2011)
Trust	1. The mobile app's privacy policy on how it would use any personal information about me makes me feel that the app is trustworthy. 2. The mobile app's online privacy policy makes me feel that the app is trustworthy. 3. The mobile app's privacy policy concerning the notice of personal information collection makes me feel this app is trustworthy	1 - Strongly Disagree 2 - Disagree 3 - Neither Agree nor Disagree 4 - Agree 5 - Strongly Agree	(Pavlou, 2003; Wu et al.,2012)
Privacy Concern	1. I am concerned about my online privacy 2. I am concerned that the information I shared wıth the mobile app could be misused. 3. I am concerned about sharing personal information to mobile app, because of what others might do with it. 4. I am concerned about sharing my personal information to the mobile app, because it could be used in a way I did not foresee.	1 - Strongly Disagree 2 - Disagree 3 - Neither Agree nor Disagree 4 - Agree 5 - Strongly Agree	(Dinev & Hart, 2006; Anic et al, 2018)

Privacy Awareness	1. I follow the news and developments about privacy issues and privacy violations. 2. I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy. 3. Mobile app service providers seeking personal information should disclose the way the data are collected, processed, and used. 4. It is very important to me that I am aware and knowledgeable about how my personal information will be used. 5. I want a m-commerce app to keep me informed of changes to it's privacy practices.	1 - Strongly Disagree 2 - Disagree 3 - Neither Agree nor Disagree 4 - Agree 5 - Strongly Agree	(Earp & Anton, 2005; Xu et al, 2011; Malhotra et al., 2004)
Willingness to Share Personal Information	1. I am willing to share my personal information with the m-commerce app 2. I feel comfortable sharing my personal information with the m-commerce app	1 - Strongly Disagree 2 - Disagree 3 - Neither Agree nor Disagree 4 - Agree 5 - Strongly Agree	(Wu et al, 2012)

Table 3. *Measurement constructs*

Sampling method

Participants for this study were selected from those who felt comfortable answering the survey in English, were 18 years of age or older, owned a mobile device with internet access, and lived in Lithuania. Therefore, non-probability, convenience sampling method was chosen for the following research.

In order to determine the desired number of participants, the comparable researches technique shown in *Table 1* was used and the sample size was estimated. In this method, previous studies were examined and a table was compiled from the number of participants by finding studies that conducted online questionnaire. An average number was then calculated for the number of participants required for the author's current study. Thus, a minimum sample size of 145,6 participants was reached, based on the number of participants in previous similar studies. Since the number of participants of 145,6 was not possible, this number was rounded to 146. The online questionnaire prepared by the author in English was shared with randomly selected participants living in Lithuania.

No.	Author	Type of questionnaire	Number of respondents
1	Aïmeur et al., (2009)	Online questionnaire	144
2	Harris et al., (2016)	Online questionnaire	128
3	Tay et al., (2021)	Online questionnaire	135
4	Wang et al., (2014)	Online questionnaire	141
5	Lwin et al., (2007)	Online questionnaire	180
Average		**145,6**	

Table 4. *Comparable Researches sampling method*

3. RESULTS OF THE RESEARCH

3.1. Sample Description

In order to conduct the necessary analysis for the research, the participants were asked about their age and gender. Since no further demographic questions were needed for this study, only the necessary demographic information was obtained from the participants. It is worth noting that the final analysis examined only participants from Lithuania. Since the participants were selected from a single country, the survey did not ask which country they participated from as a separate question. As a result, 151 participants living in Lithuania were selected for the study.

Table 3 shows that by gender of the participant, 84 women and 67 men participated in the survey, with an almost equal distribution of 55.6 percent women and 44.4 percent men.

	Frequency	Percent	Valid Percent	Cumulative Percent
Female	84	55,6	55,6	55,6
Male	67	44,4	44,4	100,0
Total	151	100,0	100,0	

Table 5. *Respondents by gender, developed by the author*

Respondents' age is the next demographic factor to consider. Participants were asked to indicate their age according to the groupings provided. According to Table 4, 24.5% of the participants in the survey were in the 18-24 age range, 53% were in the 25-34 age range, 16.6% were in the 35-44 age range and 6% were 45+ years old.

	Frequency	Percent	Valid Percent	Cumulative Percent
18-24 years old	37	24,5	24,5	24,5
25-34 years old	80	53,0	53,0	77,5

35-44 years old	25	16,6	16,6	94,0
45+ years old	9	6,0	6,0	100,0
Total	151	100,0	100,0	

Table 6. *Respondents by age, developed by the author*

Additionally, all participants who answered the survey were asked whether they used a mobile device with internet access. Since all participants responded positively to this question, no participant's data was deleted.

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	151	100,0	100,0	100,0

Table 7. *Mobile device usage of respondents, developed by the author*

3.2. Reliability test of scales

Before starting the analysis, a reliability test was conducted for each scale assessing the constructs to ensure compliance with measurement standards. The researcher identified components with elevated Cronbach's coefficients during measurement, contributing to the evaluation of the questionnaire's reliability. Utilizing the statistical software SPSS, the collected data were processed to assess the reliability of each construct through Cronbach's alpha. The outcomes indicated powerful results, surpassing Cronbach's alpha (α) of 0.6 and demonstrating a high level of satisfaction with the results.

Scales	**Cronbach‘s alpha**
Perceived Effectiveness of Privacy Policy	0,911
Trust	0,916
Privacy Concern	0,922

Privacy Awareness	0,785
Willingness to Share Personal Information	0,866

Table 8. *Cronbach's alpha for research scales, compiled by the author*

3.3. Research of the Perceived Efffectiveness of Privacy Policy on User's Willigness to Share Personal Information Data Analysis and Results

A multiple correlation analysis was used to present differences between independent and dependent variables created in the research model and to confirm or reject the proposed hypotheses. As a result, the evaluation of each hypothesis and sub-hypothesis is presented below.

Decsriptive Analysis of Perceived Effectiveness of Privacy Policy

In the study, the privacy policy of an existing mobile commerce brand, prepared in accordance with the GDPR rules and principles, was chosen as the privacy policy given to the users. As a result of the studies conducted, it was concluded that this privacy policy is suitable for the study. However, users were given a fictitious scenario and mobile application in the survey and were told that this privacy policy belonged to the fictitious application. The purpose here was to prevent the impact of the brand to which the privacy policy belongs on the user's responses. Therefore, it was aimed for users to approach the survey questions more objectively.

In order to analyze the construct of perceived effectiveness of privacy policy the score mean of four items was summed up. When it comes to Question 1 to Question 4 the score emerged from 1 "Strongly Disagree" to 5 "Strongly Agree". As it can be seen on Table 7, the Total Score Mean for the perceived effectiveness of privacy policy construct is 3,6821. According to Zaki & Ahmad (2017), the mean score between 3.50 to 4.29, considered as high. In other words, this score is defined as the privacy policy provided has proven to have a positive impact for participants and its perceived effectiveness is positive.

	N	Mean	Std. Deviation
Question 1	151	3,5828	1,09153
Question 2	151	3,6093	1,12531
Question 3	151	3,6821	1,03519
Question 4	151	3,8543	0,96192
Total	151	3,6821	1,05348

Table 9. *Descriptive Statistics of Perceived Effectiveness of Privacy Policy*

HYPOTHESES:

H1: As the perceived effectiveness of privacy policy increases, trust also increases.

After analyzing previous studies, it has been concluded that the perceived effectiveness of privacy policy has positive influence on trust (Wang et al, 2022; Papova et al, 2012; Balapour et al, 2020; Lauer & Deng, 2007). Therefore, H1 was developed to examine the effect of the perceived effectiveness of the privacy policy on trust. To test H1, correlation analysis was conducted between the perceived effectiveness of the privacy policy and trust constructs. The results of the statistical analysis showed that there is a statistically significant relationship between 2 above-mentioned variables ($p<0.001$), with the strong positive correlation coefficient between them R= 0.735 (see Table 8). Thus, H1 is confirmed.

		Perceived Effectiveness of Privacy Policy	Trust
Perceived Effectiveness of Privacy Policy	Pearson Correlation	1	0,735
	Sig (1-tailed)		< 0,001
	N	151	151
Trust	Pearson Correlation	0,735	1
	Sig (1-tailed)	< 0,001	
	N	151	151

Table 10. *Correlation Analysis of H1, developed by author*

H2: As perceived effectiveness of privacy policy increases, privacy concern decreases.

As stated in the literature, there is a negative relationship between perceived effectiveness of privacy policy and privacy concern, and as the perceived effectiveness of the privacy policy increases, users' privacy concerns decrease (Papova et al, 2012; Milne & Culnan, 2004; Aljukhadar et al., 2010; Bansalet al., 2008; Zhou, 2017). Therefore, H2 was developed to test the effect of the perceived effectiveness of the privacy policy on the user's privacy concern. H2 was analyzed using correlation analysis between perceived effectiveness of privacy policy and privacy concern. The results of the analysis demonstrate that there is a statistically significant relationship between 2 above-mentioned variables (p<0.001), with a moderate negative correlation coefficient between them R= -0,312 (see Table 9). Thus, H2 is confirmed.

		Perceived Effectiveness of Privacy Policy	Privacy Concern
Perceived Effectiveness of Privacy Policy	Pearson Correlation	1	-0,312
	Sig (1-tailed)		< 0,001
	N	151	151
Privacy Concern	Pearson Correlation	-0,312	1
	Sig (1-tailed)	< 0,001	
	N	151	151

Table 11. *Correlation Analysis of H2, developed by author*

H3: As the trust increases, the willingness to share personal information also increases.

As in the previous hypotheses, the correlation analysis method was used to analyze the H3 hypothesis. As stated in the literature, trust has an impact on users' willingness to share personal information, and research argues that as users' sense of trust increases, their willingness to share personal information increases (Dinev and Hart, 2006; Popova et al, 2012; Castañeda & Montoro, 2007). Therefore, H3 was developed to test the effect of trust on the willingness to share personal information. Correlation analysis was used to test the accuracy of H3. The results of the analysis demonstrate that there is a statistically significant relationship between 2 above-mentioned variables (p<0.001), with a moderate positive correlation coefficient between them R= 0.516 (see Table 10). Thus, H3 is confirmed.

		Trust	Willingness to Share Personal Information
Trust	Pearson Correlation	1	0,516
	Sig (1-tailed)		< 0,001
	N	151	151
Willingness to Share Personal Information	Pearson Correlation	0,516	1
	Sig (1-tailed)	< 0,001	
	N	151	151

Table 12. *Correlation Analysis of H3, developed by author*

H4: As the privacy concern increases, the willingness to share personal information decreases.

Correlation analysis method was used to analyze the H4 hypothesis, which is another hypothesis of the study. Previous studies have mentioned that users avoid sharing their personal information due to privacy concerns, and therefore there is a negative relationship between privacy concerns and willingness to share personal information (Min and Kim, 2015; Kehr et al, 2015; Anic et al, 2018; Popova et al, 2012; Mothersbaugh et al, 2012). Based on previous studies, H4 was developed to test the relationship between privacy concern and willingness to share personal information. Correlation analysis was used to test the accuracy of H4. The results of the analysis shows that there is a statistically significant relationship between privacy concern and willingness to share personal information (p<0.001), with a moderate negative correlation coefficient between them R= -0,406 (see Table 11). Thus, H4 is confirmed.

		Privacy Concern	Willingness to Share Personal Information
Privacy Concern	Pearson Correlation	1	-0,406
	Sig (1-tailed)		< 0,001
	N	151	151
Willingness to Share Personal Information	Pearson Correlation	-0,406	1
	Sig (1-tailed)	< 0,001	
	N	151	151

Table 13. *Correlation Analysis of H4, developed by author*

H5: As the privacy awareness increases, privacy concern also increases.

Lastly, the correlation analysis method was used to analyze the H5 hypothesis, which is the final hypothesis of the study. As mentioned in the literature section of the research, previous studies have concluded that users with higher privacy awareness have higher privacy concerns (Malhotra et al. 2004; Phelps et al. 2000; Cespedes and Smith 1993; Nowak and Phelps 1995; Smith et al, 2011). A correlation analysis was performed to evaluate the accuracy of this hypothesis. The results revealed a statistically significant positive relationship between privacy awareness and privacy concern (p<0.001), with a moderate positive correlation coefficient of 0.318 (refer to Table 12). Therefore, H5 is supported by the findings, indicating that higher levels of privacy awareness are associated with increased privacy concerns among users. Thus, H5 is confirmed.

		Privacy Awareness	Privacy Concern
Privacy Awareness	Pearson Correlation	1	0,318
	Sig (1-tailed)		< 0,001
	N	151	151

Privacy Concern	Pearson Correlation	0,318	1
	Sig (1-tailed)	< 0,001	
	N	151	151

Table 14. *Correlation Analysis of H5, developed by author*

3.4. Summary of statistical analysis

In the current research 5 hypotheses were derived, with the intention to analyze the impact of perceived effectiveness of privacy policies to users willingness to share personal informations. Table 13 below represents and summarizes the results of the derived hypotheses.

Hypotheses	**Results**
H1: As the perceived effectiveness of privacy policy increases, trust also increases.	Confirmed
H2: As perceived effectiveness of privacy policy increases, privacy concern decreases.	Confirmed
H3: As the trust increases, the willingness to share personal information also increases.	Confirmed
H4: As the privacy concern increases, the willingness to share personal information decreases.	Confirmed
H5: As the privacy awareness increases, privacy concern also increases.	Confirmed

Table 15. *Status of hypotheses*

Performed statistical analysis showed that:

The purpose of the research was to determine the impact of the perceived effectiveness of the privacy policy on users' willingness to share their personal information. The author also included the factors of trust, privacy concern and privacy awareness in this study and took their effects into consideration. After empirical examination, it was discovered that all five of the five hypotheses were supported. Table 15 shows the status of the hypotheses as a result of the research.

The positive effect of the perceived effectiveness of the privacy policy on user trust was analyzed under hypothesis H1. By analyzing the data obtained as a result of the survey research, it was found that the privacy policy is effective on users. Therefore, the findings regarding the perceived effectiveness of privacy policies and it’s positive impact on trust align with previous research (Wang & Wang, 2021; Xu et al, 2011; Lauer & Deng, 2007). As a result of the H1 hypothesis, it was seen that the perceived effectiveness of the privacy policy had a positive effect on trust, and if the perceived effectiveness increased, trust also increased, and H1 was approved.

Hypothesis H2 focuses on the relationship between the perceived effectiveness of privacy policies and users' privacy concerns. According to the H2 hypothesis, there is an inverse relationship between the two variables and it is assumed that privacy concern decreases in case of the perceived effectiveness of the privacy policy. As a result of the analysis of the data obtained from the survey research, it was proven that the H2 hypothesis was confirmed. As mentioned in previous studies (Milne & Culnan, 2004; Aljukhadar et al., 2010; Bansalet al., 2008; Papova et al, 2012), there is a negative relationship between the perceived effectiveness of the privacy policy and the user's privacy concern. Therefore, it is very important and necessary for service providers to offer well-prepared privacy policies to users in order to reduce their concerns.

Another hypothesis of the research, H3 hypothesis, argues that trust and willingness to share personal information are directly proportional and as one increases, the other will also increase. As mentioned in previous studies, the risk perceived by users is higher in the online environment. Accordingly, as user trust increases, perceived risk decreases and willingness to share personal information is positively affected (Zimmer et al, 2010; Popova et al, 2012; Castañeda & Montoro, 2007). As a result of the survey conducted by the author with Lithuanian participants, the accuracy of the H3 hypothesis was proven. As a result, service providers need to establish a sense of trust with users in order to collect the personal information they want users to share.

The fourth hypothesis of the study, H4, focuses on the impact of users' privacy concerns on their willingness to share personal information. After the analysis of the two variables, the analysis results show that there is an inverse relationship between the variables. Therefore, as privacy concern increases, the willingness to share personal information decreases and H4 is confirmed. The results of the study are compatible with the results of previous research. When users do not know how and for what purpose their personal information will be used, with whom and for how long it will be shared, they feel privacy concerns and do not want to share their personal data (Anic et al, 2018; Popova et al, 2012; Mothersbaugh et al, 2012).

The fifth and final hypothesis, H5, is based on the relationship between users' privacy awareness and privacy concern. According to H5, as users' privacy awareness increases, their privacy concerns also increase and a direct proportion is observed between the two variables. Based on this, H5 was confirmed as a result of the research and data analysis. The results of the study are consistent with previous research. As users' level of knowledge about privacy agreements and practices increases, their concerns also increase. Because as users become more aware of the possibility of personal data being stolen, shared without permission, or leaked, they become more concerned about sharing their data (Malhotra et al. 2004; Phelps et al. 2000; Cespedes and Smith 1993).

In general, the study aimed to investigate the impact of the perceived effectiveness of privacy policies on users' willingness to share personal information, incorporating factors like trust, privacy concern, and privacy awareness. Analyzing the collected data supported all five hypotheses. These findings shows the crucial role of effective privacy policies in fostering trust, mitigating privacy concerns, and influencing users' willingness to share personal information in the mobile commerce.

4.CONCLUSIONS, SUGGESTIONS AND PRACTICAL IMPLICATIONS OF THE STUDY BASED ON THE ANALYSIS OF RESEARCHED FACTORS

With digitalization, the concept of data privacy entered our lives and, accordingly, the concept of user privacy gained importance. Data privacy can have positive or negative effects on users. For example, a negative impact of data privacy is that users are likely to have privacy concerns and therefore hesitate to share their data. On the other hand, the positive effects of data privacy may be that users know how their data will be protected, stored and used, and therefore they can trust the service they will use and be more likely to share their personal data easily.

Privacy policies alone generally do not have a direct impact on a user's willingness to share personal information. Along with the privacy policy itself, the concepts of trust and privacy concern and the user's level of privacy awareness are factors that play a role in the user's willingness to share personal information. As mentioned above, one of the tasks of the current research is to explore how the perceived effectiveness of the privacy policy affects the user's willingness to share personal information in line with the trust or concern it creates in the user.

The findings show that the perceived effectiveness of the privacy policy has an impact on users' sense of trust and privacy concerns. The mobile commerce app privacy policy given to participants was a privacy policy prepared in accordance with the GDPR principles and rules. The survey research results showed that the participants confirmed the effectiveness of the given privacy policy. Participants' opinions on whether and how well the given privacy policy adequately protects their personal information reflect the perceived effectiveness of the privacy policy. Therefore, it was concluded that the privacy policy given to the participants was an effective privacy policy.

After measuring the perceived effectiveness of the privacy policy, its impact on user trust and privacy concern was examined in the next stage. As a result of the current research, many important findings were obtained. Firstly, it was concluded that when users perceive the privacy policy as effective, their sense of trust increases. The results of the rersearch suggests that trust increases as the perceived effectiveness of the privacy policy increases, were found to be consistent and statistically significant. Analysis of survey data revealed a positive relationship between the perceived effectiveness of the privacy policy and participants' level of trust. This means that participants who perceive the privacy policy as more effective tend to have higher levels of trust in the service provider. The finding emphasizing the importance of well-crafted and transparent privacy policies in fostering user trust. Consequently, increasing the perceived effectiveness of privacy policies can contribute to building and strengthening user trust towards online platforms or services. As service providers and companies aim to build and maintain positive and trustful user relationships, serving effective privacy policies emerges as a key determinant in fostering a trusting user base.

Next important result revealed was the reversed relationship between the perceived effectiveness of privacy policies and users' privacy concerns. The statistical analysis of survey responses showed significant negative correlation, indicating that an increase in the perceived effectiveness of the privacy policy is associated with a parallel decrease in users' privacy concerns. Studies support the idea that well-crafted and transparent privacy policies play a crucial role in alleviating users' concerns about privacy issues. The underlying hidden meaning is that users are more inclined to engage with online/mobile platforms and share personal information when they are assured of the efficacy and transparency of the privacy policies. The results shows the strategic importance for service providers to invest in privacy policies that not only comply with legal standards but also serve as effective communication tools. By doing so, businesses can built a sense of trust among users, alleviate their concerns about privacy matters and thereby promoting a more positive and constructive user-provider relationship in the digital landscape. This result further underscores the importance of addressing privacy concerns through effective privacy policies, emphasizing their crucial role in shaping user perceptions and interactions in online.

Another important part of the research is to investigate the fundamental interaction between user trust and willingness to share personal information. The positive relationship revealed in the analysis as a result of the research shows that as users' trust in the digital platform increases, their desire to share personal information also increases. This alignment between trust and information sharing behavior is consistent with previous researches that emphasize the importance of trust in online transactions and interactions. The research results underline the important role of trust plays in shaping user attitudes towards sharing personal data. When users have a higher level of trust to the service provider, they tend to be more open and willing to share information. For mobile businesses and service providers, this result highlights the strategic importance of developing and maintaining trust. By doing this, they are not only improve the user experience, but also create an environment where users are more likely to provide personal information. This finding is particularly relevant in the context of e-commerce, m-commerce, and online services, highlighting the need for companies to prioritize trust-building initiatives to encourage positive user behaviors regarding information sharing.

In the next step of the research, the interaction between users' privacy concerns and their willingness to share personal information was examined. A detailed analysis of the study found a negative correlation between privacy concerns and willingness to share personal information. As privacy concerns increase, users are noticeably unwilling to share personal information. Concerns such as potential misuse of users' personal data, fear of unauthorized access and unauthorized sharing create visible tension in the digital space for users. Acknowledging and making improvements to reduce these concerns is of great importance for businesses and service providers which is aiming to increase trust and user participation.

In the last step of the research, the relationship and impact between users' privacy awareness and privacy concerns were examined. The analysis concluded that as users' awareness of privacy issues increases, the depth of their concerns about privacy issues also increases. The conclusion is perfectly in line with previous research, which highlights that awareness of potential risks associated with personal data, including concerns about unauthorized sharing or potential data breaches, tends to increase users' general concerns. As users become more aware of privacy practices, the responsibility falls on businesses and service providers to develop transparent and informative communication between them and the user. It is a critical role for businesses to create strategies that not only address concerns but also actively contribute to increasing user awareness.

After conducting the research which has successfully analyzed the perceived effectiveness of privacy policies and its impact on users' behavior in the digital space, the recommendations could be suggested:

1. The fact that users who are confident about effectiveness of the policy are more willing to share personal information further emphasizes the strategic importance of privacy policies. This emphasize the need for businesses to view privacy policies not only as legal requirements but also as tools for effective communication and trust-building.
2. This comprehensive research on privacy perceptions provides valuable information for businesses in the digital environment.
3. The findings emphasize the strategic importance of effective privacy policies, transparent communication, and trust-building initiatives in fostering positive user behavior and relationships in the digital environment.

Limitations of the study and areas of future research

One of the main limitations of the research was that the survey given to users could not measure whether users actually read the privacy policy and made an accurate and detailed evaluation. Because the research was conducted as an online survey and shared with users through online channels. A more accurate analysis would be to conduct research with fewer participants in the next study, give participants a confidentiality agreement in a physical environment, and have them answer the survey questions by making sure they have read and evaluated them correctly. In this way, more detailed and accurate answers can be obtained from users. On the other hand, in the next study, providing users with more than one privacy policy prepared under the consultancy of legal experts will provide a more detailed and accurate analysis. Since the author did not receive advice from any legal expert and is not a legal expert, it was not possible to prepare a new privacy policy. Therefore, the privacy policy of an existing m-commerce brand, prepared in accordance with GDPR principles, was used. In the next study, preparing different privacy policies with the help of legal experts and sharing them with the participants will provide a more detailed and accurate analysis for the research. Additionally, in future studies, investigating how elements such as privacy policy presentation formats and contents affect perceptions and trust will provide a different and broader perspective to the research.

Additionally, the study focused only on participants from Lithuania. Cultural factors may influence perceptions of privacy and trust. Repeating the study in different cultural contexts or making cross-cultural comparisons can provide a more detailed understanding of the impact of cultural variables. Conducting cross-country studies to compare privacy perceptions and behaviors across different countries and legal frameworks can provide insight into the role of cultural and legal contexts in shaping user expectations.

THE PERCEIVED EFFECTIVENESS OF M-COMMERCE APP PRIVACY POLICIES ON USER WILLINGNESS TO SHARE PERSONAL INFORMATION

VILNIUS UNIVERSITY BUSINESS SCHOOL

Study programme: Digital Marketing

Emine Ozmen

Supervisor Lecturer Gintarė Gulevičiūtė

SUMMARY

Thesis completed – 2024, Vilnius

Paper volume – 52 pages

Number of tables – 15

Number of figures – 2

Number of literature references – 119

With the introduction of digitalization and information technologies into our lives, businesses continued to develop their services online. With the transition to the online environment, consumers began to purchase services through online services, and this caused the concept of data privacy to come to the fore. As consumers shopped online, they had to share different personal data with service providers. With data privacy coming to the fore, governments have introduced laws and regulations to protect data privacy, and privacy policies have entered our lives. The purpose of privacy policies was to legally protect the rights of users and service providers. However, it has been observed that the perceived effectiveness of privacy policies can have different effects on the user. Therefore, it has been observed that privacy policies play an important role in creating a sense of trust in the user and reducing privacy concerns, and have a great impact on users' willingness to share their personal information. Therefore, the author's aim is to analyze the impact of the perceived effectiveness of the privacy

policy on users' willingness to share their personal information while considering the factors of trust, privacy concern and privacy awareness for the respondents from Lithuania.

In order to achieve the purpose of the research and evaluate the hypotheses, data was collected using the survey method, correlation analysis was made using the SPSS program and the hypotheses were tested. Lithuanian users' attitudes towards privacy policy, willingness to share personal data, levels of trust, privacy concerns and privacy awareness were measured with different survey questions, and by analyzing the results, all five hypotheses developed were confirmed.

The findings of the survey show that the perceived effectiveness of the privacy policy has a significant impact on the user's willingness to share personal data. In addition, the author added a different dimension to the research and contributed to the literature by addressing the factors of trust, privacy concern and privacy awareness at the stage of users' willingness to share their personal data. As a result, for Lithuanian users, the perceived effectiveness of the privacy policy appeared to increase the sense of trust and reduce privacy concern. On the other hand, it has been concluded that the privacy concerns of users with high awareness and knowledge about privacy also increase, and as a result, their willingness to share personal information decreases. To summarize, the current research is helpful to both the academic and business communities in terms of m-commerce companies and service providers.

SUVOKIAMO M-KOMERCIJOS PROGRAMĖLIŲ PRIVATUMO POLITIKOS VEIKSMINGUMAS NAUDOTOJŲ NORUI DALYTIS ASMENINE INFORMACIJA

VILNIAUS UNIVERSITETAS VERSLO MOKYKLA

Studijų programa: Skaitmeninė rinkodara

Emine Ozmen

Supervisor Lektorė Gintarė Gulevičiūtė

SANTRAUKA

Darbas parengtas – 2024 m., Vilnius

Darbo apimtis – 52 puslapių

Lentelių skaičius – 15

Figūrėlių skaičius – 2

Literatūros ir šaltinių skaičius – 119

Mūsų gyvenima įsigalėjus skaitmenizacijai ir informacinėms technologijoms, įmonės toliau plėtojo savo paslaugas internetu. Perėjus prie internetinės aplinkos, vartotojai pradėjo aktyviai naudotis internetine prekyba, todėl duomenų privatumo samprata išryškėjo. Pirkdami internetu vartotojai turėjo dalytis skirtingais asmeniniais duomenimis su paslaugų teikėjais. Išryškėjus duomenų privatumui, vyriausybės priėmė įstatymus ir kitus teisės aktus, skirtus apsaugoti duomenų privatumą, o privatumo politika įžengė į mūsų gyvenimą. Privatumo politikos tikslas buvo teisiškai apsaugoti vartotojų ir paslaugų teikėjų teises. Tačiau pastebėta, kad suvokiamas privatumo politikos efektyvumas gali turėti skirtingą poveikį vartotojui. Todėl pastebėta, kad privatumo politika vaidina svarbų vaidmenį kuriant pasitikėjimo jausmą ir mažinant susirūpinimą dėl privatumo bei darant didelę įtaką vartotojų norui dalytis savo asmenine informacija. Todėl šio darbo tikslas – išanalizuoti suvokto privatumo politikos efektyvumo įtaką vartotojų norui dalytis savo asmenine informacija, įvertinant respondentų iš Lietuvos pasitikėjimo, susirūpinimo privatumu ir privatumo suvokimo veiksnius.

Norint pasiekti tyrimo tikslą ir įvertinti hipotezes, apklausos metodu buvo renkami duomenys, SPSS programa atlikta koreliacinė analizė ir hipotezės patikrintos. Lietuvos vartotojų požiūris į privatumo politiką, noras dalytis asmens duomenimis, pasitikėjimo lygis, susirūpinimas dėl privatumo ir privatumo suvokimas buvo matuojamas skirtingais tyrimo klausimais, o analizuojant rezultatus pasitvirtino visos penkios iškeltos hipotezės.

Apklausos išvados rodo, kad suvokiamas privatumo politikos efektyvumas turi didelę įtaką vartotojo norui dalytis asmeniniais duomenimis. Be to, autorius papildė tyrimą kitokiu aspektu ir prisidėjo prie literatūros, nagrinėdamas pasitikėjimo, susirūpinimo privatumu ir privatumo suvokimo veiksnius vartotojų noro dalintis savo asmens duomenimis etape. Dėl to Lietuvos vartotojams atrodė, kad privatumo politikos efektyvumas padidino pasitikėjimo jausmą ir sumažino susirūpinimą dėl privatumo. Kita vertus, prieita prie išvados, kad taip pat daugėja vartotojų, turinčių didelį sąmoningumą ir žinias apie privatumą, susirūpinimas dėl privatumo didėja, todėl mažėja jų noras dalytis asmenine informacija. Apibendrinant, atliktas tyrimas yra naudingas tiek akademinei, tiek verslo bendruomenei, kalbant apie m-komercijos įmones ir paslaugų teikėjus.

LIST OF REFERENCES

1. Aalst, W, (2016). Process Mining: Data Science in Action. Springer.
2. Acquisti, A., Friedman, A., Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study. In ICIS 2006 Proceedings (Paper 94).
3. Aïmeur, E., Gambs, S., Ho, A. (2009). UPP: User Privacy Policy for Social Networking Sites. Fourth International Conference on Internet and Web Applications and Services. Doi: 10.1109/ICIW.2009.45
4. Aljukhadar, M., Senecal, S., Ouellette, D., Montreal, H. and Abdelmoety, Z.H.S. (2010). Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environment. International Journal of Electronic Commerce. 14(4). pp. 103-126.
5. Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., Agarwal, Y. (2015). Your location has been shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In Proceedings of the 33rd annual ACM conference on human factors in computing systems. CHI '15 pp.787–796. doi: 10.1145/2702123.2702210
6. Al-Jabri, I., Eid, M., Abed, A. (2019). The willingness to disclose personal information. Trade-off between privacy concerns and benefits. Information & Computer Security. 28(2). pp. 161-181
7. Anic, I., Budak, J., Rajh, E., Recher, V., Skare, V., Skrinjaric, B., (2018). Extended model of online privacy concern: what drives consumers' decisions?. Online Information Review. pp.799-817.
8. Anton, A. I., Earp, J.B., He, Q., Stufflebeam, W., Bolchini, D., Jensen, C., (2004). Financial Privacy Policies and the Need for Standardization. IEEE Security and
   - Privacy Magazine. doi: 10.1109/MSECP.2004.1281243
9. Aydin, A., Piorkowski, D., Tripp, O., Ferrara, P., Pistoia, M., (2017). Visual configuration of mobile privacy policies. In R. Huisman (Ed.), Fundamental approaches to software engineering. pp. 338–355
10. 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. doi: 10.1016/j.ijinfomgt.2019.102063
11. Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., Cranor, L. (2015). The impact of timing on the salience of Smartphone App Privacy Notices. In Proceedings of the 5th

annual ACM CCS workshop on security and privacy in Smartphones and mobile devices. SPSM ’15 pp. 63–74

12. Bansal, G., Zahedi, F.M. and Gefen, D. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: a multiple-context investigation. Paper Presented at the International Conference on Information Systems (ICIS), Paris, pp. 1-19
13. BBC. (2015). Ashley Madison infidelity site's customer data 'leaked'. [online] Retrieved July 10, 2023, from http://www.bbc.com/news/business-33984017.
14. Berendt, B., Günther, O., Spiekermann, S. (2005). Privacy in E-commerce: Stated preferences vs. actual behavior. Communications of the ACM, 48(4), pp. 101–106.
15. Betzing, J. H., Tietz, M., Brocke, J., Becker, J., (2019). The impact of transparency on mobile privacy decision making. Electronic Markets. pp. 607-625, doi: 10.1007/s12525-019-00332-3
16. Brandtzaeg, P. B., Pultier, A., Moen, G. M. (2018). Losing Control to Data-Hungry Apps: A Mixed-Methods Approach to Mobile App Privacy. Social Science Computer Review. 37(4). doi: 10.1177/0894439318777706
17. Castañeda, J., Montoro, F. (2007). The effect of Internet general privacy concern on customer behavior. Electron Commerce Res. doi: 10.1007/s10660-007-9000-y
18. Cespedes, F. V., and Smith, H. J. 1993. Database Marketing: New Rules for Policy and Practice. Sloan Management Review. 34(4)
19. Chiang, C. F., Jang, S., Canter, D., Prince, B. (2008). An expectancy theory model for hotel employee motivation: Examining the moderating role of communication satisfaction. International Journal of Hospitality & Tourism Administration. 9(4). pp. 327–351
20. Chin, G.A., 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. pp. 49-59
21. Cleff, E. (2007). Privacy Issues in Mobile Advertising. International Review of Law, Computers & Technology. 21(3). pp. 225-236
22. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of. Information Technolog MIS Quarterly. 13(3). pp. 319–340
23. Degirmenci, K. (2020). Mobile users’ information privacy concerns and the role of app permission requests. International Journal of Information Management. pp:261-272. doi: 10.1016/j.ijinfomgt.2019.05.010

24. Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research. 17(1), pp. 61-80.
    - doi: 10.1287/isre.1060.0080
25. Earp, J., & Baumer, D. (2001). Innovative web use to learn about consumer behavior and online privacy. Communications of the ACM, 46(4), 81–83.
26. Eastin, M.S., Brinson, N.H., Doorey, A., Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. Computers in Human Behavior. pp. 214-220. doi: 10.1016/j.chb.2015.12.050
27. Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS: Detecting privacy leaks in iOS applications. In Proceedings of NDSS (pp. 177-183).
28. Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P., & Sheth, A. N. (2010). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (pp. 393-408).
29. Esayas, S. Y. (2017). The idea of “emergent properties” in data privacy: Towards a holistic approach. International Journal of Law and Information Technology, 25, pp.139–178.
30. Farnden, J., Martini, B., Choo, K. K. R. (2015). Privacy risks in mobile dating apps. Twenty First Americas Conference on Information Systems. arXiv:1505.02906.
31. Fife, E., Orjuela, J. (2012). The privacy calculus: mobile apps and user perceptions of privacy and security, International Journal of Engineering Business Management. pp. 1-10
32. GDPR EU. (2016). A Guide to GDPR Data Privacy Requirements. [online] Retrieved July 10, 2023, from https://gdpr.eu/data-privacy/?cn-reloaded=1
33. General Data Protection Regulation, Article 4. 2016 (April 27). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. [online] Retrieved July 5, 2023. from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1489-1-1
34. Gimpel, H., Kleindienst, D., Nüske, N., Rau, D., Schmied, F., (2018). The upside of data privacy – delighting customers by implementing data privacy measures. Electronic Markets. pp. 437–452, doi: 10.1007/s12525-018-0296-3
35. Ginosar, A. and Ariel, Y. (2017). An analytical framework for online privacy research: what is missing?. Information & Management. 54(7). pp. 948-957.

36. Gurau, C. and Ranchhod, A. (2009). Consumer privacy issues in mobile commerce: a comparative study of British, French and Romanian consumers. Journal of Consumer Marketing. pp.496-507

37. Harris, M. A., Brookshire, R., Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. International Journal of Information Management, 36(3), pp. 441–450. doi: 10.1016/j.ijinfomgt.2016.02.004

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

39. Isley, Steven C. (2015). A Data Transparency Framework for Mobile Applications. The RAND Corporation. pp.1-5. doi: 10.48550/arXiv.1501.00335

40. Jensen, C., Potts, C., (2004). Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notice. College of Computing The Georgia Institute of
    - o Technology Atlanta. 6(1), pp. 471-477

41. Jupiter Research. "Security and Privacy Data." FTC Security Workshop. May 20, 2002

42. Jurevičiūtė, E. (2011). Key Factor Affecting Consumers' Intention to Use Mobile Commerce in Lithuania. ISM UNIVERSITY OF MANAGEMENT AND ECONOMICS. Master Thesis

43. Jost, J. T., Banaji, M. R. (1994). The role of stereotyping in system justification and the production of false consciousness. British Journal of Social Psychology. 33(1). pp. 1–27

44. Kay, A. C., Gaucher, D., Napier, J. L., Callan, M. J., Laurin, K. (2008). God and the government: Testing a compensatory control mechanism for the support of external systems. Journal of Personality and Social Psychology, 95(1). pp. 18–35

45. Kiatkawsin, K., Han, H. (2017). Young travelers' intention to behave pro-environmentally: Merging the value-belief-norm theory and the expectancy theory. Tourism Management, 59, pp. 76–88

46. Kim, Y.J., Han, J. (2014). Why smartphone advertising attracts customers: A model of Web advertising, flow, and personalization. Computers in Human Behavior. doi: 10.1016/j.chb.2014.01.015

47. Kim, S., & Yoon, D. (2013). Antecedents of mobile app usage among smartphone users. In American Academy of Advertising Conference Proceedings pp. 72–83

48. Khalifa, M., N Cheng, S.K., Ning Shen, K., (2012), Adoption of mobile commerce: a confidence model. The University of Wollongong in Dubai (UOWD). pp. 14-22.

49. Lauer, T., Deng, X. (2007). Building online trust through privacy practices.International Journal of Information Security. pp. 323-331. doi: 10.1007/s10207-007-0028-8

50. Levenson, H. (2016). 7 common reasons users are abandoning your app. . [online] Retrieved July 10, 2023, from Web Analytics World https://www.webanalyticsworld.net/2016/08/why-users-are-abandoning-your-mobile-app.html

51. 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), 434–445. doi:10.1016/j.dss.2011.01.017.

52. Li, Y. (2011). Empirical studies on online information privacy concerns: literature review and an integrative framework. Communications of the Association for Information Systems. pp. 453-496

53. Liu, C., Marchewka, J., & Ku, C. (2004). American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce. Journal of Global Information Management. 12(1). pp.18–40

54. Liu, F., Wilson, S., Story, P., Zimmeck, S., Sadeh, N. (2018). Towards Automatic Classification of Privacy Policy Text. School of Computer Science. Carnegie Mellon University.

55. Lim, S. L., Bentley, P. J., Kanakam, N., Ishikawa, F., Honiden, S. (2015). Investigating country differences in mobile app user behavior and challenges for software engineering. IEEE Transactions on Software Engineering. pp. 40–64.

56. Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J.I., Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile App privacy through Crowdsourcing. In Proceedings of the 2012 ACM conference on ubiquitous computing. UbiComp '12 pp. 501–510. doi: 10.1145/2370216.2370290

57. Lowry, P. B., Cao, J., Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. Journal of Management Information Systems, 27(4), 163–200. doi:10.2753/mis0742-1222270406.

58. Lyon, D. (2001). Facing the future: Seeking ethics for everyday surveillance. Ethics and Information Technology. pp. 171-181

59. Lwin, M., Wirtz, J. and Williams, J.D. (2007). Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. Journal of the Academy of Marketing Science. 35(4). pp. 572-585

60. Malhotra, N., Kim, S., Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research, 15(4), pp. 336-355.

61. Masclet, D., Pénard, T. (2012). Do reputation feedback systems really improve trust among anonymous traders? An experimental study. Applied Economics, 44(35), pp.4553–4573

62. McDonald, A.M., Cranor, L.F. (2008). The cost of reading privacy policies. Journal of Law and Policy for the Information Society, 4(3), pp. 543–568

63. Michael, A., Salter, B. (2006). Mobile Marketing: Achieving Competitive Advantage Through Wireless Technology.

64. Mildebrath, H., (2023). Understanding EU Data Protection Policy. European Parliamentary Research Service. pp. 1-12.

65. Milne, G., & Boza, M. (2000). Trust and concern in consumers' perceptions of marketing information management practices. Journal of Direct Marketing, 13(1), pp. 5–24. (13,p891)

66. Milne, G., & Culnan, M. (2004). Strategies for reducing online privacy risks: Why consumers read (or Don't Read) online privacy notices. Journal of Interactive marketing, 18(3), pp.15–29

67. Min, J. and Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. Journal of the Association for Information Science and Technology. 66(4) pp. 839-857.

68. Miyazaki, A.D. and Krishnamurthy, S. (2002). "Internet seals of approval: effects on online privacy policies and consumer perceptions". The Journal of Consumer Affairs. 36(1), pp. 28-49.

69. Mothersbaugh, D., Foxx, W., Beatty, S., Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. Journal of Service Research. 15(1). pp. 76-98

70. Mutimukwe, C., Kolkowska, E. and Grönlund, A. (2020), Information privacy in e-service: effect of organizational privacy assurances on individual privacy concerns,

perceptions, trust and selfdisclosure behavior. Government Information Quarterly. 37(1)

71. Nowak, G. J., and Phelps, J. 1995. Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters. Journal of Direct Marketing. 9(3), pp. 46-60

72. Official Gazette, (2021), https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf (Accessedi: 18.07.2021).
https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.html

73. Okazaki, S., Li, H., Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. Journal of Advertising, 38(4), pp.63-77.

74. Olurin, M., Adams, C., Logrippo, L., (2012). Platform for Privacy Preferences (P3P): Current Status and Future Directions. IEEE, doi: 10.1109/PST.2012.6297943

75. OpenAI. (2023). ChatGPT (December). 3.5 version. [The great model of speech]. https://chat.openai.com/chat

76. Sullivan, B. (2015). Hackers target Starbucks gift cardholders. CNBC. [online] Retrieved July 10, 2023. From https://www.cnbc.com/2015/05/13/hackers-target-starbucks-gift-cardholders.html

77. Panko, R., 2018, (March 15). Mobile App Usage Statistics 2018. The Manifest. [online] Retrieved May 23, 2023, from https://themanifest.com/app-development/blog/mobile-app-usage-statistics

78. Peterson, D., Meinert, D., Criswell II, J., Crossland, M., (2007). Consumer trust: privacy policiesand third-party seals. Journal of Small Business and Enterprise Development. 14(4), pp. 654-669.

79. Phelps, J. E., D’Souza, G., Nowak G. J., (2001). Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation. Journal of Interactive Marketing. 15(4), pp. 1-16.

80. Phelps, J., Nowak, G., Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing, 19(1), pp.27–41.

81. Preibusch, S., Kübler, D., Beresford, A. R. (2013). Price versus privacy: An experiment into the competitive advantage of collecting less personal information. Electronic Commerce Research. 13(4). pp. 423–455.

82. Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. International Journal of Human-Computer Studies. 71(12). pp.1133–1143.

83. Renko, M., Kroeck, K. G., Bullough, A. (2012). Expectancy theory and nascent entrepreneurship. Small Business Economics, 39(3). pp. 667–684.

84. Smith, H. J., Milberg, S., Burke, S. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly, 20(2), pp.167-196.

85. Smith, H.J., Dinev, T. and Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly. 35(4). pp. 989-1016.

86. Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F. (2015). A design space for effective privacy notices. In Proceedings of the 11th symposium on usable privacy and security. SOUPS '15.

87. Shah, M. H., Peikari, H. R., Yasin, N. M. (2014). The determinants of individuals' perceived e-security: Evidence from Malaysia. International Journal of Information Management, 34(1), pp. 48–57. doi: 10.1016/j.ijinfomgt.2013.10.001

88. Sheehan, K.B., & Hoy, M.G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. Journal of Advertising, 28(3), pp.37– 52.

89. SNIA, (2023). What is Data Privacy?. [online] Retrieved July 5, 2023, from https://www.snia.org/education/what-is-data-privacy#_ftnref1

90. Statista. (2023). Number of Mobile App Downloads Worldwide. [online] Retrieved May 23, 2023, from https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

91. Statista. (2023). Number of Smartphone Users Worldwide. [online] Retrieved May 23, 2023, from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

92. Statista. (2023). Mobile commerce share of total digital commerce spending in the United States from 4th quarter 2017 to 4th quarter 2022. [online] Retrieved July 20, 2023, from https://www.statista.com/statistics/252621/share-of-us-retail-e-commerce-dollars-spent-via-mobile-device/

93. Steinfield C., (2004). The development of location based services in mobile commerce. Physica Verlag Heidelberg. pp. 177-197

94. Shepherd, S., Kay, A. C. (2012). On the perpetuation of ignorance: System dependence, system justification, and the motivated avoidance of sociopolitical information. Journal of Personality and Social Psychology, 102(2). pp. 264–280

95. Tanner, A. (2013). Here Are Some of America's Most Privacy Friendly Companies. [online] Retrieved June 10, 2023, from http://www.forbes.com/sites/adamtanner/2013/09/11/here-are-some-of-americas-most-privacy-friendly-companies/

96. Tay, S.W., Teh, P.S., Payne, S.J. (2021). Reasoning about privacy in mobile application install decisions: Risk perception and framing. International Journal of Human-Computer Studies. https://doi.org/10.1016/j.ijhcs.2020.102517

97. The Guardian. (2011). iPhone keeps record of everywhere you go. [online] Retrieved June 10, 2023, from https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears.

98. The Telegraph. (2010). Facebook admits 'inadvertent' privacy breach. [online] Retrieved June 10, 2023, from http://www.telegraph.co.uk/technology/facebook/8070513/Facebook-admits-inadvertent-privacy-breach.html.

99. 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), pp.254–268

100. Tiwari, R., Buse, S and Herstatt, C. (2006). From electronic to mobile commerce. Institute of Technology and Innovation Management Hamburg University of Technology.

101. Vasileiadis, A. (2013). SECURITY CONCERNS AND TRUST IN THE ADOPTION OF M-COMMERCE. MYKOLAS ROMERIS UNIVERSITY FACULTY OF SOCIAL INFORMATICS. Master Thesis

102. Vimercati, S.D.C., Foresti, S., Livraga, G., Pierangela, S., (2012). Data Privacy: Definitions and Techniques. International Journal of Uncertainty. 20(6), pp. 793-817.

103. Vroom, V. H. (1964). Work and motivation. New York: Wiley.

104. Wang, C., Wang, X., Guo, Y. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern. Journal of Enterprise Information Management. 35(3). pp. 774-795. doi:10.1108/JEIM-12-2020-0481

105. Wang, X., Hong, Z., Xu, Y., Zhang, C., Ling, H. (2014). Relevance Judgments of Mobile Commercial Information. JOURNAL OF THE ASSOCIATION FOR INFORMATION SCIENCE AND TECHNOLOGY. 65(7)

106. Wetherall, C., Greenstein, H., Hornyack, J., Schechter, W. (2011). Privacy revelations for web and mobile apps. In Proceedings of the 13th USENIX conference on hot topics in operating systems. HotOS ’11.

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

108. Wu, K., Huang, S. Y., Yen, D. C., Popova, I., (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior. pp. 889-897, doi:10.1016/j.chb.2011.12.008

109. Wurmser, Y. (2020, July 9). The Majority of Americans’ Mobile Time Spent Takes Place in Apps. eMarketer. [online] Retrieved May 23, 2023, from https://www.insiderintelligence.com/content/the-majority-of-americans-mobile-time-spent-takes-place-in-apps

110. Wurmser, Y. (2018). Mobile time spent 2018: Will smartphones remain ascendant? eMarketer. [online] Retrieved July 10, 2023, from https://www.emarketer.com/content/mobile-time-spent-2018

111. Xu, H., Teo, 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), pp.135–174. doi:10.2753/mis0742- 1222260305.

112. Xu, H., Gupta, S., Rosson, M. B., Carroll, J. M. (2012). Measuring mobile users’ concerns for information privacy. Paper Presented at the Thirty Third International Conference on Information Systems. Orlando 2012.

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

114. Yan, Z., Zhang, P., Deng, R. H. (2012). TruBeRepec: A trust-behavior-based reputation and recommender system for mobile applications. Personal and Ubiquitous Computing. 16(5). pp. 485–506.

115. Zang J, Dummit K, Graves J, Lisker P, Sweeney L. Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science*. 2015103001. October 29, 2015. https://techscience.org/a/2015103001/

116.Zaki, A.S., Ahmad, A. (2017). The Level of Integration among Students at Secondary School: A Study in Limbang, Sarawak. The International Journal of Social Sciences and Humanities Invention. 4(2). doi: 10.18535/ijsshi/v4i2.05

117.Zimmer, J., Arsal, R. Al-Marzouq, M., Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. Information & Management. doi:10.1016/j.im.2009.12.003

118.Zhang, R., Chen, J.Q., Lee, C.J. (2015). Mobile Commerce and Consumer Privacy Concerns. Journal of Computer Information Systems. doi:10.1080/08874417.2013.11645648

119.Zhou, T. (2017). Understanding location-based services users' privacy concern An elaboration likelihood model perspective. Internet Research. 27(3). pp. 506-519. doi: 10.1108/IntR-04-2016-0088

APPENDIXES

Appendix 1: Questionnaire

Dear respondent, I’m a master student at Vilnius University Business School who intend to research the effectiveness of M-commerce app privacy policies on users’ willingness to share personal information. This means you'll be questioned about your views about M-commerce privacy policies and if you'd like to share your personal information. Your participation is highly important and will contribute a lot for the further research development. Please respond to the questions by selecting the options that best reflect your opinion.

The questionnaire will consist of 6 parts. For the 1st part there are 2 demographical questions and 1 question which will help us to define are you eligible for this survey or not. For the next 5 parts, before you start answering the questions you will need to read the given privacy policy example and select the answers which are mostly reflecting your opinion and inner emotions. Please also be ensured that the questionnaire form is fully anonymous, and all the information which is going to be collected – will be kept confidential.

The author of the study would like to express in advance his appreciation for your participation in this survey, which will help to develop the findings of this study. Your personal information will be kept private and confidential, and it would take approximately 15 minutes of your time to fulfill the questionnaire. If you have any concerns or questions about the research, feel free to reach out to me at emine.ozmen98@gmail.com.

Thanks for your participation!

4. **What is your gender?**

- Female
- Male
- Prefer Not to Say

5. **Please, indicate your age in years**

    - 18-24 years old
    - 25-34 years old

- 35-44 years old
- 45+ years old

6. **Do you have a mobile device with internet access?**
    - Yes
    - No

Please imagine you want to buy a Bluetooth headset from an M-commerce app you've never used before. In order to use this mobile application and purchase the headset, you need to share some of your personal information with the application. You plan to read the privacy policy to decide whether to continue to use the app and purchase. Please read the provided privacy policy and answer the following questions.

To find the X M-Commerce App Privacy Policy, click here.

Please read and rate the statements from Strongly disagree to Strongly Agree:

Perceived Effectiveness of Privacy Policy	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I am confident that this privacy policy of the mobile commerce app genuinely reflect their commitment to safeguarding my personal information					
With this privacy policy, I believe that my personal information will be kept private and confidential by mobile commerce app					
I believe that these mobile commerce applications` privacy policies are an effective way to demonstrate their commitment to privacy					
The privacy policy provided by the mobile app, clearly and completely describes how users' privacy would be protected and used by it					

Trust	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
The mobile app's privacy policy on how it would use any personal information about me makes me feel that the app is trustworthy.					
The mobile app's online privacy policy makes me feel that the app is trustworthy.					
The mobile app's privacy policy concerning the notice of personal information collection makes me feel this app is trustworthy.					

Privacy Concern	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I am concerned about my online privacy					
I am concerned that the information I shared wıth the mobile app could be misused					
I am concerned about sharing personal information to mobile app, because of what others might do with it					
I am concerned about sharing my personal information to the mobile app, because it could be used in a way I did not foresee					

Privacy Awareness	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I follow the news and developments about privacy issues and privacy violations					
I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy					
Mobile app service providers seeking personal information should disclose the way the data are collected, processed, and used					
It is very important to me that I am aware and knowledgeable about how my personal information will be used					
I want a m-commerce app to keep me informed of changes to it's privacy practices					

Willingness to Share Personal Information	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I am willing to share my personal information with the m-commerce app					
I feel comfortable sharing my personal information with the m-commerce app					

Appendix 2

X COMMERCE MOBİLE APP PRIVACY POLICY

PRIVACY POLICY

GENERAL PROVISIONS

We, X Commerce, take your privacy seriously.

How we process your personal data depends on how you use our services. We process your personal data by providing online services of your choice, processing your requests, contacting you about products and services that may be of interest to you, organizing prize lotteries, games or contests or providing related services. All personal data is processed in accordance with the requirements of current data protection laws.

We disclose your personal data only to those third parties that help provide you with services and, if you allow us, to our group companies, for customer relationship management, analysis and marketing purposes.

If you agree, we also use cookies for marketing, fulfillment and statistical purposes.

We value our customers and give you the opportunity to determine yourself how your personal data is handled. For example, if you want to update your cookie preferences, click on the "Cookie Allower" option at the bottom right of our website window.

In addition, if you have created a personal account (on the website or mobile device app), you can update your contact information and privacy preferences in the "My Account" section. You can also contact our customer service by e-mail privacy@xcommerce.com

If you would like more information about the processing of your personal data and what we use cookies for, you can familiarize yourself with our detailed Privacy Policy below.

Our Privacy Policy was last updated: 2023. on October 20.

Our privacy principles

We take your privacy seriously and give you 5 promises:

1. We will ALWAYS ensure that your personal data is processed in accordance with the requirements of applicable data protection laws.
2. We will ALWAYS provide you with detailed and transparent information on how and for what purposes we process your personal data. This includes informing you about what data we collect about you, what we do with it, who we share it with and who you should contact if you have any questions.
3. We will ALWAYS give you the opportunity to simply say STOP if you no longer wish to receive marketing communications from us.
4. We will ALWAYS take all reasonable measures to protect your personal data and ensure that it is not accessed by unauthorized persons.
5. We will ALWAYS respond immediately to your questions about the processing of personal data.

We protect your privacy and ensure that your personal data is protected

In this Privacy Policy, we explain what personal data we collect, how we process and store it, while providing the services we offer. This includes information collected outside of online physical stores or received in the course of providing services to customers and online through the website www.xcommerce.com, apps (including apps for mobile devices) and third-party platforms ("Websites").

This Privacy Policy also applies to our targeted content, including online offers and advertisements for products and services, that you may see on third party websites, platforms and apps ("Third Party Sites") while browsing the Internet. Please note that these Third Party websites may have their own separate privacy policies and terms. Please read them before using these Third Party Sites.

WHO IS RESPONSIBLE FOR PROCESSING YOUR PERSONAL DATA?

We, "X Commerce" (**"X"** or **"we"**) are responsible for processing your personal data on our Websites.

HOW CAN I CONTACT THE DATA PROTECTION OFFICER?

If you have any questions related to how we process your personal data, you can contact our data protection officer by e-mail at privacy@xcommerce.com

WHAT IS PERSONAL DATA?

Personal data is information by which you can be directly or indirectly identified ("personal data"). This usually includes your name, address, e-mail address. email address, phone number, but may also include IP address, purchasing habits, information about your health, beauty, lifestyle and priorities, hobbies and interests. We note that health information is classified as a special category of personal data subject to higher protection requirements, given the sensitive nature of this information.

WHAT HAPPENS WHEN YOU PROVIDE US WITH YOUR PERSONAL DATA OR WE OTHERWISE OBTAIN YOUR PERSONAL DATA?

We collect your personal data directly in several ways, such as when you provide us with your personal information, register as a customer on our Websites or participate in our loyalty programs, register for prize sweepstakes, games and contests, subscribe to our newsletter, receive information or electronic communications, use our apps, purchasing products and services from us, completing questionnaires, performing beauty and health diagnostic tests, commenting, making inquiries or contacting our customer service.

When you provide us with your personal data, we process it for the purposes and in the manner defined in this Privacy Policy. If you do not want us to process your personal data in this way, please do not submit them to us

We may also receive your personal data from other sources, including commercial sector data sources such as public databases and data aggregators and information from third parties. If you do not want us to receive your personal data from other sources, indicate your preferences to the relevant sources.

We process your personal data in order to provide you with services. In specific cases, we can process your personal data only after receiving your consent, for example, usually when we process your personal data for marketing purposes, use cookies or location data, as well as when we process your sensitive personal data classified as special categories of personal data. In other cases, we may be guided by another legal basis for the processing of your personal data, e.g. to fulfill a contract with you or to have other legitimate interests, e.g. to prevent crime.

If you become a member of one of our loyalty programs, we may consider this as consent that you want us to process your personal data for marketing purposes. You can opt out of these marketing communications at any time and this will not affect your participation in the loyalty program and its benefits.

When processing your personal data with your consent, we will ask for your consent for a specific purpose of data processing. We will also ask for your consent if we need your personal data for other purposes not specified in this Privacy Policy.

FOR WHAT PURPOSES DO WE PROCESS YOUR PERSONAL DATA?

5.1 We process the following categories of your personal data for the following purposes:

Browsing our Sites

What personal data can we collect?

Information about the browser you use when you visit our Websites, your IP address and device address, links you clicked, other websites visited before our Website and information collected by cookies and similar tracking tools. Your username, profile picture, gender, relationships and any other information you agree to share when you use third-party websites (such as when you like us on Facebook).

What is the purpose of processing this data?

We (and third-party service providers acting on our behalf) use cookies and similar technologies to manage data about you when you visit our Sites. We want to know if you have visited our Sites before and what you prefer so that we can tailor our experience to you.

How long do we store your personal data?

The storage time is linked to the validity of the cookies, which are valid according to the order set by the browser and can be deleted from it if necessary.

What is the legal basis for data processing?

Your consent when you click "accept and continue" on the Cookie Allower on our websites. In some cases and whenever permitted by law, we will assume that you consent to the use of cookies based on your actions. Please note that we need to process basic data about your browsing in order to provide you with the basic functions of the Websites, such as a secure login, or to remember what stage of the order you are at.

You can change your cookie preferences at any time in our Cookie Allower or by changing your browser settings.

Purchase/Acceptance of Service

What personal data can we collect?

Name, surname, postal address, e-mail email address, home phone number, mobile phone number, loyalty card number, passwords, order history, payment history, payment information (ie bank or credit card details), order history / wish list, age / date of birth, gender, your order fulfillment information (including information related to drugs and other medications or beauty products that you order) and other personal data that you voluntarily provide to us.

What is the purpose of processing this data?

We process personal data to provide you with the products and services you have ordered, including sending you ordered products or samples.

How long do we store your personal data?

As long as you buy from us. If no transactions have taken place within 3 (three) years, we delete or anonymize your personal data, except in cases where the law establishes a longer term for the storage of such data.

What is the legal basis for data processing?

We use this information to fulfill your order or any other service ordered by you (execution of the contract). In the event that we need your sensitive personal data (e.g. information about your health due to medication), we will clearly inform you of our legal obligations when processing such personal data.

Customer service

What personal data can we collect?

First name, last name, mailing address, home phone number, mobile phone number, loyalty card number, passwords, order history, payment history, payment information (ie bank or credit card information), order history / wish list, age / date of birth , gender, request fulfillment information, postings and other content you provide on our Sites, as well as other information you provide when purchasing or ordering a service, making a request (including sensitive personal data).

What is the purpose of processing this data?

We process your personal data when you contact us and when we respond to your inquiries and comments.

How long do we store your personal data?

General inquiries and comments related to service issues, store standards, product availability, etc. Are stored for 3 (three) years from the date of the last contact with you. Correspondence related to personal injury, accidents and other health and safety issues may be kept longer if there is litigation or settlement.

What is the legal basis for data processing?

Processing of your requests, comments and complaints at your request (execution of an obligation arising from a contract or other legal actions).

Offering products and services that may be of interest to you

What personal data can we collect?

Name, surname, postal address, e-mail email address, mobile phone number, loyalty card number, order history / wish list (including your purchases on our Website, mobile app, store), payment history, age, date of birth, gender, products you view on our Website, favorite brands, your favorite store, your actions on our Website and when reading our letters, your answers in surveys or contests, your shopping habits and priorities and information about your lifestyle, hobbies and areas of interest.

What is the purpose of processing this data?

To offer you customized products or services (including from related third parties) that may be of interest to you based on your purchase history and behavior, priorities and our marketing segmentation strategies. We can do this by sending you information by mail, e-mail. by mail, newsletters, SMS messages, active app notifications or by phone about products, services, promotions, etc. We may also contact you to invite you to participate in customer surveys, promotions, sweepstakes and contests. You may also receive in-store promotions (such as coupons) when you create an account on our Site or participate in a loyalty program.

How long do we store your personal data?

As long as you buy from us. If you have a loyalty card and no transactions have taken place within 3 (three) years, we delete or anonymize your personal data, except in cases where the law establishes a longer storage period for such data. If you shop online as a guest, we store your data for 1 (one) year after shopping. If you have subscribed to our newsletter, we will store your data until you unsubscribe.

What is the legal basis for data processing?

You allow us to process your personal data if you become a member with a loyalty card and agree to the terms of our customer loyalty program (execution of the contract).

If you do not participate in the loyalty program, you give us permission to process your personal data by subscribing to our newsletters.

If you shop online as a guest, we will contact you about related offers to the extent permitted by law, including spam provisions.

You can opt-out of our marketing communications at any time by using the Privacy Settings panel in your profile (if you have one) or by clicking the unsubscribe button in our marketing emails sent to you.

Contests and games

What personal data can we collect?
Name, surname, postal address, e-mail e-mail address, home or mobile phone number, age, date of birth, gender, user-generated content or any other personal data provided by you - according to the needs of the competition or game.

What is the purpose of processing this data?
To conduct prize sweepstakes, games and contests in which you choose to participate and to determine the winner or transfer the prize if you win.

How long do we store your personal data?
3 (three) months after the end of the game or competition, except in cases where the law establishes a longer term for the storage of such data.

What is the legal basis for data processing?
We need this data to identify the participants/winners of the contest or game and to transfer the prize to you (execution of the contract). If we intend to use your personal data for marketing purposes, we will clearly inform you before starting data processing and ask for your consent.

Online shopping

What personal data can we collect?
Name, surname, postal address, e-mail e-mail address, home phone or mobile phone number, information about ordered products (including health products or medicines if you ordered from our online store), order history, detailed information about your purchases, payment information, payment history, age.

What is the purpose of processing this data?

To process your online order and deliver the ordered products. Your personal data related to payment execution may be forwarded to payment intermediaries for the purpose of payment execution.

How long do we store your personal data?

As long as you buy from us. If no transactions have taken place within 3 (three) years, we delete or anonymize your personal data, except in cases where the law establishes a longer term for the storage of such data.

If you pay as a guest, we store your data for 1 (one) year after shopping.

What is the legal basis for data processing?

We need these data to fulfill your online order (execution of the contract); data about health, beauty or diagnostic data are processed only after receiving your consent.

Loyalty program

What personal data can we collect?

Name, surname, postal address, e-mail email address, home phone or mobile phone number, information about the products you ordered using the loyalty program, transactions related to the loyalty program, account status and information about received and used points, payment information (e.g. bank information), payment history, age.

What is the purpose of processing this data?

To provide you with all services under the loyalty program, including exclusive offers and collecting points.

How long do we store your personal data?

While you are participating in one of our loyalty programs. If no transactions have taken place within 3 (three) years, we delete or anonymize your personal data, except in cases where the law establishes a longer term for the storage of such data.

What is the legal basis for data processing?

By registering for one of our loyalty programs, you allow us to process your personal data in order to provide you with all services under the loyalty program (performance of the contract). Crime prevention and service services, such as registration

Crime prevention and service services

What personal data can we collect?

Name, surname, postal address, e-mail postal address, home telephone or mobile phone number, health information or diagnostic details, NHS number (UK only), payment details (eg bank details), payment history, age.

What is the purpose of processing this data?

To provide our services, including processing your service requests, preventing fraud and other crimes, verifying your identity and credit/payment status, and executing payment instructions. Your personal data related to payment execution may be forwarded to payment intermediaries for the purpose of payment execution or to the police for fraud prevention purposes.

How long do we store your personal data?

As long as you buy from us. If no transactions have taken place within 3 (three) years, we delete or anonymize your personal dataCookies and similar technologies, except in cases where the law establishes a longer storage term for such data.

What is the legal basis for data processing?

Dedicated to fraud detection and prevention to ensure your identity and transactions are secure (combining interests with ours to prevent fraud and protect our customers).

We provide other services to provide you with relevant additional services (execution of the contract).

5.2 Cookies and similar technologies

We use cookies and similar technologies (**"cookies"**) to improve our products and your experience on our Sites by collecting information about how you use our Sites. Some of the cookies used are necessary for the main functions of the Website, for example to provide a secure login or to remember which stage of the order you are at; however, we also use cookies to analyze the use of the Website (to evaluate and improve its performance); advertising cookies are used by advertising companies to present advertising that matches your interests.

Also, by collecting information about your device and linking it to your personal data, we can better adapt our Website to your needs and interests, and ensure that our Website provides you with the best experience.

With Google Analytics, we have set the service so that as soon as the data is received by the Analytics Collection Network **https://support.google.com/analytics/answer/2763052?hl=en** before the data is stored or processed, your IP address will be anonymized. To opt out of being tracked by Google Analytics on all Sites, please visit **http://tools.google.com/dlpage/gaoptout** .

You can find more information about the cookies we use in your settings window by using the Cookie Permission tool on our Website. We draw your attention to the fact that without cookies you may not be able to use all the services of our Websites.

5.3 Your personal data in the X Commerce mobile app

X Commerce mobile app does not collect or store photos taken with your smartphone.

We will ask you for separate permissions to give our mobile app access to the camera. If you change your mind, you can revoke permissions at any time by changing your device settings. Please note that denying or disabling these permissions will limit the features you can use in our mobile app.

We also use facial recognition technology already on your smartphone (such as the TrueDepht API) to create augmented reality effects in our mobile app. We do not share this information with third parties, store or otherwise process the data we access using this technology.

TO WHOM CAN WE TRANSFER (SHARE) YOUR PERSONAL DATA?

6.1 Our service providers

We share your personal data with the following data processors (i.e. service providers who help us perform the above tasks):

- Trusted third parties that help us manage and analyze your personal data and support when we offer 6.1. products and services discussed in the point that may be of interest to you.
- If you order a product or service from us, to trusted third parties to enable payments and the delivery of the products you ordered and the provision of services. If you have not given your consent, these trusted third parties do not have our authority to use your personal data in any way other than as set out in this clause; we require these trusted third parties to use appropriate technical and organizational measures to ensure the security of your personal data.

We emphasize that we impose strict requirements on these data processors in accordance with the applicable data protection laws, so that they process your personal data only in accordance with the purposes and scope specified by us and comply with high IT security standards.

6.2 Other Recipients

We share your personal data with the following third parties who process your personal data for their own purposes (ie these third parties are not our authorized data processors, they use your personal data for their own interests or because you have agreed to it):

- To interested third parties (not ASW Group companies or CK Hutchison affiliates) who will send you marketing material, but only if you have agreed to receive it from them.
- To law enforcement and other institutions, if disclosure of your personal data is required by law, legal order of authorities/officials or court decision.

Please note that we never share your personal data on social networks. When we expand our customer base or target customers through social networks such as Facebook or Google, we anonymize your personal data before transmitting it. If there are changes in the future and we have to share your personal data on social networks, we will ask for your consent in advance.

6.3 Sharing information about your use of the Website

With your consent, we will share information about your use of the Site with trusted third parties (ie, advertisers, advertising agencies, ad networks, data exchange entities, etc.) in order to provide you with content that is tailored to you and may be of interest to you based on your past activity on our Site.

WHAT ARE YOUR RIGHTS?

If the relevant requirements are met, you have the following rights:

- Get confirmation from us that we process your personal data or not, and if so, get access to your personal data and familiarize yourself with them;
- Require us to correct inaccurate personal data about you;
- Require us to delete your personal data ("right to be forgotten");
- Disagree with the processing of your personal data;
- Require us to limit the processing of your personal data and
- To contact us regarding the portability of your personal data means to receive your personal data in a structured, commonly used and automatically readable form and forward it to another data controller.

You can learn more about these rights at https://www.ada.lt/go.php/JUSU-TEISES770 .

To exercise your rights, contact e-mail by mail privacy@xcommerce.com

Please note that you do not need to contact the Data Protection Officer to exercise your right to stop receiving marketing communications from us. You may opt-out of these communications in the "Privacy Settings" area of the "My Account" window on our Site.

CAN YOU WITHDRAW YOUR CONSENT TO US PROCESSING YOUR PERSONAL DATA?

In cases where your consent constitutes a legal basis for us to process your personal data, you can withdraw your consent in the following ways:

- Marketing Communications: By logging into your account in the Privacy Settings area or using the unsubscribe link in any marketing communications we send you.
- Other purposes: Email us email privacy@xcommerce.com

Please note that the withdrawal of your consent does not affect the lawfulness of the processing of your personal data before the withdrawal.

CAN YOU COMPLAIN TO DATA PROTECTION AUTHORITIES?

If you believe that we violate data protection laws when processing your personal data, you can contact us by e-mail. by mail privacy@xcommerce.com and if the issue you are concerned about cannot be resolved, file a complaint with the competent authorities in accordance with the procedure established by legal acts.

HOW DO WE ENSURE THE SECURITY OF YOUR PERSONAL DATA?

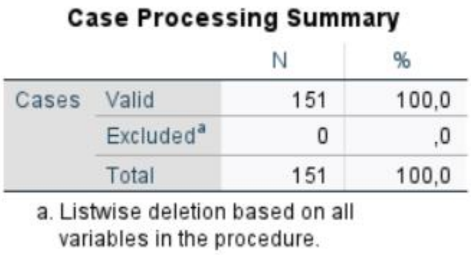
We use appropriate technical and organizational measures to protect the personal data provided by you against accidental or unlawful destruction, loss, alteration, unlawful disclosure or unlawful access to your personal data.

CAN WE CHANGE THE PRIVACY POLICY?

If necessary, we may change this Privacy Policy by posting an updated version of the Privacy Policy here. We kindly ask you to visit this section often and familiarize yourself with the current version of the Privacy Policy.

Tables from SPSS related to reliability test

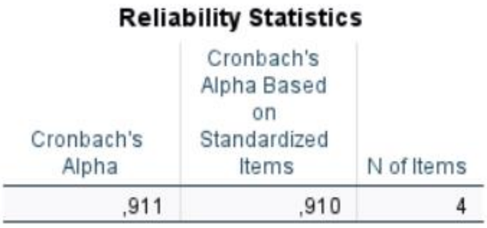
Appendix 3: Perceived Effectiveness of Privacy Policy



Case Processing Summary

		N	%
Cases	Valid	151	100,0
	Excluded[a]	0	,0
	Total	151	100,0

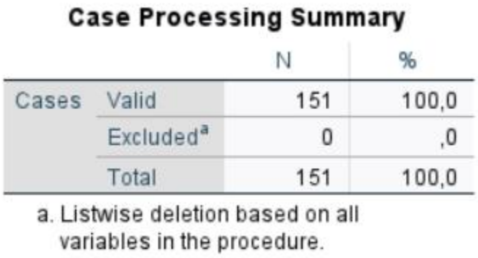
a. Listwise deletion based on all variables in the procedure.



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,911	,910	4

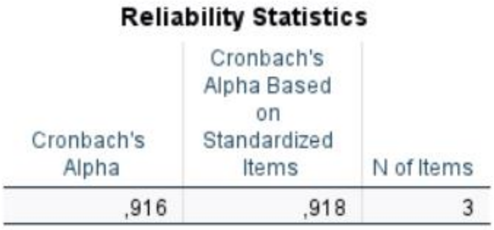
Appendix 4: Trust



Case Processing Summary

		N	%
Cases	Valid	151	100,0
	Excluded[a]	0	,0
	Total	151	100,0

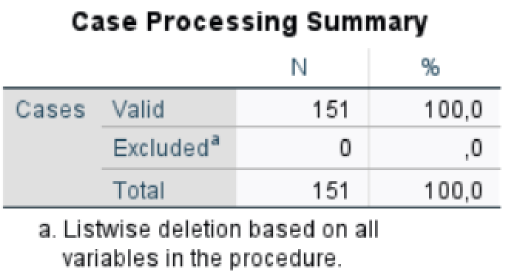
a. Listwise deletion based on all variables in the procedure.



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,916	,918	3

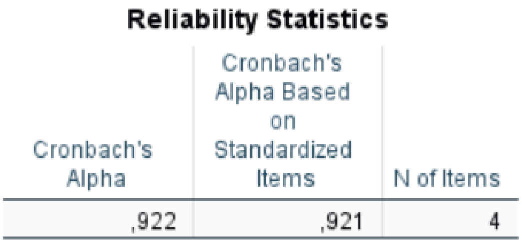
Appendix 5: Privacy Concern



Case Processing Summary

		N	%
Cases	Valid	151	100,0
	Excluded[a]	0	,0
	Total	151	100,0

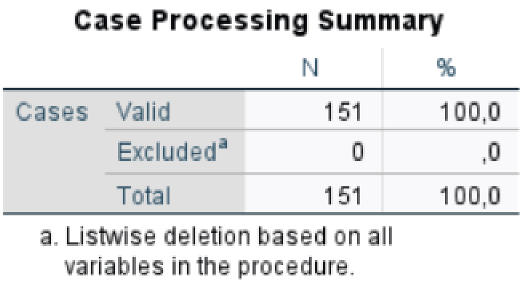
a. Listwise deletion based on all variables in the procedure.



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,922	,921	4

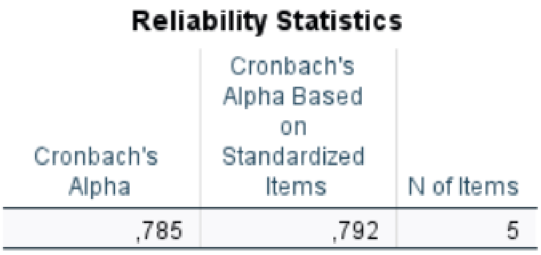
Appemdix 6: Privacy Awareness



Case Processing Summary

		N	%
Cases	Valid	151	100,0
	Excluded[a]	0	,0
	Total	151	100,0

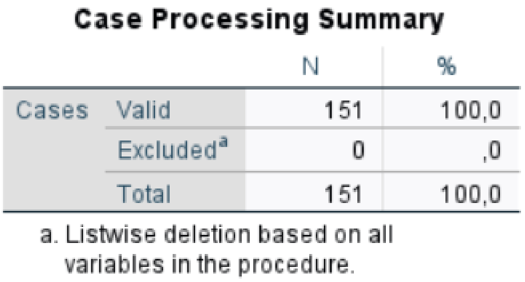
a. Listwise deletion based on all variables in the procedure.



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,785	,792	5

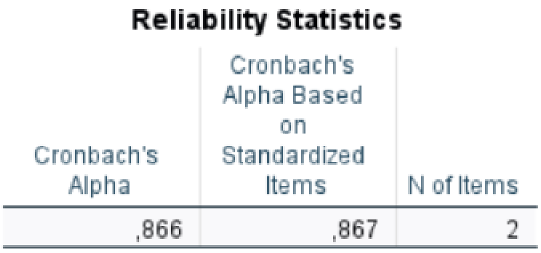
Appendix 7: Willingness to Share Personal Information



Case Processing Summary

		N	%
Cases	Valid	151	100,0
	Excluded[a]	0	,0
	Total	151	100,0

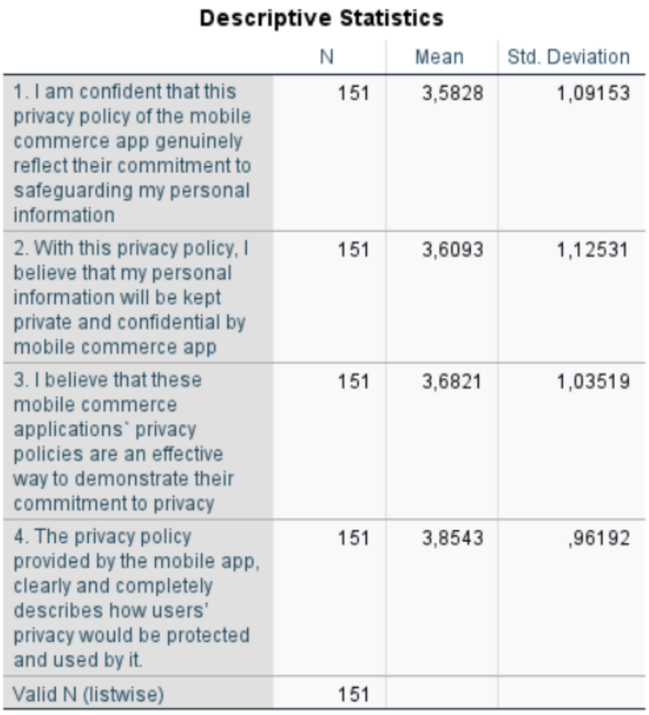
a. Listwise deletion based on all variables in the procedure.



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,866	,867	2

Appendix 8: Descriptive Statistics of Perceived Effectiveness of Privacy Policy

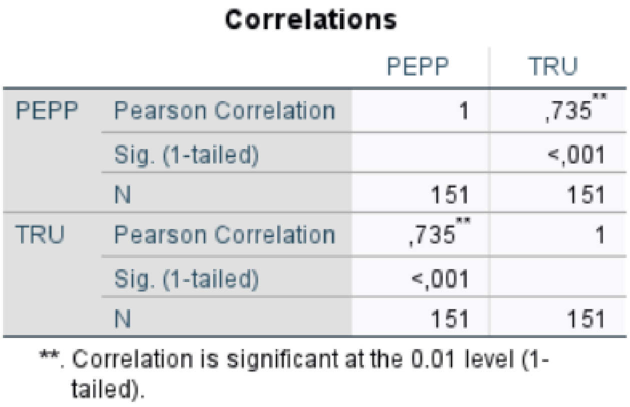


Descriptive Statistics

	N	Mean	Std. Deviation
1. I am confident that this privacy policy of the mobile commerce app genuinely reflect their commitment to safeguarding my personal information	151	3,5828	1,09153
2. With this privacy policy, I believe that my personal information will be kept private and confidential by mobile commerce app	151	3,6093	1,12531
3. I believe that these mobile commerce applications` privacy policies are an effective way to demonstrate their commitment to privacy	151	3,6821	1,03519
4. The privacy policy provided by the mobile app, clearly and completely describes how users' privacy would be protected and used by it.	151	3,8543	,96192
Valid N (listwise)	151		

Correlation Analysis

Appendix 9: Correlation Analysis of H1

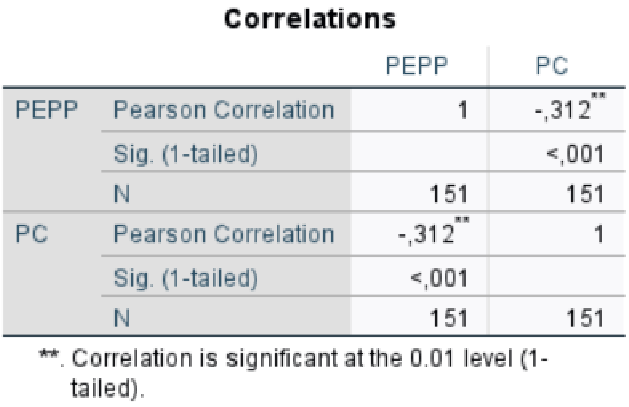


Correlations

		PEPP	TRU
PEPP	Pearson Correlation	1	,735**
	Sig. (1-tailed)		<,001
	N	151	151
TRU	Pearson Correlation	,735**	1
	Sig. (1-tailed)	<,001	
	N	151	151

**. Correlation is significant at the 0.01 level (1-tailed).

Appendix 10: Correlation Analysis of H2

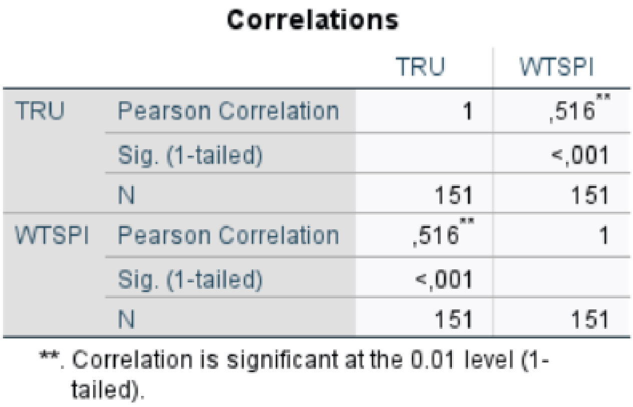


Correlations

		PEPP	PC
PEPP	Pearson Correlation	1	-,312**
	Sig. (1-tailed)		<,001
	N	151	151
PC	Pearson Correlation	-,312**	1
	Sig. (1-tailed)	<,001	
	N	151	151

**. Correlation is significant at the 0.01 level (1-tailed).

Appendix 11: Correlation Analysis of H3

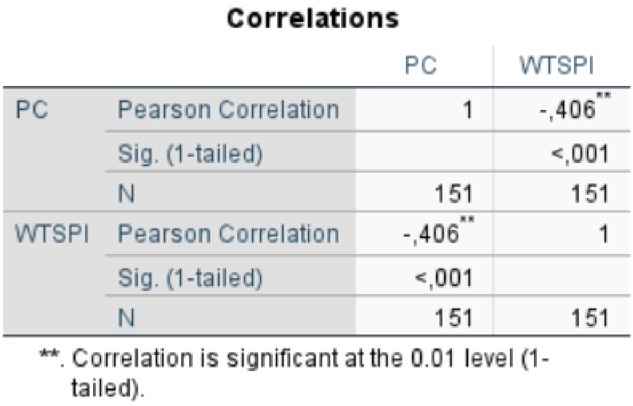


Correlations

		TRU	WTSPI
TRU	Pearson Correlation	1	,516**
	Sig. (1-tailed)		<,001
	N	151	151
WTSPI	Pearson Correlation	,516**	1
	Sig. (1-tailed)	<,001	
	N	151	151

**. Correlation is significant at the 0.01 level (1-tailed).

Appendix 12: Correlation Analysis of H4

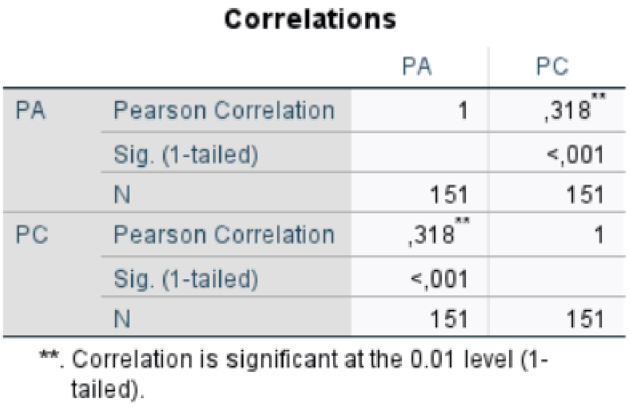


Correlations

		PC	WTSPI
PC	Pearson Correlation	1	-,406**
	Sig. (1-tailed)		<,001
	N	151	151
WTSPI	Pearson Correlation	-,406**	1
	Sig. (1-tailed)	<,001	
	N	151	151

**. Correlation is significant at the 0.01 level (1-tailed).

Appendix 13: Correlation Analysis of H5



Correlations

		PA	PC
PA	Pearson Correlation	1	,318**
	Sig. (1-tailed)		<,001
	N	151	151
PC	Pearson Correlation	,318**	1
	Sig. (1-tailed)	<,001	
	N	151	151

**. Correlation is significant at the 0.01 level (1-tailed).