NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Assessing the willingness of customers to share their data in exchange for the free use of mobile apps

Daniela Coelho Carrapiço

Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

ASSESSING THE WILLINGNESS OF CUSTOMERS TO SHARE THEIR DATA IN EXCHANGE FOR THE FREE USE OF MOBILE APPS

by

Daniela Coelho Carrapiço

Dissertation presented as the partial requirement for obtaining a Master's degree in Information Management, Specialization in Knowledge Management and Business Intelligence

Co-supervisor: PhD. Frederico Miguel Campos Cruz Ribeiro de Jesus, IMS

Co-supervisor: PhD. Mauro Castelli, IMS

November 2020

DEDICATION

To my father, Fernando Joaquim Martins Carrapiço, who was an inspiration my whole life to always achieve my goals, no matter how hard they would be. He was (and still is) my role model and I am forever blessed to have him as my father.

To my mother, Ana Paula Martins Coelho, for being the most amazing mother, for being my sunshine in the darkest days, for the unconditional love and the incredible support even when I felt like giving up.

I could not ask for better parents. This is the end of a cycle and if I came this far, it was entirely due to them, and I am forever grateful.

ACKNOWLEDGEMENTS

First, I would like to thank both my co-advisors, Frederico Cruz Jesus and Mauro Castelli who guided me through the writing of this thesis from the very beginning, embracing this journey, understanding my vision, and sharing the same enthusiasm regarding this theme as I do. Thank you from the bottom of my heart for the countless hours of work and dedication to this study, it would be impossible without their support.

Second, I would like to thank my university, Nova University of Lisbon – Information Management School (Nova IMS), including all the teaching and non-teaching personnel for providing me with the tools to accomplish my goals, to allow me to graduate in an area that I love and for being a place where I grew as an individual, not only on a professional level but also on a personal level for almost 5 years.

Finally, I would like to thank my family and friends for the amazing support through this journey. With special attention to Alice, Miguel, Sara, and Catarina who always knew what to do to encourage me through the process of research and writing of the thesis. Thank you.

ABSTRACT

The market of free mobile apps is vaster than the paid ones, gathering data in exchange for its use, leaving to wonder if that disclosure is worthwhile. This study aims to understand the tradeoff people are willing to accept between their privacy and the free use of a smartphone app. The proposed model was empirically evaluated using data from 331 valid questionnaires and tested with Partial Least Squares. Results showcased the users' intention to continue disclosing their data is driven by satisfaction and perceived benefits, not being influenced by perceived risks. Moderation effects of perceived benefits and satisfaction were found.

KEYWORDS

mobile apps; customer behavior; willingness; personal data; privacy.

INDEX

INDEX OF FIGURES

INDEX OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

APPS	Applications.
AVE	Average variance extracted.
CFIP	Concerns for information privacy.
CMB	Common Method Bias.
CR	Composite reliability.
ECM	Expectation Confirmation Model.
ICT	Information and communication technologies.
IUIPC	Internet user's information privacy concerns.
NGOs	Non-governmental organizations.
PLS-SEM	Partial Least Squares Structured Equation Modeling.

1. INTRODUCTION

Personal data privacy is systematically being threatened by multiple mobile apps that require the disclosure of personal data for their use (Fife & Orjuela, 2012; Wottrich, van Reijmersdal, & Smit, 2018). Most mobile apps attract users' downloads due to their "free" aspect (Wottrich et al., 2018) but then require in exchange some personal data creating multiple privacy concerns among users (Keith, Thompson, Hale, Lowry, & Greer, 2013; Koohikamali, French, & Kim, 2019). This is the usual tradeoff consumers have to face when they want to have access to the mobile app (Gu, Xu, Xu, Zhang, & Ling, 2017), creating among them a privacy paradox between the privacy concerns they have and their actual behavior (Barth, de Jong, Junger, Hartel, & Roppelt, 2019; Keith et al., 2013; Wang, Duong, & Chen, 2016). However, there is still a lack of knowledge among the users regarding how the mobile apps are treating their data (King, Lampinen, & Smolen, 2011), leading to the urge for personal data privacy (Gilbert, Chun, Cox, & Jung, 2011; Hui, Teo, & Lee, 2007; Phelps, Nowak, & Ferrell, 2000).

This study aims to shed light on the drivers that influence the willingness to continue disclosing personal data in exchange for the free use of mobile apps on smartphones, assessing the impact that the benefits and risks can have on this behavior; differentiating from other studies in the same area by not focusing on the app permission requests (Wottrich et al., 2018) but rather on the personal information that the user has to willingly give after the download of the app, i.e., creation of an account and fulfill the requested data. Most studies only approach the willingness to share in a more marketing targeted way (H. Li, Sarathy, & Xu, 2011; Phelps et al., 2000), not approaching the specific issue of mobile apps neither the specialization on the free ones. In this study, we aim to analyze the tradeoff people are willing to do between their privacy concerns when disclosing personal data and the benefit of using mobile apps for free. To do so we ground on the privacy calculus model which has been widely used for understanding privacy concerns in the context of technology adoption (Dinev & Hart, 2006; H. Li et al., 2011), Wang et al., (2016) used the privacy calculus to explain the disclosure of personal information in mobile apps, what differentiates that study from the present study is that this study introduces the use of the mobile app for free in exchange for the disclosure of personal information, being the tradeoff related to the benefit of using the mobile app without costs. In particular, we aim to answer the following research questions:

- *What are the most influential drivers in the disclosure of personal information for the free use of a mobile app?*
- *What is the relative importance that perceived benefits and perceived risks have on the decision for one to disclose personal information for the free use of a mobile app?*
- *Does previous experience in disclosing personal information for the free use of a mobile app influence further similar experiences?*

In answering these questions, the remainder of this work is structured as follows: Section 2 has the theoretical background; Section 3 the research model and hypothesis; Section 4 the methodology; Section 5 the data analysis and results; Section 6 will be the discussion; whereas section 7 the conclusions.

2. THEORETICAL BACKGROUND

2.1. DIGITAL REVOLUTION

The world of information and communication technologies (ICT) has fully entered our lives (Choi, Jeon, & Kim, 2019), including the use of smartphones and its mobile apps (Beldad & Citra Kusumadewi, 2015; Hsiao, Chang, & Tang, 2016; Tang, 2019; Yang, 2013). The pervasiveness of mobile apps is well noticeable, as these influence many aspects of one's lives, from social life, to professional, health, education, etc. Because mobile apps are ubiquitous, the term the "App Economy" is often used to depict this fact. However, most of these apps are not actually free and, because of that, users usually need to disclose sensitive information and accept it as being normal (Dinev & Hart, 2006) since it is part of the digital revolution to reveal personal information, whether consciously or unconsciously (Fife & Orjuela, 2012; Mai, 2016). Data is an asset for companies and is being generated at a huge volume and velocity (Landau, 2015) due to this increasingly high engagement and download of mobile apps this data can no longer be treated as regular data (Eastin, Brinson, Doorey, & Wilcox, 2016): this is the era of "Big Data" (Mai, 2016; Zwitter, 2014). People should be aware of how data regarding their actions is being generated, how the internet works as a system, and understanding the potential consequences to their privacy and protect themselves (Alessandro Acquisti et al., 2013; Kang, Dabbish, Fruchter, & Kiesler, 2015), particularly on mobile apps (King et al., 2011).

According to statistics from *We Are Social*[1], there were 200 billion mobile apps downloaded worldwide in 2019 by smartphone users; being a market where nearly 100% of Android apps and nearly 92% of iOS apps are available for free (Fife & Orjuela, 2012). But how are these new technologies making huge amounts of money in revenues every year (Taylor, Voelker, & Pentina, 2011) if they are "free"? By gathering your data (Eastin et al., 2016; Tene & Polonetsky, 2012; Wang et al., 2016; West, 2019; Wottrich et al., 2018).

2.2. THE NEW SOCIAL CONTRACT

According to article 4 of chapter 1 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th of 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), personal data is any information about a person either identified or identifiable, known as the data subject. Making part of personal data information such as name, address, income, medical records, IP address, passport number, racial/ethnic origin, sexual orientation, political opinions, beliefs, or even criminal data[2].
It is mandatory to assess what people conceptualize regarding the term "personal information" to evaluate their willingness to share it. Mai (2016), compares three different visions about the concept of personal information: Floridi's (2005), Solove's (2008), and Murphy's (1996): (i) for

[1] From https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media, Last accessed on November 1st, 2020.
[2] See article 4 of Chapter 1 of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Floridi's (2005), personal information is not something that people own, so the address, income, profession or even marital status are not considered to be “personal information” because it is temporary; (ii) Solove's (2008) considers that “personal information” belongs to both parties involved in a relationship. For example, when you buy something online, the information is both yours and all of the parties involved in that situation. Hence, mobile apps would be entitled to the information the users produce in the mobile app; (iii) for Murphy (1996), “personal information” is more consensus with the definition given by the European Union, defending that it refers to any data about an individual that can identify him. However, according to Eastin et al. (2016), these definitions are no longer accurate, as a definition of personal information needs to be rethought to adapt to this new era; it is important to analyze if some terms should be classified as personal information (such as online profiles or passwords) and reconsider the term information privacy (Isaak & Hanna, 2018).

When people use a service that provides real-time route information it also collects your real-time location data (Degirmenci, 2020; Fife & Orjuela, 2012; Landau, 2015; Wang et al., 2016). This is a usual trade-off of “free” mobile apps: the exchange of privacy over the expected benefits (Barth et al., 2019; Dinev & Hart, 2006; Pentina, Zhang, Bata, & Chen, 2016). When we go to a store and buy something, we are making a social contract where we exchange money for some products or services. Nowadays there is a new type of social contract we do with mobile apps providers: we exchange our personal information for the “free” use of the mobile app, transforming our personal information into the “currency” used on the mobile app market (Wottrich et al., 2018). In other words, users monetize their data. This new kind of social contract is perceived as the willingness to share personal information in which people will continue to engage till perceived benefits exceed the possible risks (Culnan & Armstrong, 1999), and since these huge amounts of data create both personal and social benefits (Koohikamali et al., 2019) its collection is unlikely to stop (Landau, 2015). However, it is necessary to balance between the business needs and the privacy concerns users experience (Bellman, Johnson, Kobrin, & Lohse, 2004). This is not a new topic, the collection of personal information has been a theme in privacy literature since 1970 (Smith, Milberg, & Burke, 1996).

This new social contract arose since companies started to acknowledge that personal data is valuable (Fife & Orjuela, 2012; Hui et al., 2007; Schawrtz, 2004; Tene & Polonetsky, 2012), and increasingly started to solicit it from their consumers (J. C. Zimmer, Arsal, Al-Marzouq, Moore, & Grover, 2010). Modahl (2000) had already predicted that this use of data may occur “*a company that develops the ability to act quickly on data that it collects from the Internet will possess a hard-to-copy advantage*”(p.137), now only a few companies do not do it (Graeff & Harmon, 2002; Phelps et al., 2000). The act of sale of individual behavioral profiles associated with user data is called data capitalism (West, 2019). Personal data, being in the digital form, is easily copied, shared, and integrated (Malhotra, Kim, & Agarwal, 2004) so it is impossible to track where it is or even delete it completely since you do not know how diffuse it already is.

The urge for data privacy began to emerge: people started to understand that the information they disclose can be used to other terms (see, e.g., Gilbert et al., 2011; Hui et al., 2007; Kosinski, Stillwell, & Graepel, 2013; Pentina et al., 2016; Phelps et al., 2000; Wang et al., 2016) having, however, little idea about what data is being collect and with whom that data is being shared with (Beldad & Citra Kusumadewi, 2015; Graeff & Harmon, 2002; Kang et al., 2015; King et al., 2011; Zwitter, 2014). The Internet, but mainly smartphones, started to become a massive

storage area of personal information (Barth et al., 2019; Eastin et al., 2016), and the current methods to protect privacy no longer worked (Landau, 2015; Zwitter, 2014); Emerging the need for personal data privacy (Culnan, 1993; Egele, Kruegel, Kirda, & Vigna, 2011; Krishnamurthy & Wills, 2007).

Studies found out that the monetary incentives influence the willingness to disclose information (Alessandro Acquisti et al., 2013; Hui et al., 2007; Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Except, what if the monetary incentive was the opportunity of using the mobile app for free?

2.3. PRIOR RESEARCH ON PRIVACY

Data privacy is a branch of data security and a sub-field of data management (Kifer & Machanavajjhala, 2011) that focus on the handling of data, how that data is shared with third parties, how it is collected and stored, and if it is in conformation with the regulatory restrictions; making this kind of privacy (Finn, Wright, & Friedewald, 2013) specifically relevant since if there is a data breach, the security of that person can be at stake (Coull & Dyer, 2014).

The different conceptualizations regarding personal information can create some diffusion related to the concept of information privacy. Jeff Smith, Dinev, & Xu (2011) after analyzing more than 320 articles realized that there are different ways to approach privacy: privacy as a commodity; as a right; as a control; or as a state (Keith et al., 2013). Information privacy is the ability that individuals have to limit access or to control their personal information (Bélanger & Crossler, 2011; Liu, 2014; Smith et al., 1996).

Smith et al. (1996) characterized privacy concerns as the concerns individuals have regarding the practices for information privacy of organizations (Bélanger & Crossler, 2011) however, relating to this study, Gu et al. (2017) defined privacy concerns as being the extent to which the users concern about possible losses of privacy when they decide to download a mobile app, according to them, the download of the app is only the first layer of the privacy invasion, so in this study, the privacy invasions that occur after the download are the ones that will be analyzed. Regarding the variables that may be affecting the privacy concerns, Cooper et al. (2018) found out, when asking about the knowledge of privacy laws, that male individuals were more aware than female individuals were, making the females more willing to disclose personal information for the use of mobile apps (Wang et al., 2016); Fife & Orjuela (2012) found out that as the age increases, the privacy concerns also increase.

Smartphone users although having access to the privacy policy of mobile apps, still willingly provide personal data when interacting with mobile apps, explicitly consenting to the collection of their personal information (Liu, 2014; Wottrich et al., 2018). Liu (2014) found out that virtually every user doesn't read the privacy policies of mobile apps downloaded by them and that most of the users would not opt-out of the collection, use, and disclosure of information even if they were presented with that choice. This situation shows that individuals who claim to be concerned about their privacy do not try to become informed about the risks when that information is available (Alfssandro Acquisti & Grossklags, 2005) not acting in conformation with those concerns (Dinev & Hart, 2006; Pentina et al., 2016). Users consent with terms even though, sometimes, do not understand them (Alessandro Acquisti et al., 2017; Choi et al., 2019; Gomez, Pinnick, & Soltani, 2009; King et al., 2011; Mai, 2016), because the risks are not explicitly written

or because they are being biased by the benefits that can advert (Gomez et al., 2009; Schneier, 2015). However, many consumers have refused to give personal information at least one time to a company (Culnan & Armstrong, 1999; Phelps et al., 2000), 30% of the mobile app users have at least uninstalled an app for privacy reasons (Degirmenci, 2020; Pentina et al., 2016) reaching to 57% if it is included the users who do not even install the mobile app due to concerns on personal information sharing (Liu, 2014).

Nevertheless, there are still people who are not concern about their information being accessed or monitored because they "have little to protect" or do not do anything subversive or illegal (Kang et al., 2015); this is, according to Solove (2007), the so-called "nothing to hide" argument denying "*even the existence of a problem*" (p.767), he acknowledged that people who use this argument had a very strict view of what privacy is and perceive privacy as something "*likely to be invoked when there is something to hide and that something consists of negative information about a person*"(p.751), showing there is still a lack of information and a lot of misinformation regarding the theme of data privacy (Wang et al., 2016). Understanding what people know and don't know about how these technologies work is mandatory, so it is possible to design a more effective privacy and security control that matches with the users' perception (Alessandro Acquisti et al., 2013; Kang et al., 2015) and with their needs (Zwitter, 2014).

2.4. PRIVACY CONCERN THEORIES

Privacy concerns may influence several constraints, not only influencing the willingness to adopt new technologies (Fodor & Brem, 2015; Gu et al., 2017) but also the willingness to provide personal information (Dinev & Hart, 2006; Bélanger & Crossler, 2011; Li et al., 2011; Jeff Smith et al., 2011; Kehr et al., 2015; Shaw & Sergueeva, 2019); that influence was acknowledged since the privacy concerns increase the risks believes and decrease the intention to disclose personal information (H. Li et al., 2011).

According to the four-factor model presented by Smith et al. (1996) called Concern for Information Privacy (CFIP), four main dimensions summarize the information privacy concern aspects which are: Collection, unauthorized secondary use, improper access, and errors (Bellman et al., 2004; Milberg, Burke, Smith, & Kallman, 1995; Smith et al., 1996). Previously to CFIP, Smith also created a similar model that had only one dimension and no particular focus contrasting to CFIP which is focused on the responsibilities organizations have to handle customer information properly (Malhotra et al., 2004), it is called Global Information privacy concern.

There is also another theory purposed by Malhotra et al. (2004) called Internet user's information privacy concerns (IUIPC). IUIPC is defined as the level of concern about the collection of personal information, the control an individual has on the collected information, and the awareness regarding the use of that information. That theory includes three factors: control, awareness, and collection (Malhotra et al., 2004), explaining more variance related to the willingness of each individual to pursue a transaction (Bélanger & Crossler, 2011).

Both CFIP and IUIPC were already used to analyze the privacy concerns on the willingness to adopt new technologies where the disclosure of sensitive personal data was confirmed to have an impact on that behavior intention (Fodor & Brem, 2015) considering the intention to provide

personal information a type of behavioral intention (Yun, Lee, & Kim, 2019); however, according to Sipior, Ward, & Connolly (2013), the IUIPC second-order construct do not capture the dimensions of privacy concerns related to trusting beliefs and risk beliefs. For this study, only the CFIP theory will be used since it was already widely validated by several studies and it seems to be more reliable (Stewart & Segars, 2002); however, the factor errors will not be included since it is defined as the protection against errors included in the personal information (Smith et al., 1996). In this case, the personal information will be provided and filled by the individual himself so there will be no errors in the personal information neither need for protection against those errors.

When considering the price of mobile apps, Barth et al. (2019) found out that this is the first element individuals consider after the installation of the app, and the fourth consideration before downloading the app; In other hands, Savage & Waldman (2015) found out that, when the topic is mobile apps, people are willing to pay for the concealment of their information, being females willing to pay more compared with how much males were. These studies show that the price of a mobile app can indeed influence the decision process of disclosing personal information and using the mobile app, acknowledging that, it will be interesting to understand the behavior when the mobile app is free.

Regarding the disclosure of personal information, studies struggle with the fact that little is known about why consumers disclosure so easily their personal information (Y. Li, 2012; Straße & Hildebrand, 2010). Considering that it can be due to acting by impulse and loss of some self-control when there are immediate benefits involved in the tradeoff (Alfssandro Acquisti & Grossklags, 2005), lack of understanding about the data use policy of websites (Choi et al., 2019) or even the decrease of privacy concerns due to the perceived app popularity (Gu et al., 2017). Since individuals rely on the opinions of people (Taylor et al., 2011), it generates trust in the mobile app and, the development of trust leads to a greater willingness to disclose personal information (Bellman et al., 2004; Culnan & Armstrong, 1999). Sometimes people disclose their information because it is a requirement to use a mobile app (Alessandro Acquisti et al., 2017; Egele et al., 2011). Consumers, even knowing the risks implied, often choose to trade off long-term privacy just to have short-term benefits (Alfssandro Acquisti & Grossklags, 2005; Dinev & Hart, 2006; Eastin et al., 2016; Phelps et al., 2000). In the specific case of mobile apps, studies show that the perceived benefits have a greater influence to disclose information than the perceived risks do (Wang et al., 2016). As Schneier (2015) stated, it is mandatory to assess how much of our privacy we are willing to disclose for convenience. However, consent is not always an option, mainly if the topic is mobile apps (Liu, 2014); if consent is a condition to using a service the rate of positive consents will likely be higher (Landau, 2015).

Li (2012) suggests the intentions of individuals in disclosing information online can be determined by the dual-calculus model, which is a combination of risk calculus and the privacy calculus. The privacy calculus model refers to the tradeoff between costs and benefits influencing the behavior (Jeff Smith et al., 2011); whereas the risk calculus refers to the tradeoff between the perceived risks and the ability to deal with those risks (Y. Li, 2012). Some studies applied privacy-calculus model in the context of disclosure of personal information (Kim, Park, Park, & Ahn, 2019) and mobile app trade-off experienced by users (Pentina et al., 2016; Wang et al., 2016; Wottrich et al., 2018); the privacy calculus model, in this case, would consist on the process of considering the possible risks of disclosing personal information and compare them

with the potential benefits (Kehr et al., 2015), including the use of the mobile app for free. Kim et al. (2019) proposed a model that evaluates the willingness to provide personal information, combining the privacy calculus model and several variables related to the IoT services; since the topic of that study is related with this research in the way of understanding the willingness to provide/continuing to provide personal information, the research model will be based on that study.

Although some information is more sensitive than other (Cooper et al., 2018; Culnan, 1993; Fife & Orjuela, 2012; Kim et al., 2019; Kotz, Gunter, Kumar, & Weiner, 2016) individuals still give information that are considered to be "sensitive" (like medical and financial) easily to use mobile apps even though those applications can have security breaches (Martínez-Pérez, Torre-Díez, & López-Coronado, 2014) and the data provided by the consumers or produced by them (in the app) can be easily obtained (Coull & Dyer, 2014; Rahman, Carbunar, & Banik, 2013).

3. RESEARCH MODEL

This study proposes a research model that integrates three theories from previous known studies: the Concern for information privacy - CFIP (Smith et al., 1996) which has been a widely used model to explain the concerns experienced by people regarding their information, having a direct impact on the perceived privacy risks that someone can experience; relating to the second theory where privacy-calculus aims to understand the relation between the risks and the benefits of an action (Kim et al., 2019); and finally, the third theory which seeks understanding regarding the connection between all these models and the continuance intention to disclose personal information to use mobile apps for free, using the satisfaction to understand these relationships (Bhattacherjee, 2001). The research model and all the hypotheses can be seen in **Figure** 1**.**

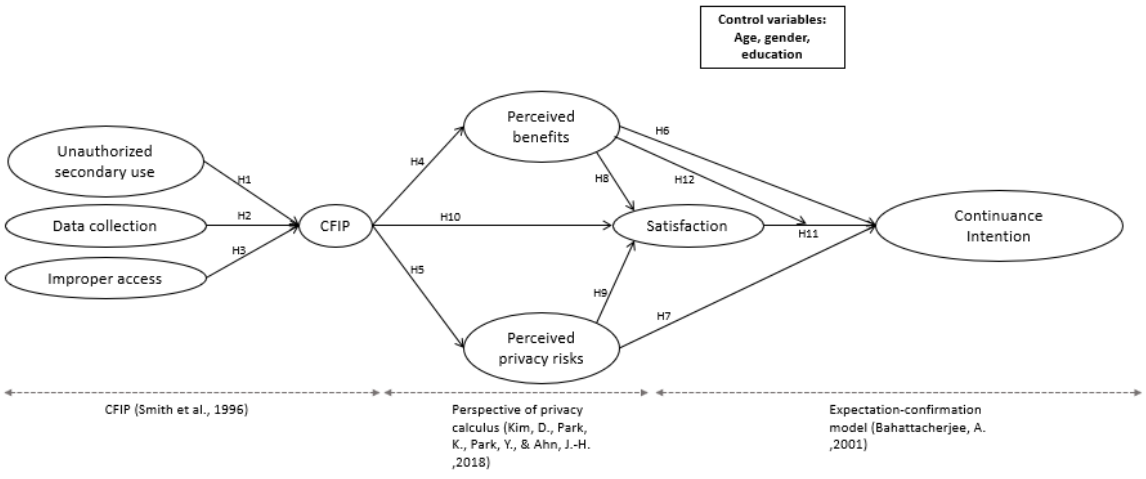

Figure 1 – Research model.

3.1. CONCERNS FOR INFORMATION PRIVACY THEORY (CFIP)

The constructs from Smith et al. (1996) – unauthorized secondary use, data collection and improper access - aim to understand the level of concern for information privacy experienced by someone, developing the second-order construct CFIP. CFIP is a second-order reflective-formative construct because it depends and derives from each of its dimensions, which will be responsible to capture the concerns for information privacy (Stewart & Segars, 2002).

Unauthorized secondary use refers to the "*concern that information is collected from individuals for one purpose but is used for another*" (Smith et al., 1996, p.172). In this study, the secondary unauthorized use will refer to use of the information, given by the user to the mobile app, by other entities (besides the app) that were not explicitly authorized by the user. This factor was used in multiple approaches to determine the privacy concerns of individuals, mainly in CFIP where it was proved multiple times by previous literature that has a direct influence on the privacy concerns (Bellman et al., 2004; Culnan, 1993; Gomez et al., 2009; Krishnamurthy & Wills, 2007; Smith et al., 1996; M. Zimmer, 2010). In the context of this study, and regarding the evidence provided by previous studies, it is expected that when people experience concerns regarding unauthorized secondary use of personal data they disclose to use mobile apps it will result in an increase in concerns for information privacy. Thus, it is hypothesized that:

H1. Unauthorized secondary use has a positive influence on Concerns for information privacy.

Data collection refers to "*the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received*"(Malhotra et al., 2004, p.338). In this study, this factor will refer to the concern about the amount of personal data that is being collected and possessed by the mobile app. Previous studies reveal that this factor has a relevant impact on the increase in privacy concerns (Gomez et al., 2009; Graeff & Harmon, 2002; Phelps et al., 2000). In the mobile app context, it would be relevant to understand if the pattern remains the same, i.e., if people who experience larger concerns regarding their personal information being collected by mobile apps would experience higher concerns for information privacy. Stating that, it is hypothesized that:

H2. Data Collection has a positive influence on Concerns for information privacy.

Improper access to information, in the context of mobile apps, refers to the access of information that the user disclosed to the mobile app by individuals or entities that were not explicitly authorized by the user. According to the literature, improper access to information refers to the concern that personal data is available to people who are not explicitly authorized to view or use it (Smith et al., 1996). This is a common privacy concern confirmed by previous studies (Bellman et al., 2004; Smith et al., 1996). It is expected that, if people are more concerned regarding improper access that can occur regarding their personal data disclosed to the mobile app, they will have higher concerns for information privacy. Regarding those shreds of evidence, the hypothesis created is:

H3. Improper access has a positive influence on Concerns for information privacy.

Past studies even identify that CFIP can positively affect perceived privacy risks (Hin, 2015), defending that the highest the concerns an individual has, the highest the privacy risks perceived

(Malhotra et al., 2004). The research proposed by Hsu & Lin (2016) also verified that CFIP is negatively associated with continuance intention to use Internet of Things services (IoT). Hence, it seems therefore reasonable to hypothesize that should also (negatively) affect perceived benefits. In the context of this study, it is believed that people with higher concerns for information privacy will perceive more privacy risks and fewer benefits when disclosing personal information to use a mobile app.

H4. Concerns for information privacy has a negative impact on perceived benefits.
H5. Concerns for information privacy has a positive influence on perceived privacy risks.

3.2. PERSPECTIVE OF PRIVACY CALCULUS

The perspective of privacy calculus aims to understand the tradeoff between the privacy risks and the benefits one perceives regarding the willingness to provide personal information (Kim et al., 2019). In this study, we take a step forward, towards post-adoption behavior, as respondents already downloaded and used free mobile apps. Hence, in comparison to the original work from Kim et al., (2019), the dependent variables in this study are satisfaction with free mobile apps that require personal information, and continuance intention to disclose personal information to grant free mobile apps use.

Perceived benefits are understood as being the advantages an individual expects to have when an action is performed, in this case, disclosure of personal information to access a free mobile app. Previous literature supports the importance of this perception for the study of the adoption and use of technology (Alfssandro Acquisti & Grossklags, 2005; Harris, Brookshire, & Chin, 2016; Hsu & Lin, 2016; H. Li et al., 2011). Alfssandro Acquisti & Grossklags (2005), for example, revealed in their study that individuals are willing to let go of some privacy, disclosing personal information in exchange for some benefits (Eastin et al., 2016), having a positive influence on the willingness to provide personal information (Kim et al., 2019; Wang et al., 2016). Hsu & Lin (2016) in their study regarding the continuance use of IoT services, acknowledged that perceived benefits had a significant effect to explain the continuance intention to use IoT services. In the context of this study, it is believed that people will be more willing to provide personal information to use a mobile app when they perceive they will have benefits.

Perceived privacy risks or perceived privacy concerns are the risks/concerns people perceive when disclosing information for the mobile application. Some studies acknowledge privacy concerns or the privacy risks influence behavior intention (Fodor & Brem, 2015; Harris et al., 2016), that behavior can be the willingness to disclose personal information (Wang et al., 2016). Given these pieces of evidence, it is hypothesized that:

H6. Perceived benefits have a positive influence on continuance intention to disclose personal information.
H7. Perceived privacy risks have a negative influence on continuance intention to disclose personal information.

3.3. EXPECTATION CONFIRMATION MODEL

The relation between the risks people perceive in disclosing their personal information and the intention to continue using it can be explained with the Expectation Confirmation Model (ECM) (Bhattacherjee, 2001). This model explains that the satisfaction obtained by some action/purchase and the confirmation of the expectations the individuals had can influence the continuous intention to perform the same action and it has been widely used in the mobile app context (Hsiao et al., 2016). In this work, ECM provides the theoretical support for the relationship between satisfaction with the intention to continue disclosing personal information for free mobile app use.

In the ECM by Bhattacherjee (2001), the constructs aim to understand the willingness of the customer to continuing using information systems; for this study, it is aimed to understand what is triggering the continuous disclose of personal information for the free use of mobile apps. Satisfaction was defined by Bhattacherjee (2001) as a "*psychological or affective state related to and resulting from a cognitive appraisal of the expectation-performance discrepancy (confirmation)*" (p.354), meaning that, when a consumer has some expectations and the performance surpasses those expectations, the satisfaction increases, influencing the continuance intention to do a certain behavior (Bhattacherjee, 2001). Some studies confirm the influence of this relation in the context of mobile apps (Hsiao et al., 2016). In the context of this study, it is believed that people will continue to disclose personal information to use for free the mobile app if they are satisfied with previous similar experiences.

Han, Wu, Wang, & Hong, (2018) found several different types of perceived benefits to influence positively the satisfaction a person can experience, however, Ofori, Larbi-Siaw, Fianu, Gladjah, & Boateng (2015) found out that the satisfaction can decrease when perceived privacy risks are higher. Accordingly, it seems plausible to sustain that if perceived privacy risks have that impact on satisfaction, the concerns for information privacy would have a similar effect on satisfaction as well. In this study, we consider that when one perceives higher benefits, he or she will also be more satisfied to disclose personal data for the free use of a mobile app. However, if one perceives higher risks or is more concerned regarding personal information in that disclosure, he or she will likely be less satisfied in providing it for the use of mobile apps for free.

Regarding the relation between the perceived benefits and the satisfaction, they are both positive outcomes of the behavior so it would be expected that, since both of them, according to literature, influence in a positive way the continuance intention, one intensifies the effect of the other. Meaning that, if someone is satisfied with disclosing data for the free use of a mobile app, the benefits they perceive would contribute even more to the continuance intention to disclose personal data for the free use of a mobile app. In the context of this study, it is believed that, when people perceive higher benefits and are satisfied with this experience, they will be more likely to continue to disclose personal information for the free use of mobile apps. The hypotheses formulated are:

H8. Perceived benefits have a positive influence on Satisfaction.
H9. Perceived privacy risks have a negative influence on Satisfaction.
H10. CFIP has a negative influence on Satisfaction.
H11. Satisfaction has a positive influence on Continuance intention.

H12. Perceived benefits moderate the relationship between Satisfaction and Continuance intention, in such a way that this will be stronger for those with higher levels of perceived benefits.

4. METHODOLOGY

4.1. MEASUREMENT DEVELOPMENT

The model and the hypotheses were tested using an online survey created on Qualtrics gathering the necessary data for the study. The instrument (please see **Table A1** in Appendix) was developed based on adapted valid constructs from previous literature and, since the questionnaire targets the Portuguese population, the questionnaire was translated to Portuguese by a professional translator to guarantee that the meaning of the items in each construct would not be compromised. The questionnaire was then translated back to English to assure the validity and reliability of the initial translation. To confirm the validity of the instrument, a pilot was conducted on a group of 30 mobile app users. Everyone who performed the pilot provided feedback evaluating the clarity of the survey and identifying questions that could lead to doubt. Those feedbacks were incorporated in the final questionnaire yet, the data collected from those questionnaires were not used for further analysis. Subsequently, the questionnaire was diffused among several social media platforms and universities.

Podsakoff, MacKenzie, Lee, & Podsakoff (2003) defines Common Method Bias (CMB) as the potential bias that the instrument used can have in the answers of the respondents, in order to verify if that bias affected the data used in this study, the Harman's single-factor test was performed, which states that the first factor must explain less than 50% of the covariance amongst all constructs (Podsakoff et al., 2003). The Harman's single-factor test revealed that the first factor only explains 25,6% of the covariance amongst all constructs, meaning that Common Method Bias does not affect the data used in this study (MacKenzie & Podsakoff, 2012; Podsakoff et al., 2003).

4.2. DATA

The respondents were individuals who have access to the internet, have a smartphone, and have downloaded at least a mobile app in the last three months (to guarantee that the sample regularly uses mobile apps). In total we had 480 collected answers., After cleaning all the questionnaires that did not belong to the target audience and questionnaires that were not fully completed, there were a total of 331 valid questionnaires (69%).

On the data collected, respondents with ages between 16 and 24 were more frequent, representing a total of 54% of the data collected. Regarding the education and professional situation, most of the respondents have a university education (79%), and more than half of the respondents are employed (56%). **Table 1** summarizes the profile of the respondents.

Table 1 – Profile of the respondents.

Characteristics	n	%
Gender		
Female	219	66.16
Male	110	33.23
Other	2	0.60
Age		
16-45	179	54.08
25-44	88	26.59
45 or older	64	19.34
Education		
Less than high school degree	5	1.51
High school degree or equivalent	66	19.94
Bachelor's degree	153	46.22
Master's degree	98	29.61
Doctorate or higher	9	2.72
Professional situation		
Student	125	37.76
Unemployed	14	4.23
Employed	185	55.89
Retired	7	2.11

5. DATA ANALYSIS AND RESULTS

For this study, the SEM (Structural Equation Modeling) was used, in specific, the PLS (Partial Least Squares) technique and SMART PLS 3.3 as the analysis tool to estimate the model and compare the correlations between constructs. PLS was chosen for the estimation of the model due to the fact it is more suitable for the type of theory that this study approaches, it does not require the sample obtained to follow a normal distribution, and even because the model used in this study is complex and has many relationships represented.

5.1. MEASUREMENT MODEL

To evaluate the internal consistency and discriminant validity of the reflective constructs it is necessary to verify some assumptions are met. These measures can be noted in **Table 2** and **Table 3**. First, to evaluate internal consistency, the composite reliability (CR) criterion was used where, if all the constructs show values of 0.7 or higher the criterion is verified. Also, to warrant the reliability of the model, the Average Variance Extracted (AVE) must be greater than 0.5 (Bagozzi & Yi, 1988). As shown in **Table 2**, all the constructs showed values greater than 0.7 verifying the existence of internal consistency and reliability.

Table 2 – Composite reliability, inter-constructs correlations and the square root of AVE.

	CR	US	DC	IA	PB	PR	S	CI
Unauthorized secondary use	0.855	**0.865**						
Data collection	0.930	0.378	**0.877**					
Improper access	0.905	0.678	0.399	**0.872**				
Perceived benefits	0.920	-0.011	0.015	0.002	**0.861**			
Perceived privacy risks	0.909	0.292	0.577	0.366	0.099	**0.845**		
Satisfaction	0.946	-0.251	-0.469	-0.288	0.143	-0.289	**0.902**	
Continuance intention	0.954	-0.116	-0.247	-0.161	0.290	-0.115	0.384	**0.934**

Note: CR=Composite reliability, US= Unauthorized secondary use, DC= Data collection, IA= Improper access, PB= Perceived benefits, PR= Perceived privacy risks, S=Satisfaction, CI= Continuance intention.

Second, it is necessary to evaluate the discriminant validity of the constructs, for that, the Fornell-Larcker criterion (Fornell & Larcker, 1981) and cross-loadings were used. Fornell & Larcker (1981) in the criteria they developed state that, for the existence of discriminant validity it is necessary the square root of the average variance extracted (AVE) to be greater than the inter-construct correlations. The square root of AVE is represented in the diagonal, in bold. As it is possible to assess in **Table 2**, all constructs obey the Fornell-Larcker criterion. Regarding the cross-loading criteria, the loadings for the items in each construct should be higher than the 0.7 benchmark and, also, higher than the cross-loadings. The loadings for each construct are represented in bold. The cross-loading criteria were not verified for the PR4, US2, US3, and PB4 since these items had low values for the loadings; for that reason, these items were removed, and the model was recalculated. In **Table 3** is possible to assess the value for all the loadings and cross-loadings of the recalculated model and it is validated that all constructs presented the cross-loadings criteria. Considering these criteria, it is possible to assess that the instruments show good discriminant validity.

Table 3 – Loadings and cross-loadings.

Constructs	Item	US	DC	IA	PB	PR	S	CI
Unauthorized sec. use	US1	**0.889**	0.385	0.604	-0.076	0.281	-0.197	-0.110
	US4	**0.840**	0.258	0.569	0.070	0.220	-0.241	-0.090
Data collection	DC1	0.291	**0.864**	0.283	0.008	0.465	-0.415	-0.218
	DC2	0.371	**0.878**	0.367	-0.028	0.468	-0.354	-0.257
	DC3	0.358	**0.910**	0.396	-0.002	0.529	-0.454	-0.200
	DC4	0.300	**0.856**	0.347	0.077	0.563	-0.422	-0.191
Improper access	IA1	0.539	0.377	**0.842**	0.042	0.340	-0.239	-0.129
	IA2	0.643	0.292	**0.859**	-0.036	0.247	-0.268	-0.165
	IA3	0.595	0.371	**0.912**	-0.002	0.365	-0.246	-0.130
Perceived benefits	PB1	-0.015	0.029	-0.023	**0.892**	0.079	0.130	0.257
	PB2	0.002	0.021	0.006	**0.903**	0.101	0.140	0.229
	PB3	-0.004	0.035	-0.023	**0.839**	0.108	0.071	0.192
	PB5	-0.017	-0.021	0.035	**0.807**	0.063	0.136	0.296
Perceived privacy risks	PR1	0.290	0.478	0.365	0.092	**0.863**	-0.275	-0.076
	PR2	0.224	0.470	0.256	0.098	**0.847**	-0.208	-0.120
	PR3	0.196	0.490	0.265	0.024	**0.859**	-0.267	-0.119
	PR5	0.271	0.510	0.339	0.119	**0.809**	-0.221	-0.077
Satisfaction	S1	-0.251	-0.432	-0.263	0.143	-0.244	**0.906**	0.371
	S2	-0.195	-0.454	-0.239	0.152	-0.259	**0.917**	0.328
	S3	-0.215	-0.411	-0.270	0.101	-0.277	**0.889**	0.326

	S4	-0.240	-0.392	-0.266	0.119	-0.264	**0.894**	0.359
Continuance intention	CI1	-0.069	-0.210	-0.143	0.317	-0.112	0.341	**0.939**
	CI2	-0.123	-0.238	-0.156	0.220	-0.119	0.376	**0.930**
	CI3	-0.136	-0.244	-0.153	0.274	-0.091	0.361	**0.934**

Note: US= Unauthorized secondary use, DC= Data collection, IA= Improper access, PB= Perceived benefits, PR= Perceived privacy risks, S=Satisfaction, CI= Continuance intention.

5.2. STRUCTURAL MODEL

The path coefficients, t-value, and variance explained (R^2) were used to examine the structural model and to empirically validate the hypotheses that were defined in Section 3. To determine the path coefficients and test the relationships between the constructs, the method used was bootstrapping, using a subsample of 5,000 samples.

In **Table 4** is possible to acknowledge that most path coefficients regarding the hypotheses are significant, however, not all of them are supported since they demonstrate a different influence than what it was expected. Regarding the R^2, the model explains 24.3% of the variance of the continuance intention to disclose personal information for the free use of mobile apps (CI), see **Figure 2**.

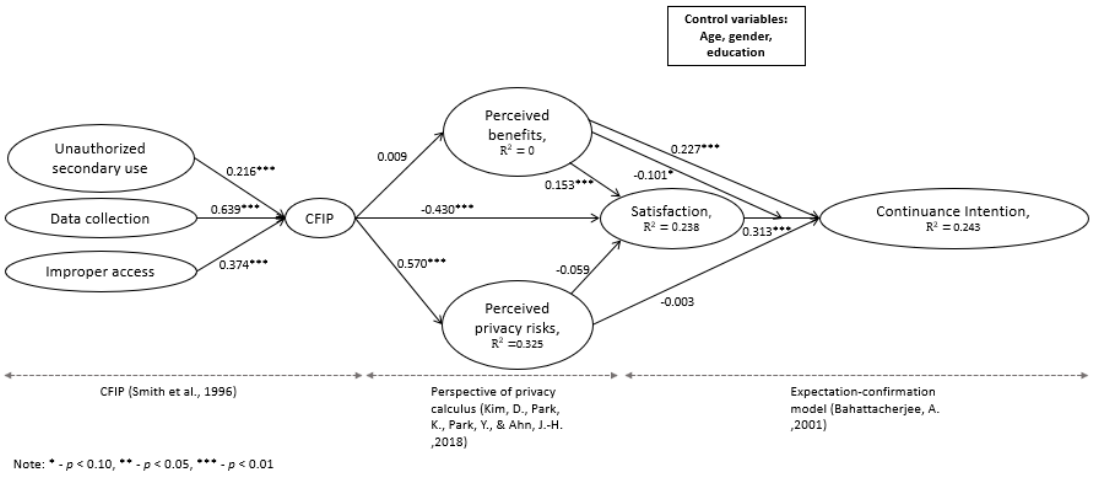

Figure 2 – Research model including path coefficients.

The results show that the constructs that explain the second-order construct (CFIP): unauthorized secondary use (US), improper access (IA) and data collection (DC) are statistically significant and have a positive influence in concerns for information privacy therefore supporting H1($\hat{\beta}$ = 0.216 ; ρ < 0.01), H2 ($\hat{\beta}$ = 0.639 ; ρ < 0.01) and H3 ($\hat{\beta}$ = 0.374 ; ρ < 0.01) respectively, as it can be seen in **Table 4**. Concerning the CFIP, and as expected, the second-order construct has a positive influence on the perceived privacy risks (PR) as described in H5, being this hypothesis statistically significant; however, the hypothesis described in H4 is not statistically significant, so CFIP has no influence in the perceived benefits (PB) yet, the same does not occur regarding the satisfaction: CFIP has a negative influence in satisfaction (S), supporting H10.

Satisfaction (S) and perceived benefits (PB) positively influence the continuance intention (CI) to disclose personal information to use mobile apps for free, supporting H11 ($\hat{\beta}$ = 0.227 ; ρ <

0.01) and H6 ($\hat{\beta}$ = 0.313 ; ρ < 0.01), in line with those findings, perceived benefits (PB) have a positive influence on satisfaction(S) supporting also H8 ($\hat{\beta}$ = 0.153 ; ρ < 0.01) however, the moderation effect of perceived benefits (PB) on the effect of satisfaction (S) on continuance intention (CI) has a negative path coefficient ($\hat{\beta}$ = -0.101 ; ρ < 0.10) leading to H12 not being supported. Surprisingly, H7 was not supported since the effect of perceived privacy risks (PR) on the continuance intention (CI) is not statistically significant.

Age, gender, and education were used as control variables, only age was found to be statistically significant, having a negative influence on the continuance intention to disclose personal information for free mobile apps use.

Table 4 – Results of hypothesis testing.

Hyp	Independent variable	Dependent variable	Findings	Support
H1	Unauthorized secondary use	CFIP	Positive and statistically significant ($\hat{\beta}$ = 0.216; ρ < 0.01)	Supported
H2	Data collection	CFIP	Positive and statistically significant ($\hat{\beta}$ = 0.639; ρ < 0.01)	Supported
H3	Improper access	CFIP	Positive and statistically significant ($\hat{\beta}$ = 0.374; ρ < 0.01)	Supported
H4	CFIP	Perceived Benefits	Non-significant effect ($\hat{\beta}$ = 0.009; ρ > 0.10)	Not supported
H5	CFIP	Perceived privacy risks	Positive and statistically significant ($\hat{\beta}$ = 0.570; ρ < 0.01)	Supported
H6	Perceived Benefits	Continuance intention	Positive and statistically significant ($\hat{\beta}$ = 0.227; ρ < 0.01)	Supported
H7	Perceived privacy risks	Continuance intention	Non-significant effect ($\hat{\beta}$ = -0.003; ρ > 0.10)	Not supported
H8	Perceived Benefits	Satisfaction	Positive and statistically significant ($\hat{\beta}$ = 0.153; ρ < 0.01)	Supported
H9	Perceived privacy risks	Satisfaction	Non-significant ($\hat{\beta}$ = -0.059; ρ > 0.10)	Not supported
H10	CFIP	Satisfaction	Negative and statistically significant ($\hat{\beta}$ = -0.430; ρ < 0.01)	Supported
H11	Satisfaction	Continuance intention	Positive and statistically significant ($\hat{\beta}$ = 0.313; ρ < 0.01)	Supported
H12	Perceived benefits x Satisfaction	Continuance intention	Negative and statistically significant ($\hat{\beta}$ = -0.101; ρ < 0.10)	Not supported (Significant but negative effect is observed)

6. DISCUSSION

6.1. DISCUSSION OF FINDINGS

The present study aims to understand the tradeoff mobile app users are willing to make between the disclosure of their personal information and the free use of mobile apps, considering the benefits, satisfaction, and risks they perceive from that trade-off. **Table 4** reports the hypotheses and the findings regarding the proposed model.

As expected, CFIP was proven to be a second-order construct of data collection, improper access, and unauthorized secondary use. Eight of the 12 hypotheses in our model were confirmed, three were not, whereas one was confirmed but against what we initially expected.

Our results suggest that the proposed constructs having a stronger influence in the continuance intention to disclose personal data for the free use of mobile apps are the ones related to the positive outcomes for the individual, namely perceived benefits (PB) and satisfaction (S). The satisfaction and the benefits perceived by a mobile app user will be a stronger influence than any risks that they could perceive for making the choice to continue engaging in this new social contract. The satisfaction of continuously doing the tradeoff of personal information to get access for free to a mobile app is the most significant effect found to explain the disclosure, showing that people are pleased with these conditions and intent to repeat them. As similar studies that use the expectation-confirmation theory suggests, the satisfaction plays a major influence in continuance intention (Bhattacherjee, 2001; Sarkar & Khare, 2019; Tam, Santos, & Oliveira, 2020).

There is a curious finding regarding the effects of perceived benefits and satisfaction on continuance intention to disclose personal information, seems like mobile app users when they perceive higher benefits with the access for free to a mobile app by disclosing their personal information, they don't need to be satisfied with the tradeoff to have the intention to continuing doing it. Nevertheless, and in line with previous studies (see, e.g., Han et al., 2018), when people have a higher expectation of the benefits that the transaction can bring, they feel more satisfied in doing it. Satisfaction, however, is strongly influenced by the concerns for information privacy (CFIP), which translates to that people can't feel satisfied with engaging or continuously engaging in these terms because they know the impacts it can have on their information privacy.

This study also indicates that the risks that a mobile app user perceives do not influence their decision on the disclosure of personal information, this finding contradicts similar studies regarding the risks perceived in disclosing personal information (Dinev & Hart, 2006; Keith et al., 2013) however, Wang et al. (2016) had already noted in their study that the perceived risks had a smaller influence. These conclusions illustrate that people do not consider the risks that disclosing personal information can have or there is not enough information for them to make an informed decision regarding their data. The apparent contempt by people to understand/acknowledge the privacy risks was also noticed by Alessandro Acquisti et al. (2017) who stated that this phenomenon can be due to people underestimating the probability of those privacy risks occurring to them. However, Berendt, Günther, & Spiekermann (2005) findings also support this finding stating that online users will provide personal information easily without considering the privacy concerns, stating that even if users care about their privacy they will not act accordingly, leading to privacy concerns having no impact on behavior. Also, curiously, CFIP influence Satisfaction but perceived privacy risks do not influence satisfaction, this can translate to people being overall concerned about information privacy but not aware of the risks that could be potentiated by their actions, leading to only the concerns affecting negatively the satisfaction.

The results showed that age is negatively associated with the continuance intention to disclose personal information for free mobile apps use, highlighting that older people seem to have more reticence in continuing disclosing personal information to mobile apps. This finding can be

explained since previous literature support that older people have more concerns about privacy overall (Bellman et al., 2004) what can indicate that they demonstrate more concerns in disclosing personal information due to the privacy risks that could initiate.

6.2. THEORETICAL IMPLICATIONS

Focusing on the theoretical implications this study can bring, three main points can be highlighted. First, this research is a combination of three different known models: CFIP, privacy calculus and ECM adapted to the theme of mobile apps and focusing on the intention to satisfaction with free mobile apps and the continuance intention to disclose personal information to use it, in the best of our knowledge this combination of models was not used before and could add more insights regarding the continue intention to disclose personal information for the free use of mobile apps.

Second, the findings suggest that there are parts of these models that complement each other providing additional information to understand the thinking process that each free mobile app user goes through when confronted with mobile apps asking for personal information, namely the effect of perceived benefits and satisfaction on the continuance intention, so it is suggested that these three models together should be an important part to explain the continuance intention to disclose personal information for the free use of mobile app instead of using only one of them.

Finally, while previous studies only focused on the theme of privacy in mobile apps in specific areas like medical (Kotz et al., 2016), or focusing on the requests made during the app download (Wottrich et al., 2018) and app permissions asked (Gu et al., 2017) or specific for some mobile apps (Fife & Orjuela, 2012); This study differs from them because it focuses on the privacy tradeoff that the intention to disclose personal information to use mobile apps for free can be, fulfilling the gap that existed regarding this specific theme and adding the knowledge needed to compare the different behavior an individual has in this case and in other similar scenarios of privacy in mobile apps.

6.3. PRACTICAL IMPLICATIONS

This study contributes with potentially important insights regarding the theme of mobile apps for mobile app providers, companies, policymakers or even non-governmental organizations (NGOs). First, this study showed that mobile app users do not take into consideration the privacy risks that can advert from using a certain mobile app where it is needed to disclose personal information for its use, focusing only on the positive outcomes that action can lead to, in this case, the perceived benefits and the satisfaction. This indicates that mobile app users are more concerned regarding the benefits that can advert with respect to the risks. Thus, mobile app providers should emphasize the benefits of using their mobile app in order to obtain the most adherence when publicizing it.

Second, this study also showed that the effect of the satisfaction decreases when the perceived benefits are higher in a mobile app user, which means that a user who perceives many benefits

with the tradeoff of personal data for using mobile apps for free do not need to be widely satisfied to pursue the tradeoff, this is an important insight for mobile app providers and companies since, while divulging the mobile app, they should focus differently on users with less and more mobile apps in a way that the first ones are likely to adhere even if they do not feel satisfied in doing the tradeoff but perceive enough benefits that compensate disclosing personal data for the free use of the mobile app.

Finally, it is noticed that the perceived privacy risks have no statistical influence in the continuance intention to disclose personal information for the free use of the mobile app what is an important red flag to be considered by policymakers and non-governmental organizations. Policymakers must emphasize the importance of privacy through the creation of specific laws to narrow the amount of personal information collected by mobile apps. Regarding the NGOs, they should create privacy awareness through campaigns, informing the importance of understanding the privacy implications before agreeing to them and providing examples of the consequences it can have in the long term, those campaigns should also focus on the lack of understanding experienced by mobile app users of what privacy means and what it englobes since many people still think privacy is only for those who have "something to hide" (Solove, 2007) being that one of the reasons for disclosing personal information for mobile apps so easily.

6.4. LIMITATIONS AND FURTHER RESEARCH

This research has limitations that should be noted for further studies. First, the research model was tested in a sample of the Portuguese population, which demands some caution in the generalization of the results to other contexts. A larger sample should be considered as well as a larger variety of cultures, nationalities, and ages. Also, the questionnaire being applied exclusively online, is relying on the online respondents and the sample may be exposed to self-selection bias, however, a question was included to control the bias.

Second, the variance explained by the proposed model is not ideal to explain the continuance intention to disclose personal information for the free use of mobile apps, leading to possibilities for further studies to analyze that gap and understand which variables could contribute to a better understanding; it would be interesting to analyze if the type of information requested and the perceived critical mass have an impact of continuance intention.

Finally, it would be interesting for further studies to explore more in deep the moderation effect that the perceived benefits and satisfaction have on the continuance intention to disclose personal information for the free use of mobile apps since it is a topic that, in the best of my knowledge, was not contemplated before and could lead to a better understanding of the decision process experienced by mobile app users since it showed to be a significant effect.

7. CONCLUSIONS

The growth of the mobile app world and the competition to attract possible downloads lead to the creation of a new social contract to offer mobile apps for free. But what are the implications

for the users of mobile apps? Privacy tradeoff. This study acknowledges that users when considering the use of mobile apps do not consider the privacy risks that could arise from providing their personal information, focusing more on the benefits and satisfaction. This study contributes to future research by providing new insights regarding the interaction between the perceived benefits and satisfaction, joining three different theories ECM, CFIP, and privacy calculus. In summary, the findings of the study suggest that there is contempt by the individuals for their data privacy, leading to tradeoffs that could be prejudicial because most individuals are focused on the benefits and the satisfaction that the use of the mobile app can bring. Finally, this study also shows that mobile apps users, when they perceive large benefits with the trade-off, do not need to be satisfied with disclosing personal data for the free use of mobile apps to continue on doing it.

8. BIBLIOGRAPHY

Acquisti, Alessandro, Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., … Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *50*(3). https://doi.org/10.1145/3054926

Acquisti, Alessandro, John, L. K., Loewenstein, G., Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth ? *The Journal of Legal Studies*, *42*(2), 249–274.

Acquisti, Alfssandro, & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy*, Vol. 3, pp. 26–33. https://doi.org/10.1109/MSP.2005.22

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*. https://doi.org/10.1007/BF02723327

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*(February 2019), 55–69. https://doi.org/10.1016/j.tele.2019.03.003

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

Beldad, A., & Citra Kusumadewi, M. (2015). Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. *Computers in Human Behavior*, *49*, 102–110. https://doi.org/10.1016/j.chb.2015.02.047

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce : Stated preferences vs. actual behavior. *Communications of the ACM*. https://doi.org/10.1145/1053291.1053295

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly: Management Information Systems*, *25*(3), 351–370. https://doi.org/10.2307/3250921

Choi, J. P., Jeon, D. S., & Kim, B. C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, *173*, 113–124. https://doi.org/10.1016/j.jpubeco.2019.02.001

Cooper, R., Assal, H., & Chiasson, S. (2018). Cross-national privacy concerns on data collection by government agencies (short paper). *Proceedings - 2017 15th Annual Conference on Privacy, Security and Trust, PST 2017*, 191–196. https://doi.org/10.1109/PST.2017.00030

Coull, S. E., & Dyer, K. P. (2014). Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond. *ACM SIGCOMM Computer Communication Review*, *44*(5), 5–11. https://doi.org/10.1145/2677046.2677048

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer

attitudes toward secondary information use. *MIS Quarterly: Management Information Systems*, *17*(3), 341–361. https://doi.org/10.2307/249775

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*(April 2019), 261–272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

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

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

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS Detecting privacy leaks in iOS applications. *Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS)*, 11.

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*(1), 1–10. https://doi.org/10.5772/51645

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European Data Protection: Coming of Age*. https://doi.org/10.1007/978-94-007-5170-5_1

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology*, *7*(4), 185–200. https://doi.org/10.1007/s10676-006-0001-7

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, *53*, 344–353. https://doi.org/10.1016/j.chb.2015.06.048

Fornell, C., & Larcker, D. F. (1981). SEM with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, Vol. 18, pp. 382–388.

Gilbert, P., Chun, B. G., Cox, L. P., & Jung, J. (2011). Vision: automated security validation of mobile apps at app markets. *Proceedings of the Second International Workshop on Mobile Cloud Computing and Services*, 21–26. Retrieved from http://appanalysis.org/jjung/jaeyeon-pub/appvalidation.pdf

Gomez, J., Pinnick, T., & Soltani, A. (2009). *KnowPrivacy: The Current State of Web Privacy, Data Collection, and Information Sharing*. Retrieved from http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing*, *19*(4), 302–318. https://doi.org/10.1108/07363760210433627

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Han, M., Wu, J., Wang, Y., & Hong, M. (2018). A model and empirical study on the user's continuance intention in Online China Brand communities based on customer-perceived benefits. *Journal of Open Innovation: Technology, Market, and Complexity*, *4*(4), 1–20. https://doi.org/10.3390/joitmc4040046

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

Hin, S. (2015). Consumer Personality, Privacy Concerns and Usage of Location-Based Services (LBS). *Journal of Economics, Business and Management*, *3*(10). https://doi.org/10.7763/joebm.2015.v3.316

Hsiao, C. H., Chang, J. J., & Tang, K. Y. (2016). Exploring the influential factors in continuance usage of mobile social Apps: Satisfaction, habit, and customer value perspectives. *Telematics and Informatics*, *33*(2), 342–355. https://doi.org/10.1016/j.tele.2015.08.014

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Hui, Teo, & Lee. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, *31*(1), 19. https://doi.org/10.2307/25148779

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56–59. https://doi.org/10.1109/MC.2018.3191268

Jeff Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly: Management Information Systems*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My data just goes everywhere": User mental models of the internet and implications for privacy and security. *Symposium on Usable Privacy and Security (SOUPS) 2015*, 39–52.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Proposing and testing an improved research methodology for capturing behaviour. *International Journal of Human Computer Studies*, *71*, 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Kifer, D., & Machanavajjhala, A. (2011, June 14). *No free lunch in data privacy*. 193. https://doi.org/10.1145/1989323.1989345

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is there an app for that? *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security*. https://doi.org/10.1145/2078827.2078843

Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems*, *119*(August 2018), 46–59. https://doi.org/10.1016/j.dss.2019.02.007

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy Security in Mobile Health: A research agenda. *Computer*, 22–30. Retrieved from http://seclab.illinois.edu/wp-content/uploads/2016/07/kotz2016privacy.pdf

Krishnamurthy, B., & Wills, C. E. (2007). *Generating a privacy footprint on the internet*. 65. https://doi.org/10.1145/1177080.1177088

Landau, S. (2015). Control use of data to protect privacy. *Science*, *347*(6221), 504–506. https://doi.org/10.1126/science.aaa4961

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, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Liu, Y. (2014). User control of personal information concerning mobile-app: Notice and consent? *Computer Law and Security Review*, *30*(5), 521–529. https://doi.org/10.1016/j.clsr.2014.07.008

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies. *Journal of Retailing*, *88*(4), 542–555. https://doi.org/10.1016/j.jretai.2012.08.001

Mai, J. E. (2016). Big data privacy: The datafication of personal information. *Information Society*. https://doi.org/10.1080/01972243.2016.1153010

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

Martínez-pérez, B., Torre-díez, I. De, & López-coronado, M. (2014). *Privacy and Security in Mobile Health Apps : A Review and Recommendations Privacy and Security in Mobile Health Apps : A Review and Recommendations*. (December). https://doi.org/10.1007/s10916-014-0181-3

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, Personal Information Privacy, and Regulatory Approaches. *Communications of the ACM*, *38*(12), 65–74. https://doi.org/10.1145/219663.219683

Modahl, M. (2000). Now or never: how companies must change today to win the battle for Internet consumers. *Choice Reviews Online*. https://doi.org/10.5860/choice.37-4588

Murphy, R. S. (1996). Property Rights in Personal Information: An Economic Defense of Privacy.

Georgetown Law Journal. https://doi.org/10.4324/9781315246024-4

Ofori, K. S., Larbi-Siaw, O., Fianu, E., Gladjah, R. E., & Boateng, E. O. Y. (2015). Factors influencing the continuance use of mobile social media: The effect of privacy concerns. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.426

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *1991*.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*. https://doi.org/10.1037/0021-9010.88.5.879

Rahman, M., Carbunar, B., & Banik, M. (2013). *Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device*. https://doi.org/10.1109/TMC.2015.2418774

Sarkar, S., & Khare, A. (2019). Influence of Expectation Confirmation, Network Externalities, and Flow on Use of Mobile Shopping Apps. *International Journal of Human-Computer Interaction*, *35*(16), 1449–1460. https://doi.org/10.1080/10447318.2018.1540383

Savage, S. J., & Waldman, D. M. (2015). Privacy tradeoffs in smartphone applications. *Economics Letters*, *137*, 171–175. https://doi.org/10.1016/j.econlet.2015.10.016

Schawrtz, P. M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*, *117*(7), 2055. https://doi.org/10.1525/sp.2007.54.1.23.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, *45*(December 2017), 44–55. https://doi.org/10.1016/j.ijinfomgt.2018.10.024

Sipior, J. C., Ward, B. T., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*, *26*(6), 661–678. https://doi.org/10.1108/JEIM-07-2013-0043

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly: Management Information Systems*, *20*(2), 167–195.

Solove, D. (2007). "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*, *44*(4), 745.

Solove, D. (2008). *Understanding privacy*. Harvard university press.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97

Straße, S., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of information technology*, *25*(2), 109–125.

Tam, C., Santos, D., & Oliveira, T. (2020). Exploring the influential factors of continuance intention to use mobile Apps: Extending the expectation confirmation model. *Information Systems Frontiers*, *22*(1), 243–257. https://doi.org/10.1007/s10796-018-9864-5

Tang, A. K. Y. (2019). A systematic literature review and analysis on mobile apps in m-commerce: Implications for future research. *Electronic Commerce Research and Applications*, *37*. https://doi.org/10.1016/j.elerap.2019.100885

Taylor, D., Voelker, T., & Pentina, I. (2011). *Mobile Application Adoption by Young Adults: A Social Network Perspective*. *6*(2), 60–71. Retrieved from http://digitalcommons.sacredheart.edu/wcob_fac/1/

Tene, O., & Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, *64*, 63. https://doi.org/10.5121/ijgca.2012.3203

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

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business and Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Yang, H. C. (2013). Bon appétit for apps: Young American consumers' acceptance of mobile applications. *Journal of Computer Information Systems*, *53*(3), 85–96. https://doi.org/10.1080/08874417.2013.11645635

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information and Management*, *56*(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems*, *48*(2), 395–406. https://doi.org/10.1016/j.dss.2009.10.003

Zimmer, M. (2010). "But the data is already public": On the ethics of research in Facebook. *Ethics and Information Technology*, *12*(4), 313–325. https://doi.org/10.1007/s10676-010-9227-5

Zwitter, A. (2014). Big Data ethics. *Big Data & Society*, *1*(2), 393–432. https://doi.org/10.1177/2053951714559253

9. APPENDIX

Table A1 – Instrument

Construct	Code	Description	Source
Unauthorized secondary use	US1	Mobile apps should not use personal information to any purposes unless it has been authorized by the individuals who provide information	(Smith, Milberg, & Burke, 1996)
	US2	When people give personal information to a mobile app for some reason, the mobile app should not use the information.	
	US3	Mobile apps should never sell the personal information in their computer databases to other entities.	
	US4	Mobile apps should never share personal information with other entities unless it has been authorized by the individuals who provided the information.	
Improper access	IA1	Mobile apps should devote more time and effort to preventing unauthorized access to personal information	
	IA2	Databases that contain personal information should be protected from unauthorized access.	
	IA3	Mobile apps should take more steps to make sure that unauthorized people cannot access personal information in their databases	
Data collection	DC1	It usually bothers me when mobile apps ask me for personal information	
	DC2	When mobile apps ask me for personal information, I sometimes think twice before providing it	
	DC3	It bothers me to give personal information to so many mobile apps	
	DC4	I'm concerned that mobile apps are collecting too much personal information about me	
Perceived Benefit	PB1	Using mobile apps improves my performance	(Hsu & Lin, 2016; Sun et al., 2015)
	PB2	Using mobile apps enhances my effectiveness.	
	PB3	Using mobile apps enables me to accomplish my tasks more quickly.	
	PB4	Using mobile apps helps me get useful information.	
	PB5	Using mobile apps is very useful for me.	
Perceived privacy risk		You believe there is a risk associated to the possibility that personal information... tracked by free mobile apps…	(Dinev & Hart, 2006; Kowatsch & Maass, 2012; Sun et al., 2015)
	PR1	... could be sold to third parties (entities that do not participate directly in the app).	
	PR2	... could be misused.	
	PR3	... could be made available to unknown individuals or companies without your knowledge.	
	PR4	... could be made available to governmental agencies.	
	PR5	... could be jeopardized by hacking activities.	
Satisfaction		How do you feel about your overall experience disclosing personal data for the free use of mobile apps use?	(Bhattacherjee, 2001)
	S1	Very dissatisfied/Very satisfied.	
	S2	Very displeased/Very pleased.	
	S3	Very frustrated/Very contented.	
	S4	Absolutely terrible/Absolutely delighted.	
Continuance Intention		In order to continue using mobile apps for free…	(Venkatesh, Thong, & Xu, 2012)
	CI1	I intend to continue disclosing my personal information.	
	CI2	I will always try disclosing my personal information.	
	CI3	I plan to continue disclosing my personal information.