UNIVERSITY
OF TWENTE.

INFLUENCING MILLENNIALS' TRUST, PRIVACY RISK PERCEPTIONS AND INTENTION TO REGISTER IN M-COMMERCE APPLICATIONS

EXAMINATION COMMITTEE
Dr. A.D. Beldad
Dr. J. Karreman

FEBRUARY 2020
Chiel Gasthuis

INFLUENCING MILLENNIALS’ TRUST, PRIVACY RISK PERCEPTIONS AND INTENTION TO REGISTER IN M-COMMERCE APPLICATIONS

THE EFFECTS OF LOGIN TYPES, COUNTRY OF ORIGIN
AND PRIVACY STATEMENT CONSENT

UNIVERSITY
OF TWENTE.

MASTER THESIS

Name:	Chiel Gasthuis
Student number:	s2184133
E-mail:	c.l.h.gasthuis@student.utwente.nl
Institution:	University of Twente
Faculty:	Behavioural Management and Social Sciences (BMS)
Master:	Communication Science
Specialization:	Digital Marketing Communication
Supervisor:	Dr. A.D. Beldad
Second supervisor:	Dr. J. Karreman
Date:	March 11, 2020

ABSTRACT

Purpose

M-commerce is a very popular manner of online shopping, especially among millennials. M-commerce involves mobile devices to search for, browse, compare and purchase products and services online. Most of the m-commerce platforms require users to log in by disclosing personal information during the first-time visit. Due to a large number of m-commerce platforms, consumers have difficulties with choosing suitable, secure, and trustworthy platforms. The research aims to study the influence of different login types on consumers' trust, privacy risk perceptions, and their intention to register in an m-commerce app. The interaction roles of the country of origin of the app, privacy statement consent, and privacy valuation were also included.

Method

To answer the research questions and test the hypotheses, a 2x2x2 experimental design was used in which login type (general vs. social), the apps' country of origin (EU vs. non-EU), and privacy statement consent (passive vs. active) were manipulated. The effects on privacy risk perception, trust in the app, and the intention to register in the app were measured. The focus is on Dutch millennials as millennials are the driving force of online shopping. The respondents (N = 212) were exposed to one of the eight experimental conditions.

Findings

Findings of this study show that the login type does not significantly influence consumers' trust and their privacy risk perceptions. However, the country of origin of the app significantly influences consumers' trust, privacy risk perceptions and their intention to register. Besides, trust in the app decreases privacy risk perceptions and increases consumers' intention to register in the app. Results also show that privacy risk perceptions significantly affect consumers' intention to register to an m-commerce app. No evidence was found for the interaction effects of country of origin, privacy statement consent and privacy valuation. The effect of login type on consumers' intention to register was not mediated by trust and privacy risk perception.

Conclusion

This research shows that it does not matter for m-commerce apps whether to offer general or social login to influence consumers' trust and their privacy risk perceptions. Apps from the European Union are higher trusted, create less privacy risk perceptions, and higher registration intentions compared to apps from outside the European Union. The higher consumers' trust in an app, the lower their privacy risk perceptions and the higher their intention to register in the app. Having lower privacy risk perceptions leads to a higher intention to register in the app and vice versa. Findings add to the body of research in the field of m-commerce and the growing area of login functionalities and could be used as a foundation and inspiration for future research into the influence of login functionalities. The results help app developers and organizations in improving and developing m-commerce apps and their registration environments.

Keywords: millennials, m-commerce, login functionalities, trust, privacy, registration

TABLE OF CONTENTS

1. INTRODUCTION

Nowadays, companies and consumers are increasingly using digital purchase environments, also known as e-commerce and m-commerce. In particular, millennials use these platforms, as they have grown up with purchasing online and their e-commerce usage keeps growing. Millennials even have been recognized as the driving force of online shopping (Taken Smith, 2012). The rise of m-commerce applications (apps) such as Bol.com, Zalando, and Wish, enabled them to sell to potential buyers worldwide (Guo, Bao, Stuart, & Le-Nguyen, 2017). M-commerce involves using mobile devices to search for, browse, compare and purchase products and/or services online (Marriott & Williams, 2018). M-commerce organizations encourage consumers to download the application and make them set up an account by directing them into the app-store of their device and this has become extremely popular (Morath & Münster, 2017). Due to a large number of m-commerce platforms, consumers are confused about choosing suitable, secure, and trustworthy platforms (Xu, Zhang, & Yan, 2018). In addition to the general login type which requires a username and password, many of these m-commerce platforms have built-in social login functionalities. With social login, m-commerce platforms encourage users to login with one of their social networks such as Facebook, Twitter, and Gmail (Kontaxis, Polychronakis, & Markatos, 2012). Due to increasing popularity and implementation of social login, consumer privacy concerns increased as third parties can have access to personal data from user profiles when using social login (Kontaxis et al., 2012; Krasnova, Eling, Abramova, & Buxmann, 2014; Micallef, Adi, & Misra, 2018).

Consumer trust in m-commerce involves trust in technology and consumer-business relationship issues (Zhang, Wang, Tuerxunhazi, & Yun, 2018). Most consumers feel unconfident towards current guidelines and policies related to online privacy and security (Yazdanifard, Edres, & Seyedi, 2011). Furthermore, high levels of privacy and security have a positive influence on users' trust in the app (Ling, Chai, & Piew, 2010). Therefore, the online trust of online businesses is considered as a crucial success factor (Beldad, De Jong, & Steehouder, 2010). When users do not trust an organization, most people are less likely to enter into an online transaction (Hoffman, Novak, & Peralta, 1999; Li & Pavlou, 2013). Since companies increasingly gather data, people are aware and concerned that their data might be misused (Abdullah, Ramli, Bakodah, & Othman, 2019). Therefore, privacy and security issues are major obstacles online. Besides, in some countries outside the European Union (EU), privacy is not even seen as a fundamental human right (Adelola et al., 2014). The EU is a worldwide leader when it comes to privacy regulation (Goldberg, Johnson, & Shriver, 2019). On the other hand, the digital privacy regulation laws of countries such as China and Russia do not even provide sufficient protection (Greenleaf, 2018b; Zharova & Elin, 2017).

Many factors influence consumers' m-commerce trust and usage. Several studies demonstrate that trust, risks, privacy concerns, and security significantly predict m-commerce purchase intentions and behavioural intention (Barry & Jan, 2018; Blaise, Halloran, & Muchnick, 2019). According to Basarir-Ozel and Mardikyan (2017) and Li and Pavlou (2013), consumers' usage intention and intention to register are positively influenced by trust. A study by Dinev, Hart, and Mullen (2008) shows that privacy concerns have positive effects on consumers' willingness to disclose information. Besides, security, privacy, and ease of use are some of the most important factors for consumers to trust a website (Gupta & Dubey, 2016). However, e-commerce platforms should carefully evaluate the importance of these factors. M-commerce providers should develop platforms that are not only useful and enjoyable, but also need to be private, secure, and trustworthy and should include privacy and security-building mechanisms (Barry & Jan, 2018; Kidane & Sharma, 2016).

Nilashi, Ibrahim, Mirabi, Ebrahimi, and Zare (2015) consider trust in online settings as an important research topic as a result of its powerful role within online decision making. According to Li and Pavlou (2013), research into what drives user registration is lacking and the influence of trust and information privacy concerns on user registration is not widely researched in an online context. There is a lack of understanding into what extent trust and privacy risks increase or decrease consumers' intention to adopt m-shopping (Li & Pavlou, 2013). Future research can examine consumer trust against specific retailers and m-shopping situations to obtain a greater understanding of its significance (Marriott & Williams, 2018). There is a lack of research into consumer privacy concerns concerning the increasing amount of personal data in mobile contexts (Eastin, Brinson, Doorey, & Wilcox, 2016). Besides, little research has been conducted into the influence and effects of login types, particularly on privacy concerns and app adoption (Krasnova et al., 2014; Micallef et al., 2018). Furthermore, future research can explore different ways to improve the perceived adequacy of online businesses privacy policy statements such as interactive design, and plain and clear language (Bansal, Zahedi, & Gefen, 2015). New insights are needed to understand consumers' decision to use m-commerce (Kalinic & Marinkovic, 2015).

Research has shown many factors influence trust, behavioural intentions, and the willingness to disclose personal information and registration intentions in m-commerce environments. Due to the increasing amount of data collection, the factors trust, privacy, and security become highly important. Consumers worry about the quantity of collected personal information, loss of control, privacy violations, and the increasing growth of databases (Wu, Huang, Yen, & Popova, 2012). As every organization in any country can create m-commerce apps, in combination with all the different privacy laws, it becomes interesting to investigate its effects. As online trust of online businesses is considered as a crucial success factor, it is interesting to test the interacting effects of these factors. Besides, there is a lack of insight into the degree of how these factors should be present in m-commerce environments. Therefore, this study conducts a 2 x 2 x 2 experimental design to answer the following research questions:

1: To what extent does login type influence trust, privacy risk perceptions, and the intention to register?
2: To what extent does country of origin influence trust, privacy risk perceptions, and the intention to register?
3: To what extent is the effect of the login type dependent on country of origin, privacy statement consent, and privacy valuation?
4: To what extent is the effect of login type on intention mediated by trust and privacy risk perceptions?

This study adds knowledge to the growing field of m-commerce shopping apps and the influence of trust since Marriot and Williams (2018) suggested that future research could examine consumer trust perceptions in the context of m-shopping. Theoretical and practical insights will be obtained into the influence of trust and information privacy concerns on user registration since this area is not widely researched in the online context (Li & Pavlou, 2013). Furthermore, new insights will be gathered into the underlying reasons for consumers' intention to register in m-commerce apps. New insights into the influence of different login types will be gathered since almost no studies have been conducted into the effects and relationships of login functionalities. This study should help app designers, app developers, and organizations with the improvement of m-commerce apps, especially with improving the use of login types and the design of registration environments. Besides, this study gathers valuable insights that help with the improvement of the design of privacy policy statements as Bansal et al. (2015) suggested.

The next part of this paper is organized into five sections. Following the introduction, section 2 explains the theoretical framework including the proposed research model and research hypotheses. Section 3 describes the research methodology. Section 4 presents the empirical findings and results. Section 5 presents an elaborate discussion of the results, including theoretical contributions, research limitations, and suggestions for future research. Finally, section 6 provides the conclusion.

2. THEORETICAL FRAMEWORK

Since this study focuses on the influence of login types on consumers' trust and intention to register in an m-commerce application, variables need to be identified. They will be discussed in the following section and forms a comprehensive discussion of all present variables in this study.

2.1 M-commerce

As introduced in the introduction, this study aims at the m-commerce context. M-commerce consists of consumers using mobile devices like smartphones or tablets to browse, search for, compare and purchase products or services online (Marriott & Williams, 2018). A wide variety of m-commerce applications are available, with easy to use, and sometimes personalized interfaces (Yazdanifard et al., 2011). There is no physical interaction with the m-commerce organization since users do not see real products and have to pay in advance (Yazdanifard et al., 2011; Bhaskar & Kumar, 2016). Besides, many m-commerce applications require consumers to register in the app to receive access to the platform, which means they have to log in and disclose personal information (Morath & Münster, 2017). According to Li and Pavlou (2013), disclosing personal information is not always desirable for the user. The involvement of personal information can result in a variety of issues and influence consumers' willingness to disclose and m-commerce usage (Leon et al., 2015; Yazdanifard et al., 2011). Therefore, the success of many m-commerce platforms depends on app downloads and user registration.

The intention to register is an important variable within this study since behavioural intention is described as the most important predictor of actual behaviour (Fishbein & Ajzen, 1975). Li & Pavlou (2013) describe user registration as a one-off process by establishing an identity to get access to and perform actions on a specific website or application. Most user registration processes ask for a username or email address, password, and password verification (Li & Pavlou, 2013). Once registered, users can access and start using the app, browse through the app, make purchases, and build a relationship with the organization behind. To make sure consumers download the app and register, m-commerce organization need to protect consumers' privacy and provide security (Yang, 2005; Yazdanifard et al., 2011). Besides, Nilashi et al. (2015) state that m-commerce platforms that are regarded as trustworthy reach higher retention rates and consumers reach higher degrees of purchase intention. M-commerce applications need to be useful, secure, and trustworthy concerning privacy and security (Kidane & Sharma, 2016). Studies reveal that trust, risks, security and privacy concerns are reliable predictors of the intention to use m-commerce (Blaise et al., 2018; Eastin et al., 2016). Several factors influence the intention the register in the app, but the most important factors are trust and privacy risk perceptions (e.g. Dinev & Hart, 2006; McKnight, Choudhury, & Kacmar, 2002).

2.2 Trust

Consumer trust is a key element to the usage, growth, and success of m-commerce as trust positively influences consumers' intention to register and their usage intention (Basarir-Ozel & Mardikyan, 2017; Li & Pavlou, 2013; Yazdanifard et al., 2011). In the m-commerce environment, trust belief is defined as the extent to which individuals believe that an organization is protecting and not misusing personal data (Bol et al., 2018; Li, 2011). Within this study, trust in the app refers to the degree to which consumers believe the organization keeps its promises and commitments, cares for the interests of the user, and protects the user's information (Wakefield, 2013). Obtaining trust in the mobile commerce environment is a big challenge, and trust has a big influence on consumers decision making (Nilashi et al., 2015). M-commerce consumers consider the information quality, privacy and security concerns as factors that have a main influence on their trust level in the m-commerce application (Gupta & Dubey, 2016). Consumers evaluate these factors in their decision-making process to look for the most appropriate m-commerce platforms (Nilashi et al., 2015). Nilashi et al. (2015) and Gupta and Dubey (2016) state that a lack of trust and fear of losing personal information makes consumers refuse to transact online. When a m-commerce platform is trusted, consumers' concerns about disclosing their data decrease (Eastin et al., 2016; Li & Pavlou, 2013). Previous studies (e.g. Castaneda & Montoro, 2007; Kim, Ferrin & Rao, 2008; Luo, 2002) claim that an increased trust level reduces privacy risk perceptions, especially in online vendors. High levels of trust take out the risk perceptions and encourage users to engage with online vendors by registering, sharing data, or purchase (Li & Yeh, 2010; Lu, Fan, & Zhou, 2016).

2.3 Privacy risk perception

Disclosing personal information does not only involve benefits, but also risks to users (Wang, Duong, & Chen, 2016). Risk perceptions can be defined as beliefs about possible harms or the possibility of a loss (Eastin et al., 2016). Privacy risk perceptions can be considered as risks related to privacy. Due to the disclosure of immense volumes of personal data, privacy risks have increased, such as the exploitation of personal data (Wang et al., 2016). In addition, Sharma and Crossler (2014) and Wakefield (2013) claim that when users need to share data which is of lower relevance to the exchange purpose, privacy risk perceptions are being influenced significantly. Sensitive information also higher consumers' privacy risk perceptions (Li & Pavlou, 2013). Inappropriate access by unauthorized parties, unauthorized personal data trading, personal data collection in databases without the user's permission, and data theft are the most common privacy risks (Gupta & Dubey, 2016; Li & Pavlou, 2013). Analysing the value of taking the perceived risks in a specified context is the main incentive for consumers to disclose personal information (Leon et al., 2015). Eventually, privacy risk perceptions can lead consumers to not install a certain app and is a key factor that influences consumers' intention to register (Dinev & Hart, 2006; Wang et al., 2016).

In the end, trust in the online vendor negatively influences consumers' privacy risk perceptions which encourage consumers' behavioural intention to register, share data, or make purchases (Li & Yeh, 2010; Lu et al., 2016). Furthermore, research of Dinev, et al. (2008) shows that minimizing privacy risk perceptions has a positive effect on the willingness to disclose consumer information that is necessary to register, use the application, or to conduct transactions online. The bigger the privacy risk perceptions, the lower the intention to register or to share personal information within online commerce environments (Pavlou, Liang, & Xue, 2007; Dinev & Hart, 2006). This demonstrates that trust and privacy risk perceptions are preconditions for consumers' intention to register or not.

2.4 Login type (general vs social)

Various factors influence trust and privacy risk perception, however the focus in this study will be on login type. To be able to log in, users need to register first by providing personal information. Several fields have to be filled in with information, depending on the information that is required to perform the login process (Li & Pavlou, 2013). M-commerce apps use multiple technologies for user registration (Bansal, Bhargavan, & Maffeis, 2012). There are two different types of login functionalities: general login and social login. General login asks users to log in by using an email address or username and a password (Li & Pavlou, 2013). Social login asks users to login with one of their existing social networking accounts (Bansal et al., 2012). When using social login, personal information from the user's social media profile will be shared (Kontaxis et al., 2012). Especially the security of a user's private data is the major influencer of consumers' trust in an m-commerce application (Nilashi et al., 2015; Gupta & Dubey, 2016). The higher the levels of privacy and security, the higher the users' trust in the app (Ling et al., 2010). Due to high amounts of shared personal information online, privacy risks related to the misuse of user's information increase (Wang et al., 2016). Most consumer privacy concerns are related to personal information like unauthorized data use and data collection, access without user approval, and data theft (Li & Pavlou, 2013; Wang et al., 2016). Because of all these issues, users are more likely to register and login in m-commerce applications they trust (Leon et al., 2015; Li & Pavlou, 2013; Yazdanifard et al., 2011).

General login

To be able to use many m-commerce apps, users' need to register during their first-time visit. The general login type asks users to log in by using an email address or username and a password (Li & Pavlou, 2013). Once registered with general login, users can always log in with their account but can only be used in the app the account has been created. General login is a simple functionality where little personal information is required and only the m-commerce app is involved. As discussed before, many consumers are likely to share information online. Consumers share their personal data based on the sensitivity of the information, the aim of the data collection and data use, perceived risks, and the perceived necessity of the data (Leon et al., 2015; Wakefield, 2013). The more sensitive the requested information is, the lower consumers' trusting beliefs and willingness to disclose (Li & Pavlou, 2013). This shows that consumer privacy is the major concern consumers have related to m-commerce (Yazdanifard et al., 2011). Relating these findings to the context of this study, one could say that general login can be seen as a very trustworthy, secure, and private login type. This can be attributed to the fact that only a little information is needed and only one party is involved, which leads to higher trust in the app.

Social login

Social login has become a popular feature of m-commerce apps and is supported by the biggest social networks such as Gmail, Facebook, and Twitter (Kontaxis et al., 2012). Many m-commerce applications use social login as an extra login option that allows the user to login with one of their social networking accounts like Gmail, Facebook, Instagram or Twitter (Bansal et al., 2012). Users log in by authenticating their social media account to the platform which reduces the number of passwords and accounts (Gafni & Nissim, 2014). By using social login, personal information from their social media profile as users age, gender, name, profile picture, location, networks, friends list, and user id will always be shared. Third-parties also receive access to user's personal information from their social media profiles when using social login (Kontaxis et al., 2012; Krasnova et al., 2014). Platforms can request additional profile information such as relationship status, users' likes, political and religious preferences, location history, and photos (Kontaxis et al., 2012; Krämer, Schnurr, & Wohlfarth, 2019; Krasnova et al., 2014). Social login ensures that online companies can develop a better view of the customer (Lariviere et al., 2013). The more personal data being shared, the greater the privacy risks. Therefore, there are growing concerns about the effect of social login on privacy concerns and app adoption (Kontaxis et al., 2012; Krasnova et al., 2014).

Interestingly, social login offers companies more additional customer information and is less private and secure compared to general login (Gafni & Nissim, 2014; Kontaxis et al., 2012). Therefore, important is that if users need to provide irrelevant or sensitive information during the registration or login process, users experience lower trust, more privacy risks, and are more likely to register (Li & Pavlou, 2013; Sharma & Crossler, 2014). To gain trust, m-commerce organizations need to understand consumers' privacy risks perceptions towards m-commerce apps (Nilashi et al., 2015). On top of these findings, previous research found that social login mechanisms have not always been secure (Gafni & Nissim, 2014). Relating all these findings to the context of this study, one could say that when offering general login and social login, general login is more secure, decreases privacy risk perceptions, and leads to higher trust in the m-commerce app.

2.5 Country of origin of the app (EU vs non-EU)

Previous research has shown that consumers' privacy perceptions and concerns vary in each country (Piao, Li, Pan, & Zhang, 2016; Adelola, Dawson, & Batmaz, 2014). In some countries outside the European Union (EU), privacy is not even seen as a fundamental human right (Adelola et al., 2014). Whereas in May 2018, the EU introduced the General Data Protection Regulation (GDPR), a new privacy law which introduced new individual data and privacy rights and gave firms stronger rules about handling personal data (Goldberg et al., 2019). These differences influence the data protection procedures of each country and determine the effectiveness of the countries data protection (Adelola et al., 2014). Besides, m-commerce organizations need to develop secure apps who are trustworthy in privacy and security (Ling et al., 2010; Kidane & Sharma, 2016). Gupta & Dubey (2016) argue that consumers' view of security concerning personal data handling particularly influences their trust in m-commerce. Eventually, all m-commerce apps should be able to fully protect consumers' data and privacy.

EU

To date, EU-inhabitants are much more worried about data breaches than data sharing (Sheth, Kaiser, & Maalej, 2014). Since Dutch people are the focus group of this study, research from TNO (2015) reveals that 82.5% of the Dutch population attach great importance to privacy and the protection of personal data. Many of them are reluctant to share personal data if the purpose or necessity is not entirely clear (TNO, 2015). Besides, the EU constitution describes the right to privacy and the EU is a worldwide leader when it comes to privacy regulation. The GDPR gave EU civilians new and improved data rights and placed new responsibilities on businesses, especially to data-processing firms. The collection, processing, and use of personal data of EU citizens, and of customers from EU-based organizations and organizations with EU offices are protected by the GDPR. This restricts the way companies can use personal data and specifies and defines privacy rights. Organizations can process personal data only under specific and limited conditions. They need to minimize the collection and processing of personal data and have to anonymize and encrypt personal data (Goldberg et al., 2019). Due to the GDPR, personal data is very well protected which increases consumers' trust and decreases consumers' privacy risks (Broutsou & Fitsilis, 2012; Sharma & Crossler, 2014).

Non-EU

Outside the EU, many different privacy laws have been established and some countries do not even see privacy as a fundamental human right (Adelola et al., 2014). From the list of top 53 countries by Gross Domestic Product (GDP), eight non-EU countries do not have data privacy laws including China and the United States (Greenleaf, 2018b). When looking at China, they are becoming the global capital of m-commerce apps (Kshetri, Williamson, & Bourgoin, 2006). Despite their large share in m-commerce, China's 2016 Cybersecurity Law still misses several common data privacy law elements, such as explicit user data access rights, certain sensitive data conditions, and authority for data protection. This means that one of the most fundamental components of a data privacy law is not present in China (Greenleaf, 2018b). Russia also has several data privacy laws and data protection laws

(Zharova & Elin, 2017). Similar to China, these laws do not provide sufficient protection. These laws do not govern the relationship among consumers and the firms gathering and making use of their data. This results in Russian organizations in creating their enforcement policies of the legal data protection standards based on their interpretation of the law. This makes the exploitation of personal data a serious hazard, especially for Russian citizens (Zharova & Elin, 2017). Since the security of data is a reliable predictor of the intention to use m-commerce (Blaise et al., 2018; Eastin et al., 2016), one could say that non-EU apps have lower registration intentions due to the lack of consumer data protection. This demonstrates that apps from outside the EU result consumers in having lower trust and higher privacy risk perceptions, and lower intentions to register in the m-commerce app.

Regardless of the country of origin of the app, m-commerce apps need to be private, safe, and trustworthy (Kidane & Sharma, 2016). As a result of different privacy laws globally, not all m-commerce apps meet these requirements. The GDPR protects personal data from consumers that use apps from EU-based organizations and organizations with EU offices very well, which positively influences consumers' trust, and negatively influences their privacy risk perceptions. Besides, countries outside the EU use less useful privacy and data protection laws (Broutsou & Fitsilis, 2012; Sharma & Crossler, 2014). Since European m-commerce apps deal with stronger privacy and data protection regulations compared to apps from outside the EU, apps from the EU are much more private and secure. This influences consumers' trust in the app and their privacy risk perceptions. As the security of data is a reliable predictor of the intention to use m-commerce, EU apps could also positively influence consumers' intention to register. This results in lower consumers' trust in the app, higher privacy risks perceptions, and a lower intention to register in non-EU apps. Besides, the high amount of personal information social login needs from the user, and the fact that third parties are involved makes social login less trustworthy, private, and secure compared to general login (Gafni & Nissim, 2014; Kontaxis et al., 2012). This means for the study at hand that consumers, who use m-commerce apps from outside the EU, will trust the app higher when the general login type is used compared to social login. Therefore, it is interesting to also study the interacting effect of country of origin.

Based on the basis described above, the following hypotheses can be drawn up:

> ***H1:*** *Consumers' trust in an m-commerce app is higher when a general login type is used compared to when a social login type is used.*
> ***H2:*** *Consumers' level of privacy risk perception is higher when an m-commerce app uses a social login type than when a general login type is used.*
> ***H3:*** *Consumers' trust in an m-commerce app is higher when that app is from the EU compared to an app that is from outside the EU.*
> ***H4:*** *Consumers' privacy risk perceptions are higher when that app is from outside the EU compared to an app that is from the EU.*
> ***H5:*** *Consumers' intention to register to an m-commerce app is higher when that app is from the EU compared to an app that is from outside the EU.*
> ***H6:*** *Trust in the m-commerce app decreases privacy risk perceptions.*
> ***H7:*** *Trust in the m-commerce app increases the intention to register.*
> ***H8:*** *Higher levels of privacy risk perceptions will negatively influence consumers' intention to register to an m-commerce app.*
> ***H9:*** *Consumers' trust in an m-commerce app that uses a social login type is higher when that app is produced in the EU when compared to consumers' trust in an app that uses a social login type but is produced outside of the EU.*

2.6 The interaction effect of privacy statement consent (passive vs. active)

As a result of the variety of login types and the increasing amount of data collection, the factors trust, privacy, and security become more important. According to Wu et al. (2012), the main issue for digital organizations is to face consumers' concerns about the exploitation of personal information. As a result, data safety and data abuse are very important elements related to trust (Broutsou & Fitsilis, 2012). To make the consumer trust the app and register, privacy and security issues must be minimal (Gupta & Dubey, 2016). Privacy in particular strongly influences consumers' trust in the m-commerce organization (Liu, Marchewka, Lu, & Yu, 2005). Pan and Zinkhan (2006) and Wu et al. (2012) argue that sites are considered as less trustworthy when the privacy statement is missing. The privacy statement is an informative description to consumers of how personal information is collected, used, and treated by the website or app (Wu et al., 2012; Lauer & Deng, 2007 & Liu et al., 2005).

Therefore, consumer trust in the online environment can be built by making use of privacy assurances such as privacy statements (Bansal et al, 2015; Pan & Zinkhan, 2006). Moreover, the perceived adequacy of the privacy statement influences consumers' trust in the online environment (Bansal et al., 2015). When incorporating privacy statement notice and consent choice into the design of the online environment, consumers' trust and their behavioural intention will increase (Liu et al., 2005). According to Liu et al. (2005), the presence of a privacy policy or notice could even result in more repeat visits and more purchases. In fact, several privacy notices have different influences on consumers' trust in the online environment.

Passive consent

Multiple factors concerning privacy statements and privacy notices have an influence on consumers' trust in the online environment. Both the presence and strength of the privacy statement and privacy notice influence consumers' trust (Liu et al., 2005; Schlosser, White, & Lloyd, 2006). The study of Schlosser et al. (2006) claims that consumers' level of trust in the online environment decrease when receiving weak or no notices. In addition, privacy notices must attract attention so that consumers tend to read it (Luzak, 2014). Trust increases when consumers are actively notified to the privacy policy, meaning that passive notices have a more negative effect on consumers' trust (Lauer & Deng, 2007). This means that m-commerce organizations who are passively notifying consumers by making use of passive privacy statement consent will be less trusted by consumers.

Active consent

When consumers are actively attended on the privacy statement or privacy notice, their trust will increase (Lauer & Deng, 2007; Liu et al., 2005). Providing consumers with strong privacy notices increases their trust level (Schlosser et al., 2006). Besides, incorporating a privacy statement notice and choice into the app increases consumers' trust in the online environment (Liu et al., 2005). Organizations should make people inclined to read the privacy notice by drawing consumer's attention to the privacy notice (Luzak, 2014). The more straightforward the notice, the higher consumers' trust (Luzak, 2014; Milne & Culnan, 2004). Furthermore, online platforms create a positive reputation when using credible and transparent privacy statements (Milne & Culnan, 2004). Thereby, many people often or always look for opt-in or opt-out checkboxes online (Custers, van der Hof, & Schermer, 2014). This means that consumers will have higher trust in the m-commerce app when active privacy statement consent is incorporated.

By using active privacy statement consent, consumers are actively warned for the privacy statement and actively asked for consent. This shows the online platform cares about the users' privacy (Lauer & Deng, 2007). Through making use of active privacy statement consent, consumers' trust in the app increase (Lauer & Deng, 2007; Liu et al., 2005). Since the type of privacy statement consent, privacy, and security influence consumers' trust and feeling of privacy, the effect of login type on trust in the app will be influenced by privacy statement consent. Particularly with social login, consumers will have higher trust in the app when active consent is used, since active consent increase consumers' trust and social login is less private and secure compared to general login. That means for the study at hand that consumers who use social login have higher trust in the online environment when active consent is presented instead of passive consent. Therefore, it is interesting to test the interaction effect of privacy statement consent on the relationship between login type and trust in the app.

> ***H10:*** *Consumers' trust in an m-commerce app is higher when a social login type is used alongside an active privacy consent than when using a social login type alongside a passive privacy consent.*

2.7 The interaction effect of privacy valuation

Another important variable within this study is privacy valuation. Privacy valuation means and measures how much individuals truly value their personal information and information privacy (Adar, Fine, & Huberman, 2005). In the digital age, privacy is a key concern as internet users show serious concerns about the collection and use of personal data and their privacy (Kokolakis, 2017). But each person has its own desired amount of privacy (Trust, Kannan, & Peng, 2002). Consumer trust is even influenced by the amount of privacy digital platforms offer to its users (Gupta & Dubey, 2016). Not all businesses are effective in data protection which is important for most consumers to know when sharing personal data (Sidgman & Crompton, 2016). Besides, each person differs in their valuation of personal data and their willingness to trade their privacy (Morando, Iemma, & Raiteri, 2014; Ponciano, Barbosa, Brasileiro, Brito, & Andrade, 2017). Therefore, consumers are divided into three groups when it comes to their privacy attitudes: privacy fundamentalists, privacy pragmatists, and privacy unconcerned. Privacy fundamentalists are generally unwilling to share personal information, they highly value their privacy. Privacy pragmatists are willing to share reasonable amounts of personal information as long as it is used to their benefit, they attach medium value to their privacy. The privacy unconcerned have no concerns about the collection and use of personal information and are likely to share personal information, they do not attach value to their privacy (Ponciano et al., 2017). The amount of privacy a platform offers influences consumers' trust. People who do not care about their privacy are still likely to trust the platform and login, even when the platform and login type offer no privacy. When using social login, people who highly value their privacy will have low levels of trust in the app as social login offers lower privacy to its users compared to general login. It is expected that the use of social login in combination with low privacy valuation leads to an increased level of trust in the app, whereas high privacy valuation would result in the opposite. Therefore, it is interesting to test the interaction effect of privacy valuation on the relationship between login type and trust in the app.

> ***H11:*** *Consumers' trust in an m-commerce app is higher when a social login type is used when having low privacy valuation than when using a social login type and having high privacy valuation.*

2.8 The mediating role of trust and privacy risk perception

Besides the direct effect of login type on trust and privacy risk perception, the intention to register in the app is expected to be influenced by the login type mediated by trust and by privacy risk perception. Leon et al. (2015) and Li and Pavlou (2013) claim that when users consider the information they have to share as sensitive or unnecessary, consumers are less likely to disclose personal information which means that they have a lower intention to register in the app. People will be less likely to register, the more information the platform asks (Hui, Teo, & Lee, 2007). This means for this study that the login type that requires unnecessary, high amounts and sometimes sensitive personal information influence consumers' intention to register. Besides, trust and privacy risk perceptions influence consumers' intention to register and usage intention as well (Basarir-Ozel & Mardikyan, 2017; Li & Pavlou, 2013). When consumers consider information as sensitive or unnecessary, their trust level decrease, and their risk perceptions increase which in the end influences consumers' intention to register (Li & Pavlou, 2013; Malhotra, Kim, & Agarwal, 2004). Building on the aforementioned theory, the effect of login type on consumers' intention to register is expected to be mediated by trust and by privacy risk perception. It is expected that the social login type which requires sensitive and high amounts of personal information results in lower trust and higher privacy risk perceptions and a lower intention to register in the app.

> ***H12a:*** *Trust in an m-commerce app mediates the effect of a login type on users' intention to register to an m-commerce app.*
> ***H12b:*** *Privacy risk perception mediates the effect of a login type on users' intention to register to an m-commerce app.*

2.9 Research model

Several hypotheses are based on literature, derived from the theoretical framework. An overview of all the hypotheses of this study can be found in table 1 below.

Table 1. Hypotheses overview

	Hypothesis
H1	Consumers' trust in an m-commerce app is higher when a general login type is used compared to when a social login type is used.
H2	Consumers' level of privacy risk perception is higher when an m-commerce app uses a social login type than when a general login type is used.
H3	Consumers' trust in an m-commerce app is higher when that app is from the EU compared to an app that is from outside the EU.
H4	Consumers' privacy risk perceptions are higher when that app is from outside the EU compared to an app that is from the EU.
H5	Consumers' intention to register to an m-commerce app is higher when that app is from the EU compared to an app that is from outside the EU.
H6	Trust in the m-commerce app decreases privacy risk perceptions.
H7	Trust in the m-commerce app increases the intention to register.
H8	Higher levels of privacy risk perceptions will negatively influence consumers' intention to register to an m-commerce app.
H9	Consumers' trust in an m-commerce app that uses a social login type is higher when that app is produced in the EU when compared to consumers' trust in an app that uses a social login type but is produced outside of the EU.
H10	Consumers' trust in an m-commerce app is higher when a social login type is used alongside an active privacy consent than when using a social login type alongside a passive privacy consent.
H11	Consumers' trust in an m-commerce app is higher when a social login type is used when having low privacy valuation than when using a social login type and having high privacy valuation.
H12a	Trust in an m-commerce app mediates the effect of a login type on users' intention to register to an m-commerce app.
H12b	Privacy risk perception mediates the effect of a login type on users' intention to register to an m-commerce app.

Based on the hypotheses and theoretical framework, the proposed research model is created and shown below in figure 1.

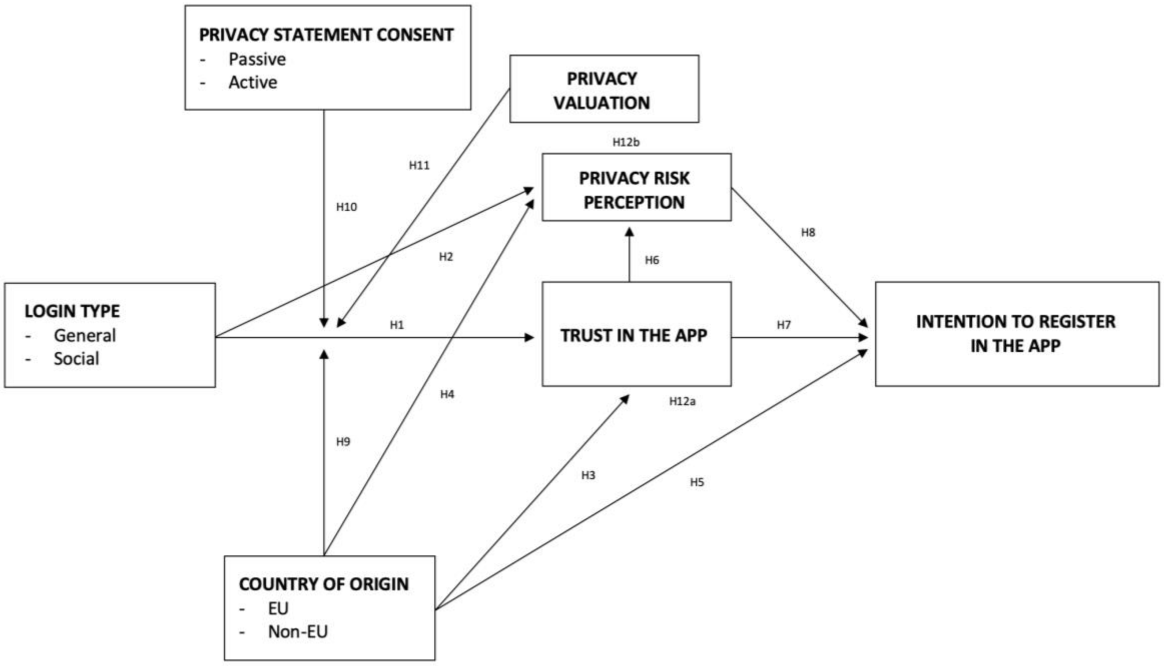


Figure 1. Research model

3. METHODOLOGY

For this study, the research model was tested using data collected with an online experiment. It included items to measure the research model constructs. This is used to test the hypotheses and answer the research questions. This chapter presents an overview of the research design, instruments, measures and manipulations used in this study.

3.1 Research design

The objective of this study is to research the influence of different login types on consumer' trust in m-commerce apps, privacy risk perceptions, and their intention to use the app. The interaction effect of privacy statement consent and country of origin of the app were the main interacting effects to be tested. To answer the research questions and test the research hypotheses, an experimental 2 (Login type: general vs social) x 2 (Privacy statement consent: passive vs active) x 2 (Country of origin: EU vs non-EU) design was used. The independent variables are login type, privacy statement consent, and country of origin. This method examined the effects of manipulated material. In this study, the effects of the three manipulated independent variables on the three dependent variables trust in the app, privacy risk perception, and intention to register in the app were tested. The experiment was conducted online. A quantitative digital experimental survey was used. The independent variables were manipulated to test their influence on the dependent variables. The dependent variables were tested by measurement statements for each dependent variable. In total there were eight experimental conditions. Each respondent saw only one experimental condition and based on that he or she filled in the online questionnaire. The experimental conditions are shown in table 2.

Table 2. Experimental conditions

Condition	Login type	Privacy statement consent	Country of origin
Condition 1	General	Passive	EU
Condition 2	General	Active	EU
Condition 3	General	Passive	Non-EU
Condition 4	General	Active	Non-EU
Condition 5	Social	Passive	EU
Condition 6	Social	Active	EU
Condition 7	Social	Passive	Non-EU
Condition 8	Social	Active	Non-EU

3.2 Experimental materials

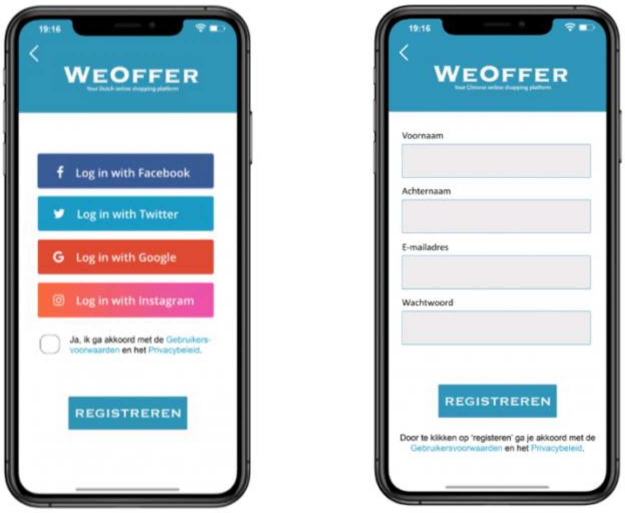
To be able to measure the effects of the independent variables of the 2 x 2 x 2 experimental design, the three independent variables were manipulated. A digital questionnaire was used to test the research design by using 8 different manipulated experimental conditions. The experimental material contained eight different versions of the case description and a screenshot, which can be found in Appendix A. Each respondent saw one of these eight cases and one screenshot.

In order to create a trustworthy but fictional m-commerce app, the design was based on literature. The colour blue has an impact on trust, security, credibility, and loyalty and could increase users' trust (Sasidharan, 2010). (Alberts & van der Geest, 2011) argues that the colour blue is the most trustworthy in a web context. Since the focus of the study is on trust in the app, the app design was blue. The cases consisted of a fictional m-commerce app called 'WeOffer' to ensure that the effects of manipulations were not influenced by predetermined attributes.

First, the independent variable login type was manipulated by offering participants general login or social login. Four of the cases and screenshots consisted of a general login menu type in which the user could only login by creating an account for the specific platform by using a first name, surname, email address, and password. The other four cases and screenshots consisted of a manipulation with a social login menu where the user was able to log in by using their Facebook, Google, Twitter or Instagram account.

Second, the independent variable privacy statement consent was manipulated by providing participants one of the two variations, passive or active privacy statement consent. Four of the cases and screenshots consisted of a passive privacy statement consent notice in which only a hidden privacy notice was given on the bottom of the page. The other four cases and screenshots consisted of an active privacy statement consent notice in which participants had to click a privacy notice checkbox.

Third, the independent variable country of origin of the app was manipulated by offering participants one of the two country of origin options, EU and non-EU. Four of the cases and screenshots consisted of an EU m-commerce app in which the app was from a Dutch company. The other four cases and screenshots consisted of a non-EU app in which the app was from a Chinese company. After reading the case and viewing the screenshot, respondents had to fill in the survey. Figure 2 demonstrates the screenshots of two experimental conditions that were used in this research.



□ Ja, ik ga akkoord met de Gebruikers-voorwaarden en het Privacybeleid.

Door te klikken op 'registeren' ga je akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

Figure 2. Examples of two experimental conditions

To test whether the manipulations were experienced by the participants, several manipulation check questions were asked at the end of the survey. To check the login type manipulation, participants were asked whether they had to log in with a general or social login during the online experiment. To check the manipulation of the type of privacy statement consent, participants were asked if they had to explicitly accept the privacy statement and if they had to check the privacy statement checkbox. To check the manipulation of the country of origin of the app, participants were asked whether the app they were shown was from China or the Netherlands. Participants who answered the manipulation check questions incorrectly because their answer did not match the condition they were assigned to were not included in the analysis. The manipulation check questions are provided in the survey in Appendix B.

3.3 Constructs validity and reliability

The research model was tested by collecting data with an online experimental questionnaire that measured four constructs. To measure these constructs, scales from existing literature were selected. These scales already have been extensively used in e-commerce and m-commerce studies and in online privacy studies. The reliability and validity of these scales also have been proven. The phrasing of the scales is sometimes adapted to fit the exact context of this study. The questionnaire used statements that were answered on a 7-point Likert scale ranging from strongly disagree to strongly agree. The 7-point Likert scale provided a wider variety of options which increases the probability of measuring people's objective reality (Joshi, Kale, Chandel, & Pal, 2015). A factor analysis was conducted for the measurements and can be found in table 3. All items loaded in the scales as proposed. When an item loaded a value below .60, the item was deleted to improve validity. Therefore, one item was deleted resulting in a total of 23 items for four constructs. Cronbach's alpha was also determined to measure each construct validity. A construct was considered as reliable if the Cronbach's alpha has a minimum value of 0.70. Values of 0.80 or higher indicate high reliability (Tilburg University, n.d.). The lowest measured construct value is .74, and the highest value was .94. Table 3 shows that all four variables were reliable constructs with all minimal Cronbach's alpha (α) values of .74. An overview of all measurement items can be found in Appendix C.

Table 3. Factor analysis measurement with 23 items for 4 constructs

Construct	Item	PV	PRP	TR	INT
Privacy valuation α: .74	Compared to others, I am more sensitive about the way online companies handle my personal information.	.82			
	To me, it is most important to keep my privacy intact from online companies.	.69			
	I am concerned about threats to my personal privacy today.	.80			
Privacy risk perception α: .85	It would be risky to disclose my personal information to this app.		.76		
	There would be high potential for privacy loss associated with disclosing personal information to this app.		.74		
	There would be too much uncertainty associated with disclosing my personal information to this app.		.73		
	Providing this app with my personal information would involve many unexpected problems.		.63		
	My personal information could be inappropriately used by this app		.62		
Trust in the app α: .94	I believe that WeOffer would act in my best interest			.72	
	If I required help, WeOffer would do its best to help me			.77	
	WeOffer is interested in my well-being, not just its own			.77	
	I perceive that WeOffer is trustful in its dealings with me			.80	
	I would characterize WeOffer as honest			.73	
	I perceive that WeOffer would keep its promises and commitments			.78	
	I perceive that WeOffer to be sincere and genuine			.80	
	I believe WeOffer is capable of protecting my personal data.			.77	
	WeOffer performs its role of protecting my personal information very well			.81	
	Overall, WeOffer is a capable and proficient organization.			.81	
	In general, WeOffer is very knowledgeable about the privacy law			.69	
Intention to register α: .89	I am likely to register in the app				.89
	I will probably register in the app				.87
	I think I would possibly share personal information with the app.				.76
	I am not willing to register in the app.				.69

Privacy valuation

Privacy valuation was measured by applying the scale of Li, Sarathy and Xu (2011). Li et al. (2011) used the term general privacy concerns and described it as the general tendency to worry about information privacy. This construct consisted of three items with a Cronbach's alpha of .74.

Privacy risk perception

To measure privacy risk perception, the scale of Malhotra et al. (2004) was used. They have used these scales in a study regarding internet users' information privacy concerns. Their model has been proven to be a useful tool for analysing online consumers' reactions to a variety of online privacy threats (Malhotra et al., 2004). Privacy risk perception consisted of five items and reached a Cronbach's alpha of .85.

Trust in the app

Trust in the app was measured by 11 statements derived from McKnight et al. (2002). They conceptualized trust in the dimension's benevolence, integrity, and competence, especially for e-commerce contexts. Benevolence stands for the caring and motivation to act in the trustor's interests. Integrity stands for the honesty and keeping of promises. Competence stands for the trustees' ability to do what the trustor needs. This construct consisted of 11 items with a Cronbach's alpha of .94.

Intention to register in the app

To measure the intention to register in the app, the scale of Li et al. (2011) and Malhotra et al. (2004) was used. Malhotra et al. (2004) used this scale to measure behavioural intention towards releasing personal information at the request of a marketer. Li et al. (2011) used this scale to measure the intention of online consumers to disclose personal information to unfamiliar online vendors. The original four seven-point semantic scales of Malhotra et al. (2004) have been changed into four statements with seven-point Likert scales. The construct intention to register came up with a Cronbach's alpha of .89 and consisted of four items.

3.4 Pre-test

Before the final version of the survey was distributed, a pre-test was conducted with 10 participants. The participants were able to give recommendations about the design, formulations, and experimental conditions. After the pre-test, several adjustments were made based on the given recommendations. The phrasing of several statements has been adjusted.

3.5 Participants

Participants were gathered by using the convenience sampling method as it is easy, fast, cheap, and the participants were directly available via the researchers' network. As the research focused on Dutch millennials, also called generation Y, participants needed to be Dutch and between 18 and 40 years old. This research focused on millennials as they have been recognized as the driving force of online shopping (Smith, 2012). The survey was offered in Dutch, the native language of the target group. Participants were not required to be familiar with m-commerce. The total millennial population in the Netherlands consists of 4.000.000 people (Motivaction, n.d.). Each experimental condition needed to include 25 valid respondents, this resulted in a sample size of n = 8 x 25 = 200. Participants were randomly and evenly assigned to the eight experimental conditions. In total, N = 212 valid respondents took part in this research of which 107 (50,5%) male and 105 (49,5%) female. Table 4 shows the demographic distribution across the eight conditions.

The mean age is 24 years and participants' age ranged from 17 to 40 years. Besides, 58.5% has HBO as their current or highest level of education. Table 4 provides an overview of the distribution of the education level in each condition. Low education includes vmbo and MBO education levels, high education includes havo, vwo, HBO, and WO. Participants who used apps on their smartphone or tablet daily formed the biggest part with 99,5%. Only 21,7% of the participants never used shopping apps on their smartphone or tablet, 14,2% daily, 38,7% weekly, and 25,5% monthly. Participants who indicated that they make purchases via shopping apps on their smartphone or tablet, either daily, weekly, monthly or several times a year, account for 81,6% of the sample. Only 18,4% of the participants never made purchases by using a shopping app on their smartphone or tablet. To get insight into the experience of the participants with m-commerce apps, they were asked how many shopping apps they have installed on their smartphone or tablet. Even 79,2% of the participants have installed between 1 or more shopping apps on their smartphone or tablet. Only 20,8% of the participants have no shopping apps installed on their smartphone or tablet.

Table 4. Demographics of the eight conditions

Condition	N =	Age (SD)	Gender	Education
1: General + Passive + EU	26	24 (2.44)	61.5% (m) / 38.5% (f)	7.7% (low) / 92.3% (high)
2: General + Active + EU	27	24 (2.11)	59.3% (m) / 40.7% (f)	11.1% (low) / 88.9% (high)
3: General + Passive + Non-EU	28	24 (3.96)	50% (m) / 50% (f)	7.1% (low) / 92.9% (high)
4: General + Active + Non-EU	29	25 (3.44)	51.7% (m) / 48.3% (f)	10.3% (low) / 89.7% (high)
5: Social + Passive + EU	24	24 (4.27)	37.5% (m) / 62.5% (f)	16.7% (low) / 83.3% (high)
6: Social + Active + EU	25	24 (3.54)	48% (m) / 52% (f)	0% (low) / 100% (high)
7: Social + Passive + Non-EU	26	23 (3.67)	42.3% (m) / 57.7% (f)	11.5% (low) / 88.5% (high)
8: Social + Active + Non-EU	27	24 (3.47)	51.9% (m) / 48.1% (f)	18.5% (low) / 81.5% (high)
Total	212	24 (3.39)	50.5% (m) / 49.5% (f)	10.4% (low) / 89.6% (high)

3.6 Procedure

The survey was created using the online survey software Qualtrics and spread using non-probability sampling via the convenience sampling method. To collect suitable respondents, an anonymous survey link was sent to millennials using Facebook, Facebook messenger, and WhatsApp. They were asked if they were willing to participate in an online questionnaire regarding an m-commerce app. The questionnaire consisted of 37 items in total, including statements, control questions, and demographics. All dependent variables were tested by asking respondents to indicate for each statement to what extent they agreed upon the statements on a seven-point Likert scale varying from totally disagree to totally agree. Due to the 2 x 2 x 2 experimental design, participants only saw one of the eight manipulated experimental conditions.

The experiment started with an introduction text with information about the study, their voluntary participation, and the data collection procedure. Then, privacy valuation was measured by 3 statements. Next, one of the eight manipulated cases were shown with a described scenario and a corresponding screenshot of a fictional m-commerce app. Then, privacy risk perception, trust in the app, and intention to register in the app were measured. After answering the statements, the manipulated case and screenshot was shown again, followed by five questions for a manipulation check. The last part of the survey consisted of four questions about their m-commerce app usage, followed by four demographic questions. After finishing the questionnaire, a thank you message was shown. The survey can be found in Appendix B.

4. RESULTS

The main focus of the study is on the effects of the independent variable login type, and the interaction variables privacy statement consent, country of origin, and privacy valuation on trust, privacy risk perception and intention. This chapter presents the analyses and interpretation of the results. In order to test different hypotheses, a multivariate analysis of variance (MANOVA) is conducted. MANOVA explains if there are statistically significant differences in means among groups. Several other hypotheses were tested through univariate analysis. To investigate mediation, PROCESS by Andrew F. Hayes was used (Demming, Jahn, & Boztug, 2017).

To investigate the different effects of the independent variables on the dependent variables, a Wilks' Lambda test was conducted. Wilks' Lambda scores (Λ) showed no significant main effect for login type on the dependent variables, with Λ = .99, F = 1.44, p = .232. Wilks' Lambda values showed significant results for the effects of country of origin (Λ = .86, F = 10.86, p = < .001) and privacy valuation (Λ = .77, F = 19.07, p = < .001) on the dependent variables. There are no significant results for the interaction effects of login type and privacy statement consent (Λ = 1, F = .03, p = .993), login type and country of origin (Λ = .99, F = .67, p = .573), and login type and privacy valuation (Λ = .99, F = .83, p = .477) on the dependent variables. This means the interaction effect hypotheses are not significant. See Table 5 and Table 6 for the multivariate results of the independent variables.

Table 5. Multivariate results of independent variables

	Λ	F	p
Login type	.978	1.441	.232
Privacy valuation	**.772**	**19.072**	**.000**
Country of origin	**.856**	**10.857**	**.000**
Login type * Privacy statement consent	1.000	.029	.993
Login type * Country of origin	.990	.667	.573
Login type * Privacy valuation	.987	.834	.477

Table 6. Multivariate results of independent variables on the dependent variables

		F (p)	
	Trust	**Privacy risk perception**	**Intention to register**
Login type	.14 (.708)	3.87 (.051)	1.68 (.196)
Privacy valuation	**13.82 (.000)**	**57.04 (.000)**	**11.79 (.001)**
Country of origin	**2.31 (.000)**	**22.09 (.000)**	**7.19 (.008)**
Login type * Country of origin	.18 (.671)	2.00 (.160)	.38 (.539)
Login type * Privacy statement consent	.02 (.880)	.01 (.911)	.02 (.891)
Login type * Privacy valuation	1.32 (.253)	.27 (.607)	.00 (.956)

The following section discusses the main effect, interaction effect, and mediation effect hypotheses. The results indicate which hypotheses are supported and which are not supported. An alpha value of .05 and below is applied to the significant outcomes. The results can be found in Table 6, further analysis of these effects can be found below.

4.1 Main effects

4.1.1 Main effects of login type

H1 was not supported. Table 6 shows there is no significant effect for the main effect of login type on trust in the app. It was expected that the general login type would result in higher trust in the app compared to the social login type. The difference in mean scores on trust between general login (M = 3.90, SD = .10) and social login (M = 3.85, SD = .11) is not significant (F = .14, p = .708). The overall mean scores for the effect of login type on trust are shown in Table 7. This means the login type does not significantly influence consumers' trust.

H2 was not supported. It was expected that social login resulted in higher consumers' privacy risk perceptions compared to general login. Table 6 shows there is no significant effect for the main effect of login type on privacy risk perceptions. The difference in mean scores between general login (M = 4.02, SD = .10) and social login (M = 4.30, SD = .11) on privacy risk perception is just not significant (F = 3.87, p = .051). This means the type of login does not have a significant effect on consumers' privacy risk perceptions. Table 7 shows the overall mean scores for the effect of login type on privacy risk perception.

Table 7. Descriptives for login type on the dependent variables

	Mean (SD)		
	Trust	**Privacy risk perception**	**Intention to register**
General	3.90 (.10)	4.02 (.10)	4.17 (.14)
Social	3.85 (.11)	4.30 (.11)	3.91 (.14)

4.1.2 Main effects of country of origin

H3 was supported. The country of origin of the app had a significant main effect on consumer' level of trust in the app as shown in Table 6. The difference is significantly proven by MANOVA (F = 23.97, p = < .001). Table 8 shows the mean scores for trust in the app differ for the country of origin. It was expected that apps from the EU would gain higher trust compared to apps from outside the EU. The level of trust for apps from the EU increases when using an app from outside the EU the level of trust decreases. The mean for trust when using an app from the EU (M = 4.23, SD = .11) is significantly higher than for apps from outside the EU (M = 3.52, SD = .10). These results show that consumers have significantly higher trust in apps from the EU.

H4 was supported. It was expected that non-EU apps would result in higher levels of privacy risk perceptions compared to EU apps. The country of origin of the app had a significant main effect on privacy risk perception (F = 22.09, p = < .001) as shown in Table 6. A non-EU app resulted consumers in having higher privacy risk perceptions (M = 4.50, SD = .10) and is significantly different than an EU app (M = 3.82, SD = .10) as shown in Table 8. The results show that when using an app from the EU app, consumers' privacy risk perceptions are lower compared to when using an app from outside the EU app.

H5 was also supported. It was expected that EU apps would result in higher intention rates compared to non-EU apps. Table 6 shows the country of origin of the app had a significant main effect on consumers' intention to register in the app. The difference is significantly proven by MANOVA (F = 7.19, p = .008). This shows that the mean scores for the dependent variable intention to register in the app significantly differ between EU and non-EU. The mean for consumers' intention to register when using an app from the EU (M = 4.31, SD = .14) is higher than when using an app from outside the EU (M =3.78, SD = .14) as shown in Table 8. These results show that when using an app from the EU, consumers' intention to register in the app is significantly higher compared to when using an app from outside the EU.

Table 8. Descriptives for country of origin on dependent variables

	Mean (SD)		
	Trust	**Privacy risk perception**	**Intention to register**
EU	4.23 (.11)	3.82 (.10)	4.31 (.14)
Non-EU	3.52 (.10)	4.50 (.10)	3.78 (.14)

4.1.3 Main effects of trust and privacy risk perception

H6 was supported. Simple linear regression was used to test the effect of trust in the m-commerce app on privacy risk perception. A single regression with privacy risk perception as a dependent variable and trust in the app as dependent variable is found to be significant (β = -.54; t (210) = -8.45; p < .001). These results reveal that trust in the app is a significant negative predictor of consumers' privacy risk perceptions. This means the higher consumers' trust in the app, the lower consumers' privacy risk perceptions.

H7 was supported. To test the effect of consumers' trust in the m-commerce app on consumers' intention to register in the app, a simple linear regression analysis was performed. This analysis shows that trust in the app is a significant predictor of intention to register in the app with a significant positive regression coefficient (β = .61; t (210) = 7.83; p < .001). These results show that consumers' trust in the m-commerce app has a significant positive effect on their intention to register in the app. This means the higher consumers' trust in the app, the higher their intention to register in the app.

H8 was supported. Simple linear regression was used to predict intention to register in the m-commerce app from consumers' privacy risk perceptions. This regression analysis shows that privacy risk perception is a significant predictor of consumers' intention to register in the m-commerce app with a significant negative regression (β = -.68; t (210) = -9.94; p < .001). This means that privacy risk perception negatively influences the intention to register in the app. The higher consumers' privacy risk perceptions, the lower consumers' intention to register in the app.

4.2 Interaction effects

4.2.1 The interaction effect of login type and country of origin

H9 was not supported. It was expected that there was an interaction effect between the two variables login type and country of origin on trust. MANOVA showed there is no significant interaction effect of login type and country of origin on trust in the app (F = .18, p = .671) as shown in Table 6. It was expected that social login resulted in more trust in the app when the app is from the EU compared to when the app is from outside the EU. The mean for trust with a social login type and app from the EU is (M = 4.17, SD = .15). When having social login and an app from outside the EU the mean for trust is (M = 3.52, SD = .15). The observed differences were far from significant. Table 9 shows the overall mean scores for the interaction effect between login type and country of origin. It can be concluded there is no significant interaction effect between login type and country of origin on trust in the app.

Table 9. Descriptives for login type * country of origin on the dependent variables

	Mean (SD)		
	Trust	**Privacy risk perception**	**Intention to register**
General * EU	4.29 (.15)	3.58 (.14)	4.50 (.20)
General * Non-EU	3.51 (.14)	4.46 (.14)	3.85 (.19)
Social * EU	4.17 (.15)	4.07 (.15)	4.12 (.21)
Social * Non-EU	3.52 (.15)	4.54 (.15)	3.71 (.20)

4.2.2 The interaction effect of login type and privacy statement consent

H10 was not supported. It was expected that there was an interaction effect between login type and privacy statement consent on trust. Table 6 shows there is no significant interaction effect of login type and privacy statement consent on trust in the app with (F = .02 and p = .880). Results also show that both manipulations with active consent have a higher trust mean compared to both manipulations with passive consent. The overall means and standard deviations for each dependent variable are shown in Table 10. It was expected that social login and active privacy statement consent resulted in higher trust compared to social login and passive privacy statement consent. When using social login, the mean of trust is higher when using active consent (M= 3.95, SD = .15) compared to passive consent (M = 3.75, SD = .15) but the difference is not significant. This means there is no significant interaction effect between login type and privacy statement consent on trust in the app.

Table 10. Descriptives for login type * privacy statement consent on the dependent variables

	Mean (SD)		
	Trust	**Privacy risk perception**	**Intention to register**
General * Passive	3.78 (.14)	4.04 (.14)	4.24 (.20)
General * Active	4.02 (.14)	3.99 (.14)	4.11 (.19)
Social * Passive	3.75 (.15)	4.34 (.15)	4.01 (.21)
Social * Active	3.95 (.15)	4.26 (.15)	3.82 (.20)

4.2.3 The interaction effect of login type and privacy valuation

H11 was not supported. There is no significant interaction effect of login type and privacy valuation on the dependent variable trust in the app. It was expected that people who use social login and have low privacy valuation would have higher trust in the app compared to people who use social login but have high privacy valuation. The overall means and standard deviations can be found in Table 11. In general, people who have a low privacy valuation score a higher mean on trust compared to people who have a high privacy valuation, regardless of the login type. The results show that when using social login, the mean of trust is higher in combination with low privacy valuation (M = 4.03, SD = .15) compared to people with high privacy valuation (M

= 3.66, SD = .15). Table 6 shows there is no significant interaction effect between login type and privacy valuation on trust in the app (F = 1.32, p = .253). This means there is no significant interaction effect between login type and privacy valuation on consumers' trust in the app.

Table 11. Descriptives for login type * privacy valuation on the dependent variables

	Mean (SD)		
	Trust	**Privacy risk perception**	**Intention to register**
Low PV	4.15 (.10)	3.62 (.10)	4.39 (.14)
High PV	3.60 (.11)	4.71 (.11)	3.70 (.14)
General * Low PV	4.26 (.14)	3.51 (.14)	4.51 (.19)
General * High PV	3.55 (.15)	4.53 (.14)	3.84 (.20)
Social * Low PV	4.03 (.15)	3.72 (.14)	4.26 (.20)
Social * High PV	3.66 (.15)	4.89 (.15)	3.57 (.21)

4.3 Mediation effects

4.3.1 Mediation effects of trust and privacy risk perception

H12a was not supported. It was expected that trust in the m-commerce app mediates the effect of login type on the intention to register in the app. In Figure 3, the three different paths are shown. First, path A shows the direct relation between login type and trust in the app. The mediation analysis showed that the effect between login type and the mediator trust in the app is not significant, with b = -.0614, t(212) = -.3907, p = .6964. Second, path B shows the direct relationship between the mediator trust in the app and the intention to register. The mediation process showed that the effect of the mediator (trust in the app) on the intention to register is significant (b = .6107, t(212) = 7.7985, p = < .001). Third, path C' shows the direct effect of login type on the intention to register. This direct effect, ignoring the mediator, showed that login type is not a significant predictor of intention to register, with b = -.2195, t(212) = -1.2308, p = .2198. Last path C, when controlling for the mediator (trust in the app), the independent variable login type was found not to be a significant predictor of intention to register, with b = -.2570, t(212) = -1.2718, p = .2049. These results show that trust leads to a significant change in the intention to register. However, when login type does not predict trust there is no ground for mediation. This means that trust in the app does not mediate the relationship between the login type and the intention to register in the app.

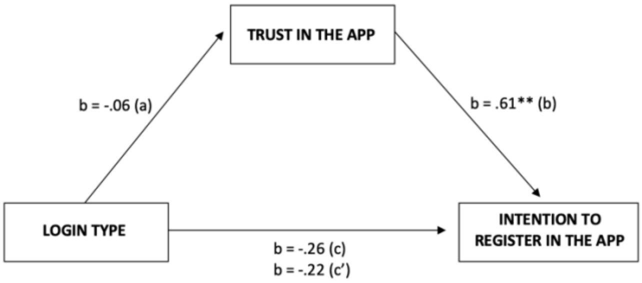


Figure 3. Mediation analysis of login type on intention to register by trust (** p < .001)

H12b was not supported. Possible mediation by privacy risk perception for the effect of login type on the intention to register was investigated. Figure 4 shows three different paths. First, path A shows the direct relation between login type and privacy risk perception. The mediation analysis showed that the effect between login type and the mediator privacy risk perception is not significant, with b = .2912, t(212) = 1.7488, p = .0818. Second, path B shows the direct relationship between the mediator privacy risk perception and intention to register. The mediation process showed that the effect of the mediator (privacy risk perception) on the intention to register is significant (b = -.6812, t(212) = -9.8071, p < .001). Third, path C' shows the direct effect of login type on the intention to register. This direct effect, ignoring the mediator, showed that login type is not a significant predictor of intention to register, with b = -.0586, t(212) = = -.3471, p = .7289. Last path C, when controlling for the mediator privacy risk perception, the independent variable login type was found not to be a significant predictor of intention to register, with b = -.2570, t(212) = -1.2718, p = .2049. These results show that privacy risk perceptions lead to a significant change in the intention to register. However, when login type does not predict privacy risk perception there is no ground for mediation. This means that trust in the app does not mediate the relationship between the login type and the intention to register in the app.

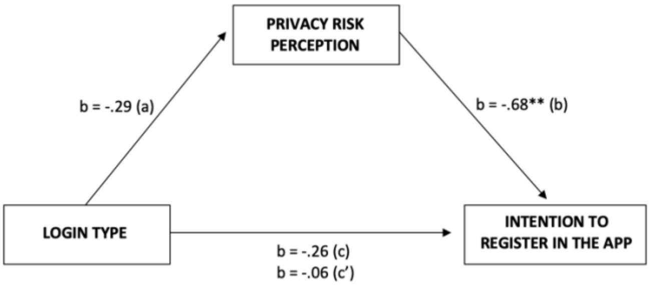


Figure 4. Mediation analysis of login type on intention to register by trust (** p < .001)

A summary of the results of the hypotheses testing section can be found below in Table 12.

Table 12. Hypotheses overview

	Hypothesis	Supported
H1	Consumers' trust in an m-commerce app is higher when a general login type is used compared to when a social login type is used.	No
H2	Consumers' level of privacy risk perception is higher when an m-commerce app uses a social login type than when a general login type is used.	No
H3	Consumers' trust in an m-commerce app is higher when that app is from the EU compared to an app that is from outside the EU.	Yes
H4	Consumers' privacy risk perceptions are higher when that app is from outside the EU compared to an app that is from the EU.	Yes
H5	Consumers' intention to register to an m-commerce app is higher when that app is from the EU compared to an app that is from outside the EU.	Yes
H6	Trust in the m-commerce app decreases privacy risk perceptions.	Yes
H7	Trust in the m-commerce app increases the intention to register.	Yes
H8	Higher levels of privacy risk perceptions will negatively influence consumers' intention to register to an m-commerce app.	Yes
H9	Consumers' trust in an m-commerce app that uses a social login type is higher when that app is produced in the EU when compared to consumers' trust in an app that uses a social login type but is produced outside of the EU.	No
H10	Consumers' trust in an m-commerce app is higher when a social login type is used alongside an active privacy consent than when using a social login type alongside a passive privacy consent.	No
H11	Consumers' trust in an m-commerce app is higher when a social login type is used when having low privacy valuation than when using a social login type and having high privacy valuation.	No
H12a	Trust in an m-commerce app mediates the effect of a login type on users' intention to register to an m-commerce app.	No
H12b	Privacy risk perception mediates the effect of a login type on users' intention to register to an m-commerce app.	No

5. DISCUSSION

This research investigated whether the login type in an m-commerce app influences consumers' trust, privacy risk perceptions, and their intention to register in the app, including the interaction role of the country of origin of the app, privacy statement consent, and privacy valuation. The independent variables consisted of two levels: login type (general vs. social), country of origin (EU vs. Non-EU), and privacy statement consent (passive vs. active). Consumers' level of privacy valuation has been separately investigated for its interaction effect. Eight experimental conditions were created within an online experiment to test and evaluate the influence on trust in the app, privacy risk perception, and intention to register. This section discusses the key findings, practical and theoretical implications, limitations of the research, and recommendations for future research.

5.1 Discussion of results

5.1.1 Discussion of main effects

Based on findings from Li and Pavlou (2013) and Sharma and Crossler (2014), it was expected that social login would result in lower trust and higher privacy risk perceptions compared to general login. Contrary to these expectations, no significant effects were found for the influence of the login type on consumers' trust in the app and their privacy risk perceptions. The results show that using social login did not lead to a significantly lower level of trust in the app. Besides, there was also no significant effect of the positive influence of social login on consumers' privacy risk perceptions. These non-significant results could both be explained by the fact that participants were maybe not fully aware of the amount of personal information social login asks. Users experience lower trust and more privacy risks when they need to provide irrelevant or sensitive information during the login process (Li & Pavlou, 2013; Sharma & Crossler, 2014). When not knowing what kind and how much personal information is asked, it becomes hard to value the level of trust and the possible risks since privacy and security concerns have a main influence on consumers' trust level in an m-commerce environment (Gupta & Dubey, 2016). Besides, users are more likely to login in m-commerce applications they trust (Leon et al., 2015; Li & Pavlou, 2013; Yazdanifard et al., 2011). Therefore, it could be the case that the fictional m-commerce app was perceived as trustworthy in general. This could have ensured that the type of login did not fully matter, as when a m-commerce platform is trusted, consumers' concerns about disclosing their data decrease (Eastin et al., 2016; Li & Pavlou, 2013).

Corresponding to the theory, all direct effects of the country were found to be significant. The results of this study indicate that country of origin significantly influences trust, privacy risk perception, and intention. The results show that consumers' level of trust in EU apps is significantly higher compared to apps that are from outside the EU. Consumers also have significantly higher privacy risk perceptions when an app from outside the EU was offered compared to an EU app. Besides, consumers have significantly lower intentions to register in an app from outside the EU compared to an app from the EU. This leads to the notion that apps from the EU are considered as higher trusted and much more private and secure which leads to lower privacy risk perceptions and a higher intention to register in EU-apps. This probably results from the European GDPR, as the GDPR protects personal data very well which resulted in consumers having higher trust and lower privacy risk perceptions (Broutsou & Fitsilis, 2012; Sharma & Crossler, 2014). On the other hand, countries outside the EU have less useful privacy and data protection regulations which could lower consumers' trust and higher their privacy risk perceptions (Broutsou & Fitsilis, 2012; Sharma & Crossler, 2014). Besides, the security of data is a reliable predictor of the intention to use m-commerce (Blaise et al., 2018; Eastin et al., 2016).

The expected effect that trust in the app negatively influences privacy risk perceptions was significant. These results support the claim that the higher the trust in the app, the lower the privacy risk perceptions (Eastin et al., 2016; Li & Pavlou, 2013; Li & Yeh, 2010; Li et al., 2016). Having high trust in the app decreases consumers' overall privacy risk perceptions. When having low trust, consumers' privacy risk perceptions increase. Besides, it was also expected that trust in the app increases consumers' intention to register. Results show that the intention to register in the m-commerce app was also significantly influenced by consumers' trust level. The higher consumers' trust in an app, the higher their intention to register in the app. These results are in agreement with the findings of Basarir-Ozel and Mardikyan (2017) and Li and Pavlou (2013) which showed that consumers intention to register is positively influenced by trust.

The results of this study show that privacy risk perceptions significantly affect consumers' intention to register to an m-commerce app. Having lower privacy risk perceptions leads to a significantly higher intention to register in the app and vice versa. These results are in line with those of previous studies who argue that privacy risk perceptions encourage consumers' behavioural intention to register (Li & Yeh, 2010; Lu et al., 2016). This means the higher consumers' privacy risk perceptions, the lower their intention to register or to share personal information with the m-commerce environment (Pavlou, Liang, & Xue, 2007; Dinev & Hart, 2006).

5.1.2 Discussion of interaction effects

Besides the main effects, several interaction effects were measured. Contrary to expectations of literature, no significant interaction effects were found. Results indicate that country of origin (EU vs. Non-EU), privacy statement consent (passive vs. active), and privacy valuation does not significantly interact the effect of login type (general vs. social) on consumers' trust in the app.

The first interaction variable, country of origin, was divided into EU apps and non-EU apps. Countries outside the EU use less useful privacy and data protection laws, and the European GDPR resulted in consumers having higher trust (Broutsou & Fitsilis, 2012; Sharma & Crossler, 2014). Besides, social login needs high amounts of personal information from the user, third parties are involved, and is less trustworthy, private, and secure compared to general login (Gafni & Nissim, 2014; Kontaxis et al., 2012). Therefore, it was expected that apps from the EU with social login are considered as higher trusted compared to apps from outside the EU with social login. Contrary to these expectations, no significant interaction effect of the country of origin of the app was found. The results show that the mean scores for trust are much higher for EU-apps in general. The trust mean scores are also higher for EU apps with social login than for non-EU apps with social login. Besides, the mean score for both login types with non-EU apps is almost identical. Still, this study outcome indicates there is no significant interaction effect of the country of origin of the app. This disagreement with earlier findings could be attributed to the fact that countries outside the EU use less useful privacy and data protection laws which lowers consumers' trust, and the European GDPR resulted in consumers having higher trust (Broutsou & Fitsilis, 2012; Sharma & Crossler, 2014). Therefore, it is likely that in this case, the country of origin of the app was the main influencer of consumers' trust as login type was also found not to be a main influencer of trust.

The second interaction variable, privacy statement consent, was divided into passive and active consent. Consumers' trust increases when they are being actively notified of the privacy policy (Lauer & Deng, 2007; Liu et al., 2005). Besides, the use of social login offers organizations more additional customer information and is less private and secure compared to general login (Gafni & Nissim, 2014; Kontaxis et al., 2012). It was expected that a social login type in combination with an active privacy statement consent would result in higher trust in in the app compared to using passive privacy statement consent. The results showed that there is no significant interaction effect of privacy statement consent within this study. An explanation could be that the perceived adequacy of the privacy statement was not enough, which influences consumers' trust in the online environment (Bansal et al., 2015). Also, privacy in particular strongly influences consumers' trust in the m-commerce organization (Liu, Marchewka, Lu, & Yu, 2005). To make consumers' trust the app, privacy and security issues need to be minimal (Gupta & Dubey, 2016). It has been suggested that the use of social login would result in lower trust (Li & Pavlou, 2013; Sharma & Crossler, 2014). As social login is already lower trusted (Li & Pavlou, 2013; Sharma & Crossler, 2014), it could be that the type of privacy statement consent did not have influence anymore.

Another interaction variable within this study is privacy valuation. Privacy valuation means and measures how much individuals truly value their personal information and information privacy (Adar et al., 2005). It was expected that when using social login, consumers with low privacy valuation have higher trust in the app compared to consumers using social login and having high privacy valuation. Results indicate that the combination of social login and low privacy valuation have a higher trust in the app than the combination of social login with high privacy valuation, however this interaction effect was found not to be significant. This finding is contrary to previous studies but could be attributed to the privacy paradox, wherein consumers claim they highly value their privacy, but do not actively take privacy concerns into account (Friedman & Wathieu, 2007). This means that individuals who have high levels of privacy valuation are still likely to trust the platform and share sensitive personal information online (Morando et al., 2014).

5.1.3 Discussion of mediation effects

In this study, it was expected that the effect of login type on the intention to register in the app was mediated by trust. Trust was found to be a strong influencer and predictor of intention to register (Basarir-Ozel &

Mardikyan, 2017; Li & Yeh, 2010; Lu et al., 2016). Nevertheless, the results show that the effect of login type on the intention to register is not mediated by trust. It was also expected that the effect of login type on intention to register in the app was mediated by privacy risk perception since low levels of privacy risk perceptions were found to positively influence consumers' intention to register (Dinev et al., 2008; Dinev & Hart, 2006; Li & Yeh, 2010; Lu et al., 2016; Pavlou et al., 2007). Results show that the effect of login type on the intention to register was not mediated by privacy risk perception. Thus, no significant mediation effects were found for trust and privacy risk perception. As login type did not significantly influence trust and privacy risk perception, there was no ground for mediation.

5.2 Implications

5.2.1 Practical implications

This research was conducted with the aim to give app designers, app developers, and organizations helpful implications for the design of apps and their login environments. The results of the study show there is no significant evidence that the general or social login type has a significant effect on consumers' level of trust in the app and on their privacy risk perceptions. Therefore, m-commerce platforms should implement both login types as the login type does not influence consumers' trust and their privacy risk perceptions. Implementing both login types makes that people have a choice which could increase the chance that they will register, either via general or social login.

Interestingly, the country of origin of the app influences consumers' trust, privacy risk perceptions and their intention to register. Apps from the EU are higher trusted, consumers have lower privacy risk perceptions and their intention to register is higher. Organizations and marketeers should therefore keep in mind how to deal with this effect. Besides, governments of non-EU countries could review and improve their privacy laws to reduce the negative difference they have compared to apps from the EU.

It appeared that trust in the app has a significant influence on consumers' privacy risk perceptions and their intention to register in the app. Therefore, organizations, app designers, and app developers should make their platforms as trustworthy as possible. Besides, the platform should try to minimalize consumers' privacy risk perceptions as they also influence consumers' intention to register. The more trustworthy the platform, the lower consumers' privacy risk perceptions, and the higher their intention to register. In the end, people will choose the platform they trust the most.

Despite the lack of significant evidence, apps that use active privacy statement consent have higher trust means compared to apps with passive privacy statement consent. Therefore, it is advisable for app designers and app developers to A/B-test the influence of passive and active privacy statement consent. Based on the A/B-testing results, app designers could decide which consent type results in more positive outcomes and could therefore be implemented in the platform.

5.2.2 Theoretical implications

This study was the first that looked into the effect of general and social login on a variety of variables in the context of m-commerce as almost no research has been conducted into the influence and effects of login types (Krasnova et al., 2014; Micallef et al., 2018). Therefore, it adds new knowledge to the growing research field of m-commerce and the influence of login functionalities. Findings can be used as a starting point to explore and compare the influence of the login type in other online contexts.

Since Marriot and Williams (2018) suggested that future research could examine consumer trust perceptions against specific retailers and m-shopping situations, this study adds to the growing field of m-commerce shopping apps. This study shows the impact trust has on consumers' in an m-commerce context. As results may differ for other types of apps or contexts, this study can be used as a foundation and applied to other types of apps and contexts to see if results will differ among different apps or online contexts.

This study also contributes to the field of research that looks into factors influencing consumers' intention to register in m-commerce apps. Li and Pavlou (2013) argued the influence of trust and information privacy concerns on user registration is not widely researched in an online context. Besides, Kalinic and Marinkovic (2015) argued that new insights are needed to understand consumers' decision to use m-commerce. This study shows that, also in the relatively new area of m-commerce, trust and privacy risk perceptions are the main influencers of online user registration. As a result, m-commerce apps should focus on gaining consumers' trust and lowering their privacy risk perceptions to increase user registration rates. These outcomes could be used to further research what specific elements in m-commerce platforms mainly influence consumers' trust and privacy risk perceptions.

Bansal et al. (2015) suggested exploring different ways to improve the perceived adequacy of privacy policy statements such as interactive design, and plain and clear language. This study adds insights into the effect of different types of privacy statement consent on consumers' trust, privacy risk perceptions, and registration intention in an m-commerce context. These findings can be used as a foundation to further explore the effects of different types of privacy statement consent in particular contexts.

5.3 Limitations and recommendations for future research

While this study offered some useful insights, this study also has several limitations. These limitations can be used as inspirations and recommendations for future research.

First, only Dutch millennials took part in this study. Besides, 76% of the participants were between 21 and 25 years old, and only 5.7% between 31 and 40 years old. As results may differ for other countries and age groups, the results are not transferable to all millennials in general and all age groups. Therefore, future research could focus on a more even distribution of the focus group and investigate different age groups.

Second, during the online experiment, participants had to look at a fictional screenshot of an m-commerce app on their smartphone, tablet, or laptop. Participants did not use the fictional app which means they were not experiencing a real app on their smartphone. This could have influenced the results; future research could investigate this study in a more realistic context where they experience the app.

Third, the Netherlands was used for the EU and China was used for non-EU in the online experiment. Since there are many other countries than the Netherlands and China, using other countries might have resulted in other outcomes. Peoples' prejudices could be different for a variety of EU and non-EU countries and could therefore influence the results. Future research could study if there are also differences in influence between different EU and non-EU countries.

Fourth, participants did not have an option to choose between the two login types. They were offered either general or social login. As many m-commerce platforms offer both login types and not only social login, future research should examine the influence of offering both login types in which consumers can choose between general login and social login. This means future studies could compare the influence of offering general login only, social login, and both login types to study what leads to the most positive outcomes.

Fifth, it was not measured if participants actually have and actively use one of the social media accounts they had to log in with during the social login conditions. Participants could attach more value to the social mediums they use the most, or the on that stores the most of their personal information, which might have influenced the results. Therefore, it could be interesting to study the different influences of the participants' highest valued, and their lowest valued social media on the dependent variables of this study.

6. CONCLUSION

This study aimed to investigate if the login type in an m-commerce app influences consumers' trust, their privacy risk perceptions, and their intention to register in the app. This study also researched the interaction effects of the country of origin of the app, privacy statement consent, and privacy valuation. The mediation of trust and privacy risk perception on the effect of login type on intention was also studied. Furthermore, the direct influence of the country of origin of the app on consumers' trust in the app, privacy risk perceptions, and intention to register was studied. A 2x2x2 experimental design was conducted online, using a total of eight different conditions.

The most important finding of this study is that the login type does not have a significant influence on consumers' trust in the app, their privacy risk perceptions, and does not lead to a higher intention to register in the app. This means that it does not matter for m-commerce apps whether to offer general or social login. However, the country of origin significantly influences consumers' trust in the app, their privacy risk perceptions, and their intention to register in the app. Apps from the EU result in higher trust, lower privacy risk perceptions, and higher consumers' intention to register in the app. Furthermore, the county of origin of the app, privacy statement consent, and privacy valuation did not significantly interact with the relationship between the login type and consumers' trust in the app. This means the effect of login type on trust in the app is not influenced by the country of origin of the app, the type of privacy statement consent, and by consumers' level of privacy valuation. Besides, privacy valuation plays a significant role in influencing consumers' trust, their privacy risk perceptions, and their intention to register in the app. The higher consumers value their privacy, the lower their level of trust in the app, the higher their privacy risk perceptions, and the lower their intention to register. Besides, the effect of the login type on consumers' intention to register in the app is not mediated by consumers' trust in the app and their privacy risk perceptions.

In the end, the results of this study add to the field of research in m-commerce and are relevant for app designers, app developers, and organizations who develop m-commerce apps. Findings can be used as a fundament and inspiration for future research within the new area of login functionalities. Besides, it can serve as a new framework for the development of m-commerce apps and their registration environments.

REFERENCES

Abdullah, L., Ramli, R., Bakodah, H. O., & Othman, M. (2019). Developing a causal relationship among factors of e-commerce: A decision making approach. *Journal of King Saud University - Computer and Information Sciences*, 1–8. https://doi.org/10.1016/j.jksuci.2019.01.002

Adar, E., Fine, L. R., & Huberman, B. A. (2005). Valuating privacy. *IEEE Security and Privacy Magazine*, *3*, 22–25. https://doi.org/10.1109/MSP.2005.137

Adelola, T., Dawson, R., & Batmaz, F. (2014). Privacy and data protection in e-commerce in developing nations: Evaluation of different data protection approaches. *International Journal for Digital Society*, 1–19. https://doi.org/10.20533/ijds.2040.2570.2014.0120

Alberts, W. A., & van der Geest, T. M. (2011). Colors matters: Color as trustworthiness cue in websites. *Technical Communication, 58*(2), 149–160. Retrieved from https://research.utwente.nl/en/publications/color-matters-color-as-trustworthiness-cue-in-web-sites

Bansal, C., Bhargavan, K., & Maffeis, S. (2012). Discovering concrete attacks on website authorization by formal analysis. *2012 IEEE 25th Computer Security Foundations Symposium*, 247–262. https://doi.org/10.1109/CSF.2012.27

Bansal, G., Zahedi, F.M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems, 24*(6), 624–644. https://doi.org/10.1057/ejis.2014.41

Barry, M., & Jan, M. T. (2018). Factors influencing the use of m-commerce: An extended technology acceptance model perspective. *International Journal of Economics, Management and Accounting*, *26*(1), 158–183. Retrieved from https://journals.iium.edu.my/enmjournal/index.php/enmj/article/view/502

Basarir-Ozel, B., & Mardikyan, S. (2017). Factors affecting e-commerce adoption: A case of Turkey. *The International Journal of Management Science and Information Technology (IJMSIT)*, (23), 1–11. Retrieved from https://www.econstor.eu/handle/10419/178834

Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in human behavior, 26*(5), 857-869. https://doi.org/10.1016/j.chb.2010.03.013

Bhaskar, P., & Kumar, D.P. (2016). Customer loyalty on e-commerce. *International Journal of Management Research & Review*, *6*(12), 1661–1668. Retrieved from http://ijmrr.com/admin/upload_data/journal_Phani%20%204dec16mrr.pdf

Blaise, R., Halloran, M., & Muchnick, M. (2018). Mobile commerce competitive advantage: A quantitative study of variables that predict m-commerce purchase intentions. *Journal of Internet Commerce*, *17*(2), 96–114. https://doi.org/10.1080/15332861.2018.1433911

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Broutsou, A., & Fitsilis, P. (2012). Online trust: The influence of perceived company's reputation on consumers' trust and the effects of trust on intention for online transactions. *Journal of Service Science and Management*, *5*(4), 365–372. https://doi.org/10.4236/jssm.2012.54043

Castaneda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research, 7*(2), 117–141. https://doi.org/10.1007/s10660-007-9000-y

Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet, 6*(3), 268–295. https://doi.org/10.1002/1944-2866.poi366

Demming, C. L., Jahn, S., & Boztug, Y. (2017). Conducting mediation analysis in marketing research. *Marketing ZFP - Journal of Research and Management, 39*(3), 76–98. https://doi.org/10.15358/0344-1369-2017-3-76

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

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*, *58*, 214–220. https://doi.org/10.1016/j.chb.2015.12.050

Friedman, A., & Wathieu, L. (2007). An empirical approach to understanding privacy valuation. *HBS Marketing Research Paper*, *7*(75). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=982593

Gafni, R., & Nissim, D. (2014). To social login or not login? Exploring factors affecting the decision. *Issues in Informing Science and Information Technology*, *11*, 57–72. https://doi.org/10.28945/1980

Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes. -,1–30. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421731

Greenleaf, G. (2018a). China's personal information standard: The long march to a privacy Law. *Privacy Laws & Business International Report*, *150*, 1–8. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3128593

Greenleaf, G. (2018b). 'European' data privacy standards implemented in laws outside Europe. *Privacy Laws & Business International Report*, *149*, 1–5. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3096314

Guo, Y., Bao, Y., Stuart, B. J., & Le-Nguyen, K. (2017). To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce. *Information Systems Journal*, *28*(2), 359–383. https://doi.org/10.1111/isj.12144

Gupta, P., & Dubey, A. (2016). E-commerce study of privacy, trust and security from consumer's perspective. *International Journal of Computer Science and Mobile Computing*, *5*(6), 224–232. Retrieved from https://www.ijcsmc.com/docs/papers/June2016/V5I6201647.pdf

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33. https://doi.org/10.2307/25148779

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert scale: explored and explained. *British Journal of Applied Science & Technology, 7*(4), 396–403. https://doi.org/10.9734/bjast/2015/14975

Kalinic, Z., & Marinkovic, V. (2015). Determinants of users' intention to adopt m-commerce: An empirical analysis. *Information Systems and E-Business Management*, *14*(2), 367–387. https://doi.org/10.1007/s10257-015-0287-2

Kidane, T.T., & Sharma, R. R. K. (2016). Factors affecting consumers' purchasing decision through e-commerce. Presented at the International Conference on Industrial Engineering and Operations Management, Kuala Lumpur, Malaysia. Retrieved from http://ieomsociety.org/ieom_2016/pdfs/52.pdf

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kontaxis, G., Polychronakis, M., & Markatos, E. P. (2012). Minimizing information disclosure to third parties in social login platforms. *International Journal of Information Security*, *11*(5), 321–332. https://doi.org/10.1007/s10207-012-0173-6

Krämer, J., Schnurr, D., & Wohlfarth, M. (2019). Winners, losers, and Facebook: The role of social logins in the online advertising ecosystem. *Management Science*, *65*(4), 1678–1699. https://doi.org/10.1287/mnsc.2017.3012

Krasnova, H., Eling, N., Abramova, O., & Buxmann, P. (2014). Dangers of 'Facebook login' for mobile apps: Is there a price tag for social information? Presented at the Thirty Fifth International Conference on Information Systems, Auckland, New Zealand. Retrieved from https://aisel.aisnet.org/icis2014/proceedings/ISSecurity/25/

Kshetri, N., Williamson, N., & Bourgoin, D. L. (2006). China: M-commerce in world's largest mobile market. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.879281

Lariviere, B., Joosten, H., Malthouse, E. C., Van Birgelen, M., Aksoy, P., Kunz, W. H., & Huang, M. H. (2013). Value Fusion: The blending of consumer and firm value in the distinct context of mobile technologies and social media. *Journal of Service Management*, *24*(3), 268–293. https://doi.org/10.1108/09564231311326996

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security, 6*(5), 323–331. https://doi.org/10.1007/s10207-007-0028-8

Leon, P. G., Rao, A., Schaub, F., Marsh, A., Cranor, L. F., & Sadeh, N. (2015). Why people are (un)willing to share information with online advertisers. Technical Report CMU-ISR-15-106, 1–25. Retrieved from http://reports-archive.adm.cs.cmu.edu/anon/isr2015/CMU-ISR-15-106.pdf

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. https://doi.org/10.1016/j.dss.2011.01.017

Li, T., & Pavlou, P. A. (2013). What drives users' website registration? -, 1–40. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369444

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*. https://doi.org/10.17705/1cais.02828

Li, Y.-M., & Yeh, Y.-S. (2010). Increasing trust in mobile commerce through design aesthetics. *Computers in Human Behavior, 26*(4), 673–684. https://doi.org/10.1016/j.chb.2010.01.004

Ling, K. C., Chai, L. T., & Piew, T. H. (2010). The effects of shopping orientations, online trust and prior online purchase experience toward customers' online purchase intention. *International Business Research*, *3*(3), 63–76. https://doi.org/10.5539/ibr.v3n3p63

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern: A privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289–304. https://doi.org/10.1016/j.im.2004.01.003

Lu, B., Fan, W., & Zhou, M. (2016). Social presence, trust, and social commerce purchase intention: An empirical research. *Computers in Human Behavior*, *56*, 225–237. https://doi.org/10.1016/j.chb.2015.11.057

Luo, X. (2002). Trust production and privacy concerns on the Internet. *Industrial Marketing Management, 31*(2), 111–118. https://doi.org/10.1016/s0019-8501(01)00182-1

Luzak, J. A. (2014). Privacy notice for dummies? Towards European guidelines on how to give “clear and comprehensive information” on the cookies’ use in order to protect the internet users’ right to online privacy. *Journal of Consumer Policy, 37*(4), 547–559. https://doi.org/10.1007/s10603-014-9263-3

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users’ information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Marriott, H. R., & Williams, M. D. (2018). Exploring consumers perceived risk and trust for mobile shopping: A theoretical framework and empirical study. *Journal of Retailing and Consumer Services*, *42*, 133–146. https://doi.org/10.1016/j.jretconser.2018.01.017

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Micallef, N., Adi, E., & Misra, G. (2018). Investigating login features in smartphone apps. Presented at the The 2018 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Singapore, Singapore. https://doi.org/10.1145/3267305.3274172

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don’t read) online privacy notices. *Journal of Interactive Marketing, 18*(3), 15–29. https://doi.org/10.1002/dir.20009

Morando, F., Iemma, R., & Raiteri, E. (2014). Privacy evaluation: What empirical research on users’ valuation of personal data tells us. *Internet Policy Review*, *3*(2), 1–11. https://doi.org/10.14763/2014.2.283

Morath, F., & Münster, J. (2017). Online shopping and platform design with ex ante registration requirements. *Management Science*, *64*(1), 360–380. https://doi.org/10.1287/mnsc.2016.2595

Nilashi, M., Ibrahim, O., Mirabi, V. R., Ebrahimi, L., & Zare, M. (2015). The role of security, design and content factors on customer trust in mobile commerce. *Journal of Retailing and Consumer Services*, *26*, 57–69. https://doi.org/10.1016/j.jretconser.2015.05.002

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 331–338. https://doi.org/10.1016/j.jretai.2006.08.006

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105. https://doi.org/DOI: 10.2307/25148783

Piao, C., Li, X., Pan, X., & Zhang, C. (2016). User privacy protection for a mobile commerce alliance. *Electronic Commerce Research and Applications*, *18*, 58–70. https://doi.org/10.1016/j.elerap.2016.03.005

Ponciano, L., Barbosa, P., Brasileiro, F., Brito, A., & Andrade, N. (2017). Designing for pragmatists and fundamentalists: Privacy concerns and attitudes on the internet of things. Presented at the XVI Brazilian Symposium on Human Factors in Computing Systems, Joinville, Brazil. https://doi.org/10.1145/3160504.3160545

Sasidharan, S. (2010). The impact of color and product congruency on user trust in B2C e-commerce. *ABD Journal,* 2, 1–16. Retrieved from https://www.ship.edu/contentassets/569211b0c6f243808c3c64f54e816cd2/v2sasidharanp1-p15.pdf

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing, 70*(2), 133–148. https://doi.org/10.1509/jmkg.70.2.133

Sharma, S., & Crossler, R. E. (2014). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Electronic Commerce Research and Applications*, *13*, 305–319. https://doi.org/10.1016/j.elerap.2014.06.007

Sheth, S., Kaiser, G., & Maalej, W. (2014). Us and them: A study of privacy requirements across north America, Asia, and Europe. Presented at the 36th International Conference on Software Engineering, Hyderabad, India. Retrieved from https://dl.acm.org/citation.cfm?id=2568225.2568244

Sidgman, J., & Crompton, M. (2016). Valuing personal data to foster privacy: A thought experiment and opportunities for research. *Journal of Information Systems*, *30*(2), 169–181. https://doi.org/10.2308/isys-51429

Smith, K.T. (2012). Longitudinal study of digital marketing strategies targeting millennials. *Journal of Consumer Marketing*, *29*(2), 86–92. https://doi.org/10.1108/07363761211206339

Tilburg University. (n.d.). SPSS: Interne consistentie - Cronbach's alpha. Retrieved 14 January 2020, from https://www.tilburguniversity.edu/nl/studenten/studie/colleges/spsshelpdesk/edesk/cronbach

TNO. (2015). *Privacy beleving op het internet in Nederland*. Retrieved from https://repository.tudelft.nl/view/tno/uuid:9ea8a097-d17d-4f50-a910-76059d46aedb

Trust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science*, *30*(4), 455–464. https://doi.org/10.1177/009207002236917

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157–174. https://doi.org/10.1016/j.jsis.2013.01.003

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Wang, T., Duong, T.D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Wu, K.-W., 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, 28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Xu, K., Zhang, W., & Yan, Z. (2018). A privacy-preserving mobile application recommender system based on trust evaluation. *Journal of Computational Science*, *26*, 87–107. https://doi.org/10.1016/j.jocs.2018.04.001

Yazdanifard, R., Edres, N. A. H., & Seyedi, A. P. (2011). Security and privacy issues as a potential risk for further ecommerce development. Presented at the 2011 International Conference on Information Communication and Management, Singapore, Singapore. Retrieved from https://pdfs.semanticscholar.org/01c5/5d28035e91cb5882bda08cb599cc63f44578.pdf

Zhang, H., Wang, L., Tuerxunhazi, M., & Yun, H. (2018). Trust and distrust in m-commerce: An integrative framework. Presented at the 2018 2nd International Conference on Management, Education and Social Science (ICMESS 2018), Qingdao, China. https://doi.org/10.2991/icmess-18.2018.142

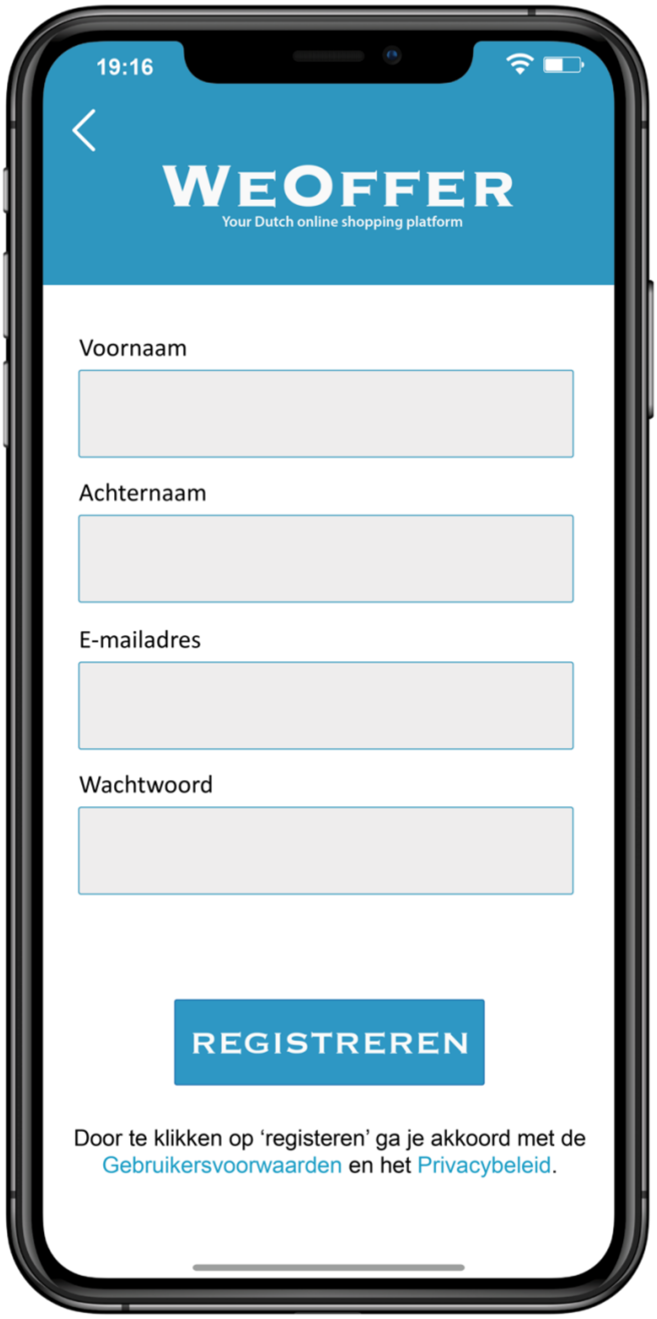
Zharova, A. K., & Elin, V. M. (2017). The use of big data: A Russian perspective of personal data security. *Computer Law & Security Review, 33*(4), 482–501. https://doi.org/10.1016/j.clsr.2017.03.025

APPENDICES

Appendix A – Experimental conditions

CONDITION 1: General login + Passive + EU

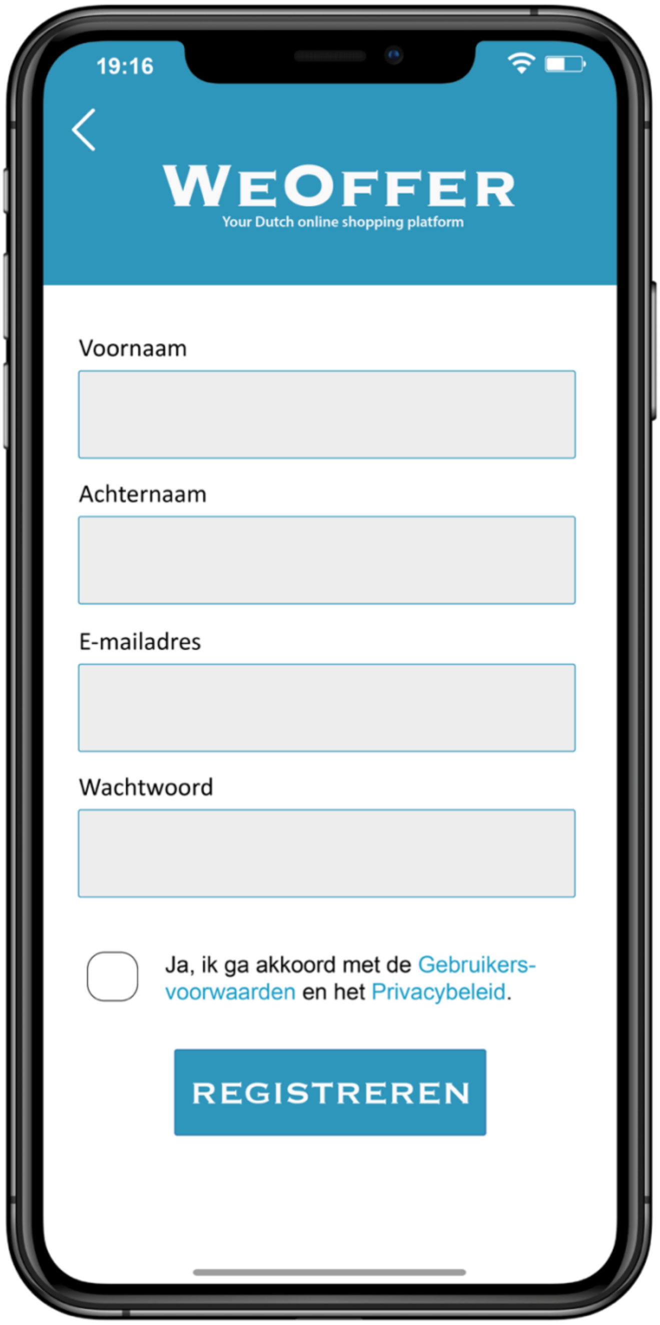
Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Nederlands bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de algemene registreeroptie. Zoals u ziet dient u hiervoor uw voornaam, achternaam, en e-mailadres in te vullen en een wachtwoord te bedenken om een account te registreren. Zodra u op registreren klikt, wordt uw account aangemaakt en accepteert u automatisch de algemene voorwaarden en het privacybeleid van het bedrijf. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



Door te klikken op ‘registeren’ ga je akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

CONDITION 2: General login + Active + EU

Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Nederlands bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de algemene registreeroptie. Zoals u ziet dient u hiervoor uw voornaam, achternaam, en e-mailadres in te vullen en een wachtwoord te bedenken om een account te registreren. Voordat u op registreren klikt, dient u het privacy-statement te accepteren door het vakje aan te vinken. Hiermee accepteert u de algemene voorwaarden en het privacybeleid van het bedrijf. Zodra u op registreren klikt wordt uw account aangemaakt. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



Voornaam

Achternaam

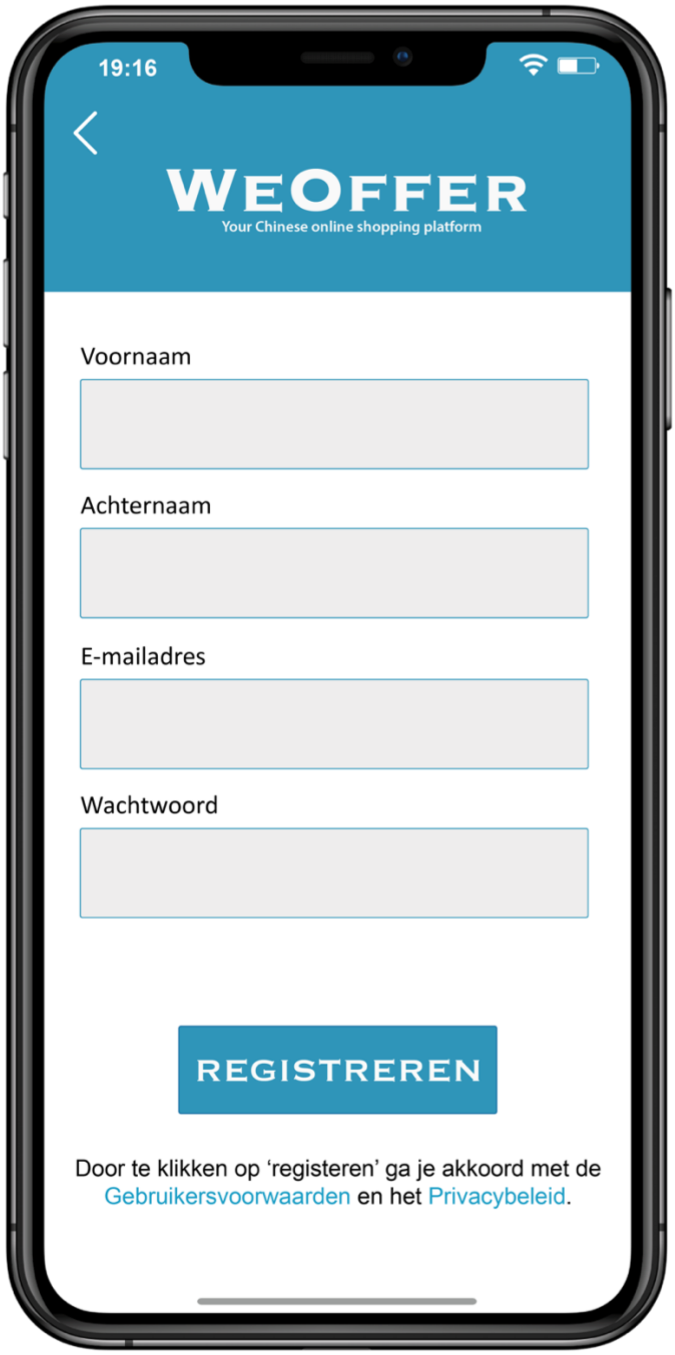
E-mailadres

Wachtwoord

□ Ja, ik ga akkoord met de Gebruikers-voorwaarden en het Privacybeleid.

CONDITION 3: General login + Passive + Non-EU

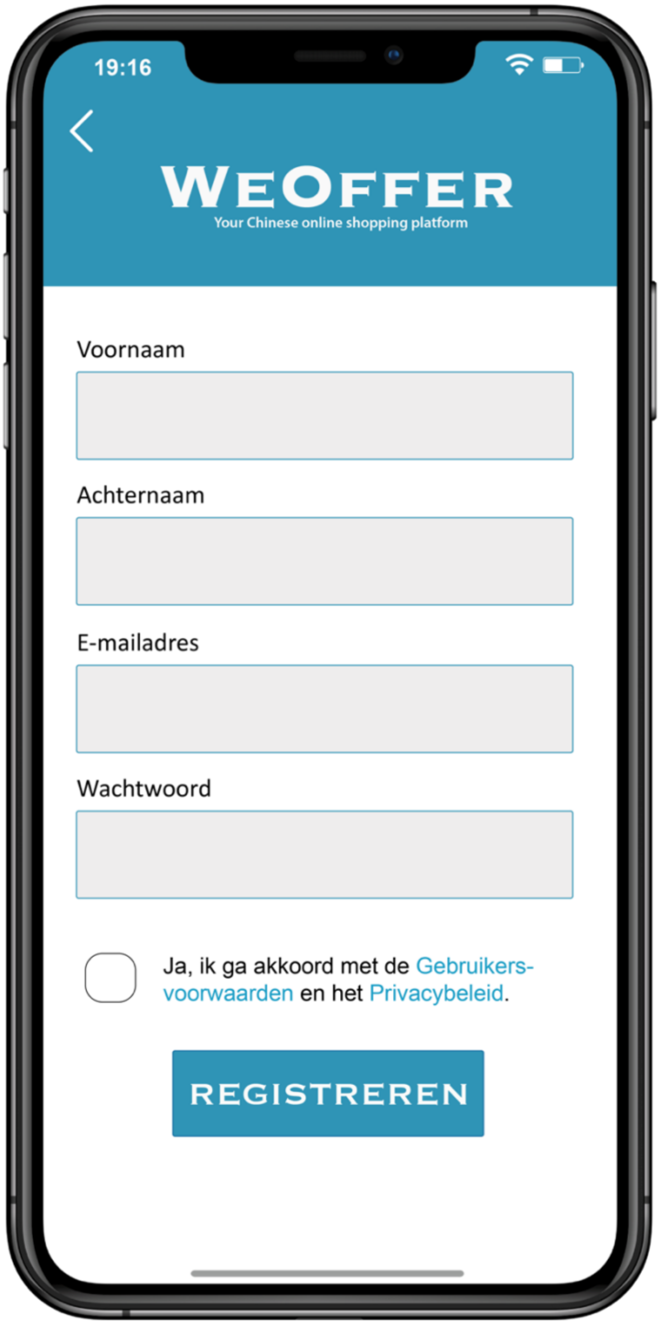
Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Chinees bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de algemene registreeroptie. Zoals u ziet dient u hiervoor uw voornaam, achternaam, en e-mailadres in te vullen en een wachtwoord te bedenken om een account te registreren. Zodra u op registreren klikt, wordt uw account aangemaakt en accepteert u automatisch de algemene voorwaarden en het privacybeleid van het bedrijf. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



Door te klikken op ‘registeren’ ga je akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

CONDITION 4: General login + Active + Non-EU

Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Chinees bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de algemene registreeroptie. Zoals u ziet dient u hiervoor uw voornaam, achternaam, en e-mailadres in te vullen en een wachtwoord te bedenken om een account te registreren. Voordat u op registreren klikt, dient u het privacy-statement te accepteren door het vakje aan te vinken. Hiermee accepteert u de algemene voorwaarden en het privacybeleid van het bedrijf. Zodra u op registreren klikt, wordt uw account aangemaakt. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



Voornaam

Achternaam

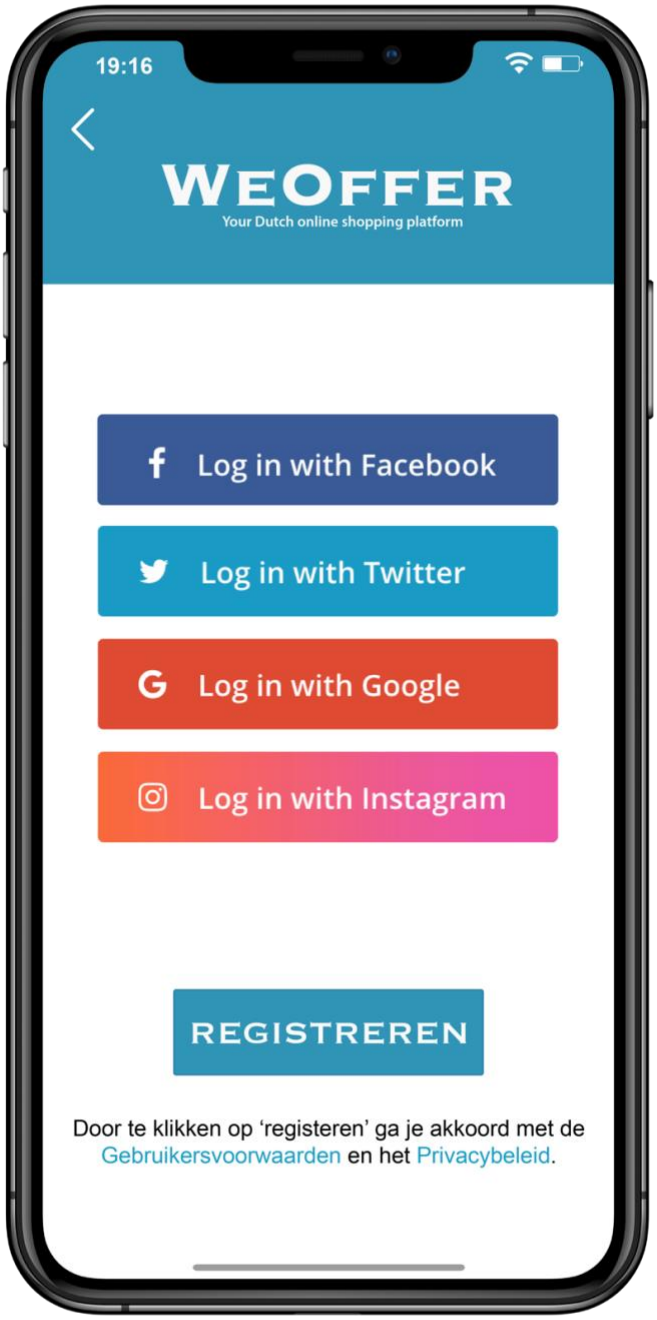
E-mailadres

Wachtwoord

□ Ja, ik ga akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

CONDITION 5: Social login + Passive + EU

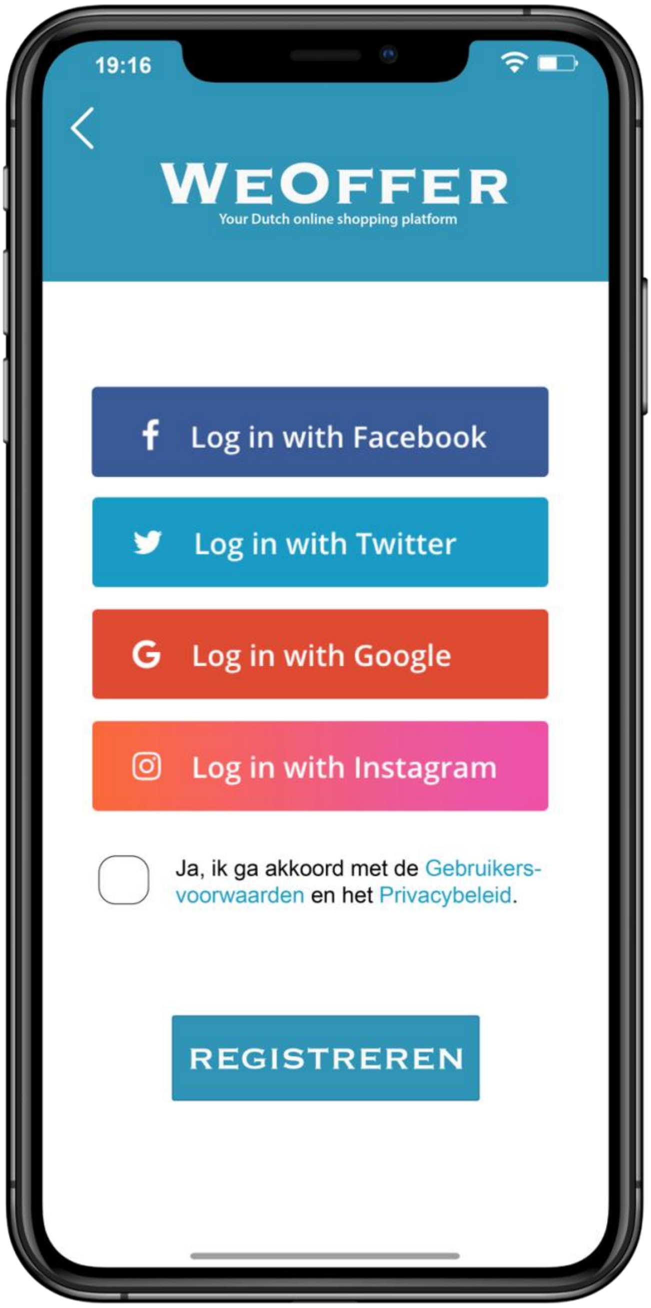
Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Nederlands bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de social login-optie. Hiervoor dient u uw Google, Facebook, Instagram of Twitteraccount aan de app te koppelen om een account te registreren. Zoals u ziet dient u enkel op de 'Log in with…' button van het door uw gekozen sociale medium te klikken. Vervolgens wordt u doorgelinkt naar een pagina om toestemming te geven het door uw gekozen sociale media-account te koppelen. Daarna komt u weer op de weergegeven pagina terecht. Zodra u op registreren klikt, wordt uw account aangemaakt en accepteert u automatisch de algemene voorwaarden en het privacybeleid van het bedrijf. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



Door te klikken op 'registeren' ga je akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

CONDITION 6: Social login + Active + EU

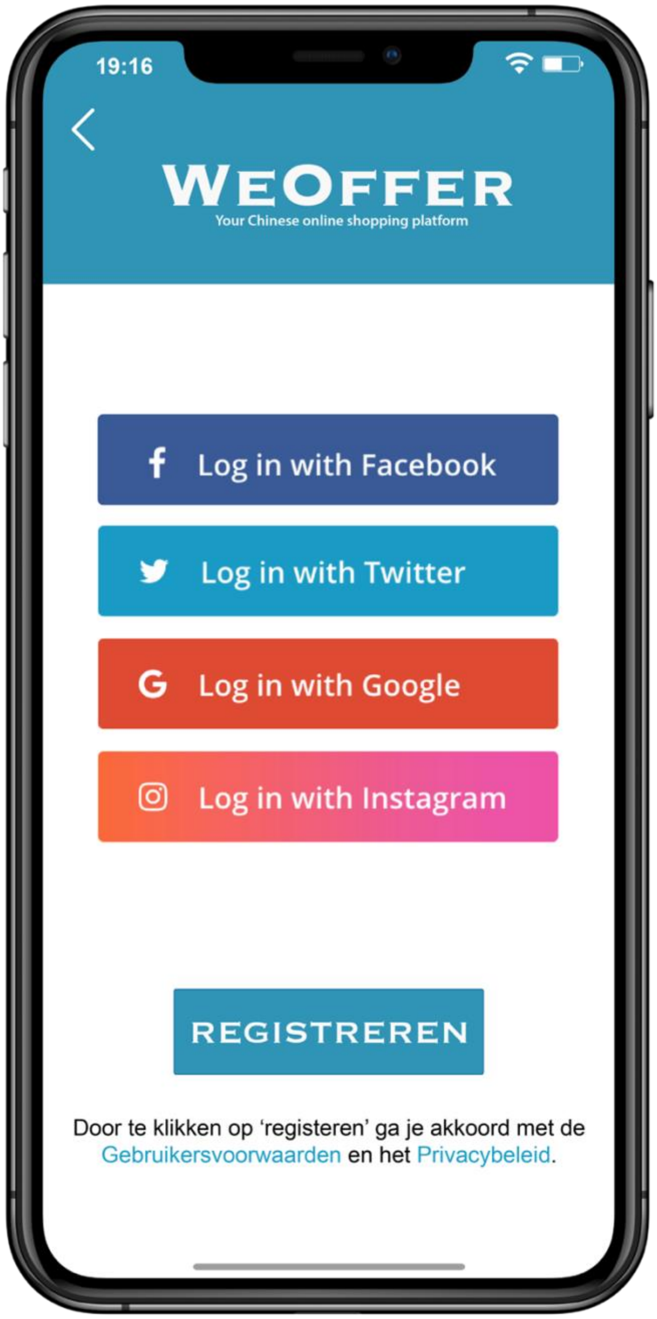
Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Nederlands bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de social login-optie. Hiervoor dient u uw Google, Facebook, Instagram of Twitteraccount aan de app te koppelen om een account te registreren. Zoals u ziet dient u enkel op de 'Log in with…' button van het door uw gekozen sociale medium te klikken. Vervolgens wordt u doorgelinkt naar een pagina om toestemming te geven het door uw gekozen sociale media-account te koppelen. Daarna komt u weer op de weergegeven pagina terecht. Voordat u op registreren klikt, dient u het privacy-statement te accepteren door het vakje aan te vinken. Hiermee accepteert u de algemene voorwaarden en het privacybeleid van het bedrijf. Zodra u op registreren klikt wordt uw account aangemaakt. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



□ Ja, ik ga akkoord met de Gebruikers-voorwaarden en het Privacybeleid.

CONDITION 7: Social login + Passive + Non-EU

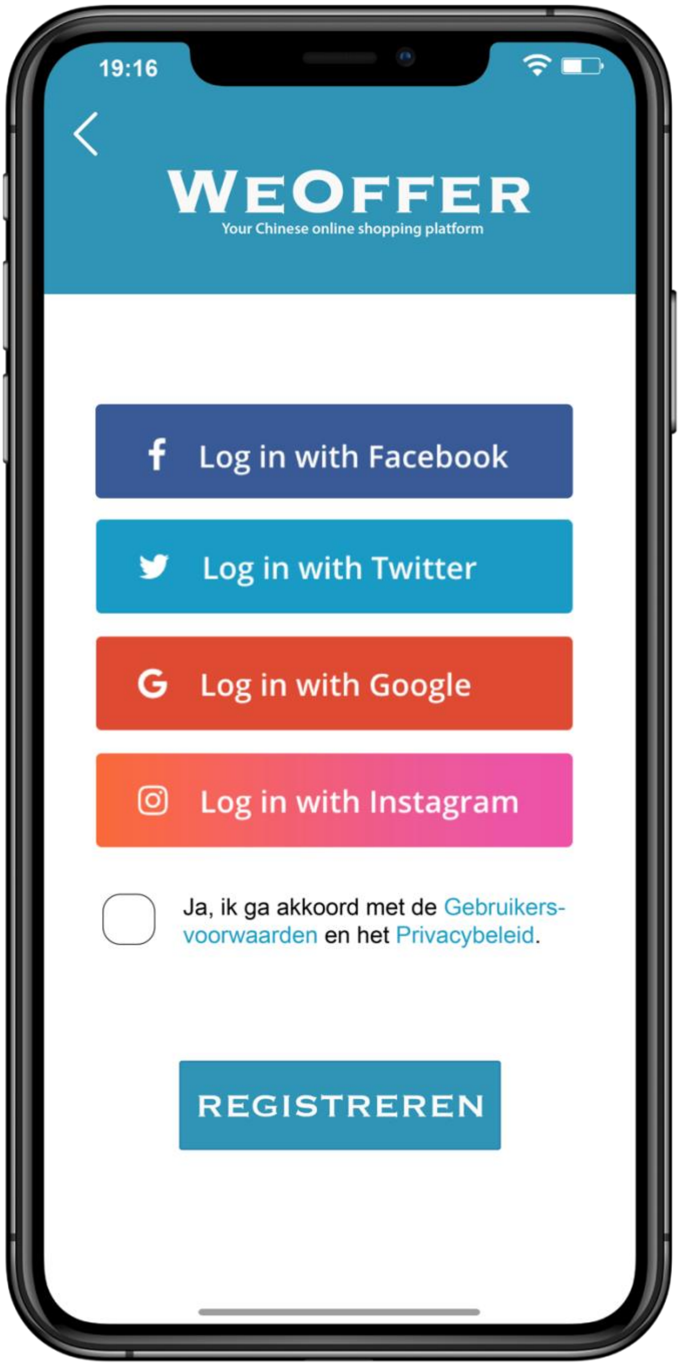
Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Chinees bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de social login-optie. Hiervoor dient u uw Google, Facebook, Instagram of Twitteraccount aan de app te koppelen om een account te registreren. Zoals u ziet dient u enkel op de 'Log in with…' button van het door uw gekozen sociale medium te klikken. Vervolgens wordt u doorgelinkt naar een pagina om toestemming te geven het door uw gekozen sociale media-account te koppelen. Daarna komt u weer op de weergegeven pagina terecht. Zodra u op registreren klikt, wordt uw account aangemaakt en accepteert u automatisch de algemene voorwaarden en het privacybeleid van het bedrijf. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



Door te klikken op 'registeren' ga je akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

CONDITION 8: Social login + Active + Non-EU

Stelt u zich voor dat u een shopping app heeft gedownload in de appstore van uw smartphone. De app is eigendom van een Chinees bedrijf. De app heet WeOffer en u kunt er van alles kopen, van kleding tot elektronica. Om de app te kunnen gebruiken zult u zich moeten registreren door middel van de social login-optie. Hiervoor dient u uw Google, Facebook, Instagram of Twitteraccount aan de app te koppelen om een account te registreren. Zoals u ziet dient u enkel op de 'Log in with…' button van het door uw gekozen sociale medium te klikken. Vervolgens wordt u doorgelinkt naar een pagina om toestemming te geven het door uw gekozen sociale media-account te koppelen. Daarna komt u weer op de weergegeven pagina terecht. Voordat u op registreren klikt, dient u het privacy-statement te accepteren door het vakje aan te vinken. Hiermee accepteert u de algemene voorwaarden en het privacybeleid van het bedrijf. Zodra u op registreren klikt wordt uw account aangemaakt. Vervolgens bent u automatisch ingelogd en kunt u de app gebruiken.



□ Ja, ik ga akkoord met de Gebruikersvoorwaarden en het Privacybeleid.

Appendix B – Survey

Beste respondent,

Fijn dat u de tijd neemt om deel te nemen aan mijn afstudeeronderzoek. Het betreft een enquête waarin u uw mening kunt geven over een app. Ik adviseer u de enquête op een computer of laptop in te vullen. Deelname zal tussen de 5 en 10 minuten van uw tijd kosten. Deelname is volledig anoniem en alle informatie die u verstrekt zal vertrouwelijk worden behandeld en zal alleen voor dit onderzoek worden gebruikt. Bij vragen of opmerkingen kunt u mij bereiken via (c.l.h.gasthuis@student.utwente.nl).

Hartelijk dank voor uw deelname!

Chiel Gasthuis
Master student Communication Studies
c.l.h.gasthuis@student.utwente.nl

Hierbij neem ik deel aan deze enquête

○ Ja
○ Nee

PRIVACY VALUATION
Geef aan in hoeverre u het eens bent met de volgende stellingen:

	Helemaal niet mee eens (1)	Niet mee eens (2)	Min of meer niet mee eens (3)	Niet mee eens en niet mee oneens (4)	Min of meer mee eens (5)	Mee eens (6)	Helemaal mee eens (7)
In vergelijking met anderen ben ik gevoeliger voor de manier waarop online bedrijven omgaan met mijn persoonlijke gegevens. (1)	○	○	○	○	○	○	○
Voor mij is het van groot belang om mijn privacy bij online bedrijven intact te houden. (2)	○	○	○	○	○	○	○
Ik maak me vandaag de dag zorgen over bedreigingen van mijn privacy. (3)	○	○	○	○	○	○	○

Op de volgende pagina zal een situatie beschreven worden en een screenshot worden vertoond. Beeldt u zichzelf in de situatie in die is beschreven en neem alles goed in u op.

C1 casus + screenshot: General login + EU + Passive consent
C2 casus + screenshot: General login + EU + Active consent
C3 casus + screenshot: General login + Non-EU + Passive consent
C4 casus + screenshot: General login + Non-EU + Active consent
C5 casus + screenshot: Social login + EU + Passive consent
C6 casus + screenshot: Social login + EU + Active consent
C7 casus + screenshot: Social login + Non-EU + Passive consent
C8 casus + screenshot: Social login + Non-EU + Active consent

Neem het beschreven scenario en het screenshot goed in u op en beantwoord de volgende vragen zorgvuldig.

PRIVACY RISK PERCEPTION

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	Helemaal niet mee eens (1)	Niet mee eens (2)	Min of meer niet mee eens (3)	Niet mee eens en niet mee oneens (4)	Min of meer mee eens (5)	Mee eens (6)	Helemaal mee eens (7)
Het zou riskant zijn om mijn persoonlijke gegevens aan deze app te verstrekken. (1)	○	○	○	○	○	○	○
Er is een grote kans op verlies van privacy als ik persoonlijke informatie vrijgeef aan de app. (2)	○	○	○	○	○	○	○
Er zal te veel onzekerheid verbonden zijn aan het vrijgeven van mijn persoonlijke informatie aan deze app. (3)	○	○	○	○	○	○	○
Deze app voorzien van mijn persoonlijke informatie zal veel onverwachte problemen met zich meebrengen. (4)	○	○	○	○	○	○	○
Ik zou me veilig voelen wanneer ik mijn persoonlijke informatie aan deze app verstrek. [r] (5)	○	○	○	○	○	○	○
Mijn persoonlijke informatie kan ongepast worden gebruikt door deze app. (6)	○	○	○	○	○	○	○

TRUST IN THE APP

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	Helemaal niet mee eens (1)	Niet mee eens (2)	Min of meer niet mee eens (3)	Niet mee eens en niet mee oneens (4)	Min of meer mee eens (5)	Mee eens (6)	Helemaal mee eens (7)
Ik geloof dat WeOffer in mijn beste belang zal handelen. (1)	○	○	○	○	○	○	○
Als ik hulp nodig heb, denk ik dat WeOffer zijn best zal doen om mij te helpen. (2)	○	○	○	○	○	○	○
Ik heb de indruk dat WeOffer geïnteresseerd is in mijn welzijn, niet alleen in zijn eigen welzijn. (3)	○	○	○	○	○	○	○
Ik heb de indruk dat WeOffer betrouwbaar is in de omgang met mij. (4)	○	○	○	○	○	○	○
Ik zou WeOffer karakteriseren als eerlijk. (5)	○	○	○	○	○	○	○
Ik heb de indruk dat WeOffer zich aan zijn beloften en toezeggingen zal houden. (6)	○	○	○	○	○	○	○
Ik denk dat WeOffer eerlijk en oprecht is. (7)	○	○	○	○	○	○	○
Ik geloof dat WeOffer in staat is om mijn persoonlijke informatie te beschermen. (8)	○	○	○	○	○	○	○
Ik heb de indruk dat WeOffer zijn rol als beschermer van mijn persoonlijke informatie zeer goed vervult. (9)	○	○	○	○	○	○	○
Over het algemeen denk ik dat de organisatie achter WeOffer capabel en bekwaam is. (10)	○	○	○	○	○	○	○
Over het algemeen denk ik dat WeOffer zeer goed is geïnformeerd over de privacywetgeving. (11)	○	○	○	○	○	○	○

INTENTION TO REGISTER IN THE APP

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	Helemaal niet mee eens (1)	Niet mee eens (2)	Min of meer niet mee eens (3)	Niet mee eens en niet mee oneens (4)	Min of meer mee eens (5)	Mee eens (6)	Helemaal mee eens (7)
Ik zou mij waarschijnlijk registreren in de app. (1)	○	○	○	○	○	○	○
Ik zou mij vermoedelijk registreren in de app. (2)	○	○	○	○	○	○	○
Ik denk dat ik mogelijk persoonlijke informatie met de app zou delen. (3)	○	○	○	○	○	○	○
Ik ben niet bereid mij te registeren in de app. [r] (4)	○	○	○	○	○	○	○

De onderstaande tekst en het onderstaande screenshot heb je aan het begin van de enquête al gelezen en gezien. Het dient als herinnering om zo betrouwbaar mogelijke antwoorden te verkrijgen.

C1 casus + screenshot: General login + EU + Passive consent
C2 casus + screenshot: General login + EU + Active consent
C3 casus + screenshot: General login + Non-EU + Passive consent
C4 casus + screenshot: General login + Non-EU + Active consent
C5 casus + screenshot: Social login + EU + Passive consent
C6 casus + screenshot: Social login + EU + Active consent
C7 casus + screenshot: Social login + Non-EU + Passive consent
C8 casus + screenshot: Social login + Non-EU + Active consent

LOGIN TYPE (GENERAL VS. SOCIAL) – manipulation check

De app vraagt mij in te loggen door middel van een social media-account

- Ja
- Nee

PRIVACY STATEMENT CONSENT (PASSIVE VS. ACTIVE) – manipulation check

De app vraagt mij het privacy statement expliciet te accepteren

- Ja
- Nee

Ik moet een check box aanvinken om de algemene voorwaarden en het privacybeleid te accepteren

- Ja
- Nee

COUNTRY OF ORIGIN (EU VS. NON-EU) – manipulation check

De app is eigendom van een bedrijf uit…

- Nederland
- China

De organisatie achter de app is gevestigd in…

- Nederland
- China

De volgende vragen gaan over uw appgebruik.

Hoe vaak gebruikt u apps op uw smartphone of tablet?

- ○ Nooit
- ○ Dagelijks
- ○ Wekelijks
- ○ Maandelijks

Hoe vaak gebruikt u shopping apps op uw smartphone of tablet?

- ○ Nooit
- ○ Dagelijks
- ○ Wekelijks
- ○ Maandelijks

Hoe vaak doet u aankopen u via shopping apps op uw smartphone of tablet?

- ○ Nooit
- ○ Dagelijks
- ○ Wekelijks
- ○ Maandelijks
- ○ Een aantal keer per jaar

Hoeveel shopping apps staan er op uw smartphone of tablet geïnstalleerd?

- ○ 0 shopping apps
- ○ 1 tot 2 shopping apps
- ○ 3 tot 4 shopping apps
- ○ Meer dan 4 shopping apps

Tot slot hebben we nog een viertal vragen over uzelf.

Heeft u de Nederlandse nationaliteit?

- ○ Ja
- ○ Nee

Wat is uw geslacht?

- ○ Man
- ○ Vrouw
- ○ Anders

Wat is uw leeftijd?

Wat is uw huidige of hoogst genoten opleiding?

- ○ Vmbo
- ○ Havo
- ○ Vwo
- ○ MBO
- ○ HBO
- ○ WO

Bedankt voor uw tijd om aan deze enquête deel te nemen. Uw antwoord is geregistreerd.

Appendix C – Measurement items

PRIVACY VALUATION
1: In vergelijking met anderen ben ik gevoeliger voor de manier waarop online bedrijven omgaan met mijn persoonlijke gegevens.
2: Voor mij is het van groot belang om mijn privacy bij online bedrijven intact te houden.
3: Ik maak me vandaag de dag zorgen over bedreigingen van mijn privacy.

PRIVACY RISK PERCEPTION
1: Het zou riskant zijn om mijn persoonlijke gegevens aan deze app te verstrekken.
2: Er is een grote kans op verlies van privacy als ik persoonlijke informatie vrijgeef aan de app.
3: Er zal te veel onzekerheid verbonden zijn aan het vrijgeven van mijn persoonlijke informatie aan deze app.
4: Deze app voorzien van mijn persoonlijke informatie zal veel onverwachte problemen met zich meebrengen.
5: Ik zou me veilig voelen wanneer ik mijn persoonlijke informatie aan deze app verstrek. [r] = left out
6: Mijn persoonlijke informatie kan ongepast worden gebruikt door deze app.

TRUST
Welwillendheid/ Benevolence
1: Ik geloof dat WeOffer in mijn beste belang zal handelen.
2: Als ik hulp nodig heb, denk ik dat WeOffer zijn best zal doen om mij te helpen.
3: Ik heb de indruk dat WeOffer geïnteresseerd is in mijn welzijn, niet alleen in zijn eigen welzijn.

Integriteit/ Integrity
1: Ik heb de indruk dat WeOffer betrouwbaar is in de omgang met mij.
2: Ik zou WeOffer karakteriseren als eerlijk.
3: Ik heb de indruk dat WeOffer zich aan zijn beloften en toezeggingen zal houden.
4: Ik denk dat WeOffer eerlijk en oprecht is.

Bekwaamheid/ Competence
1: Ik geloof dat WeOffer in staat is om mijn persoonlijke informatie te beschermen.
2: Ik heb de indruk dat WeOffer zijn rol als beschermer van mijn persoonlijke informatie zeer goed vervult.
3: Over het algemeen denk ik dat de organisatie achter WeOffer capabel en bekwaam is.
4: Over het algemeen denk ik dat WeOffer zeer goed is geïnformeerd over de privacywetgeving.

INTENTION
1: Ik zou mij waarschijnlijk registreren in de app.
2: Ik zou mij vermoedelijk registeren in de app.
3: Ik denk dat ik mogelijk persoonlijke informatie met de app zou delen.
4: Ik ben niet bereid mij te registeren in de app. [r]