Akseli Liljander

ATTITUDES TOWARDS BIOMETRIC AUTHENTICATION TECHNOLOGIES BETWEEN CULTURES: ACCEPTANCE IN FINLAND AND BRAZIL

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

ABSTRACT

Liljander, Akseli
Attitudes Towards Biometric Authentication Technologies Between Cultures: Acceptance in Finland And Brazil
Jyväskylä: University of Jyväskylä, 2019, 117 pp.
Information Systems, Master's Thesis
Supervisor(s): Woods, Naomi

Biometric authentication is based on the physical qualities, such as fingerprint or eye, of the user. Biometrics do not need remembering and cannot be stolen or lost. However, new types of problems and threats concern biometrics. Biometrics are also not always accepted by users. Acceptance may vary between countries and cultures. Most biometrics acceptance research has been conducted in Europe and North America. South America is an emerging key market of biometrics, but no studies on biometrics acceptance have been conducted there. An extended Technology Acceptance Model (TAM) and Hofstede's cultural dimension theory were combined in a quantitative survey to compare familiarity, knowledge and acceptance of biometrics between Brazil and Finland. Intention to use, familiarity and knowledge of biometrics were higher in Brazil. Most hypothesized TAM-relationships were found in at least one of the countries, but the model was not completely repeatable in either. Brazilian respondents perceived biometrics as more useful when they had a higher need for security, and they saw involving their body in the authentication process less invasive than their Finnish counterparts. Unlike Brazilians, The Finnish respondents did not favor biometrics as a way of increasing their personal security nor see ease of use as a strong enough factor to directly affect usage intentions. Hofstede's dimensions did not provide a clear explanation for the differences in acceptance formation. Some espoused cultural values affected the intention to use biometrics indirectly. The results offer valuable implications for future biometrics acceptance research and in practice for introducing biometric products in different cultural contexts.

Keywords: biometric authentication, technology acceptance, culture, Technology Acceptance Model, Hofstede's cultural dimensions, Brazil, Finland

TIIVISTELMÄ

Liljander, Akseli
Kulttuurienväliset asenteet biometrisen todennuksen teknologioita kohtaan: hyväksyntä Suomessa ja Brasiliassa
Jyväskylä: Jyväskylän yliopisto, 2019, 117 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Woods, Naomi

Biometrinen todennus hyödyntää käyttäjän fyysisiä ominaisuuksia, kuten sormenjälkeä tai silmää. Biometristä tunnistetta ei tarvitse muistaa, eikä sitä voi unohtaa tai varastaa. Uudenlaiset ongelmat ja uhat kuitenkin koskettavat biometriaa. Käyttäjät eivät myöskään aina hyväksy biometriaa. Hyväksyntä voi vaihdella maiden ja kulttuurien välillä. Suurin osa biometrian hyväksynnän tutkimuksesta on toteutettu Euroopassa ja Pohjois-Amerikassa. Etelä-Amerikka on nouseva biometrian keskeinen markkina-alue, mutta siellä ei ole toteutettu tutkimuksia biometrian hyväksynnästä. Brasiliaa ja Suomea vertailtiin kvantitatiivisessa kyselytutkimuksessa, jossa yhdistettiin Technology Acceptance Model (TAM) -malli ja Hofsteden teoria kulttuurin ulottuvuuksista. Aikomus käyttää, tuttuus ja tietoisuus biometriaa koskien olivat korkeampia Brasiliassa. Suurin osa oletetuista TAM-mallin riippuvuussuhteista löydettiin vähintään yhdessä maassa, mutta malli ei ollut täysin toistettavissa kummassakaan niistä. Brasilialaiset vastaajat kokivat biometrian hyödyllisempänä, kun heillä oli korkeampi turvallisuuden tarve, ja he näkivät oman kehonsa sisällyttämisen autentikointiprosessissa vähemmän tunkeilevana kuin suomalaiset. Toisin kuin brasilialaiset, suomalaiset vastaajat eivät suosineet biometriaa tapana parantaa henkilökohtaista turvallisuuttaan, eivätkä nähneet helppokäyttöisyyttä tarpeeksi vahvana tekijänä vaikuttamaan käyttöaikeisiin. Hofsteden dimensiot eivät tarjonneet selkeää selitystä hyväksynnän muodostumisen eroille maiden välillä. Jotkut omaksutut kulttuuriarvot vaikuttivat epäsuorasti biometrian käyttöaikeisiin. Tuloksia voidaan hyödyntää tulevassa biometrian hyväksynnän tutkimuksessa, sekä käytännössä tuodessa biometrisia tuotteita markkinoille eri kulttuuriympäristöissä.

Asiasanat: biometrinen todennus, teknologian hyväksyntä, kulttuuri, Technology Acceptance Model, Hofsteden kulttuurin ulottuvuudet, Brasilia, Suomi

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

One of the fundamental problems in computer security is how to authenticate a user to a computer system conveniently and securely (Shay et al., 2010). Identification and authentication measures are traditionally centered on utilizing something the user knows, something the user has or something the user is (Schneier, 2015). The user authentication methods based on physical qualities of the user are called biometric authentication methods.

Remembering more than 4-5 passwords is difficult to users and long passwords and secure authentication tasks can be especially problematic for people with disabilities and older adults (Adams & Sasse, 1999; Kowtko, 2014). Replacing complex passwords with hardware devices or tokens has been expensive, inconsistent and ultimately only resulted in replacing an unmanageable amount of passwords by an unmanageable amount of different devices (Smith, Wiliem, & Lovell, 2015). Biometric authentication can work as an alternative to passwords as they do not need to be remembered (Rane, Want, Draper & Ishwar, 2013). Biometric traits can neither be stolen, lost or forgotten (Buciu & Gacsadi, 2016). Biometrics can create a more convenient, reliable and thus less costly alternative to password as an authentication solution (Skaff, 2007).

Biometric authentication can provide usability advantages for users over traditional authentication methods. However, using physical means on identifying oneself also brings new problems and threats compared passwords and other traditional authentication methods. Biometric credentials can reveal sensitive information of the users, such as race, gender or an illness (Phillips, Zou, & Li, 2017). Providing biometric data to a company might risk one's privacy and might eventually lead even to illegal spying by governments or law enforcement agencies (Memon, 2017). Biometric technologies can become expensive in the name of computational capacity needed or the required equipment, and might require a lot of maintenance and suffer of credibility problems (Liang, Fleming, & Wang, 2014). And while security advantages can be accomplished by using biometric technologies, they also create new security problems. Biometrics are not secret, but in fact exposed all the time (Hamid, 2015). Biometrics are permanently associated with user and cannot be replaced (Patel, Ratha, & Chellappa, 2015).

Biometric systems can be fooled by presenting a fake sample such as a silicon finger or a face mask (El-fishawy, 2015). User acceptance and attitudes towards using biometrics can also become barriers for adoption of biometrics.

Various challenges emerge when information technologies developed in western cultures are introduced elsewhere (Riley et al., 2009). Training manuals, advertising campaigns, face-to-face contacts and other communication regarding the introduction of a technology should carry different messages in different cultures (Schepers & Wetzels, 2007). The acceptance of biometric authentication can vary greatly between different countries, cultures, groups and demographic backgrounds. For an example, certain groups of users, such as religious and civil-liberties groups have rejected biometric technologies because of privacy concerns (Liu & Silverman, 2001). In some cultures there is aversion to touching public surface and in those countries applying a biometric method requiring contact would not be preferred (El-Abed, Giot, Hemery, & Rosenberger, 2010).

1.1 Research problem

This study is the first step in resolving the problem of the lack of user acceptance research of biometric authentication technologies in South America. User centered perspective in biometrics research has been limited and most of it has been conducted in European context (Riley et al., 2009). Many studies regarding acceptance of biometrics in North America exist too, and Africa and Asia are represented in some papers. However, no academic studies have been conducted regarding the attitudes towards biometrics in South America, despite the pioneering usage and large markets of biometrics in the continent. South America is one of the emerging key regions of biometrics, with Brazil taking the biggest share of the continent's biometrics market (IriTech, inc., 2015). Fingerprint identification for criminal inspection purposes was used for the first time in Argentina in 1891, beginning the early cataloging of fingerprints (Onin.com, 2017). Developing countries in South America have incorporated biometrics in their identity management systems or used them to support public service delivery, and Brazil already replaced their traditional ID card with biometrics enhanced registry in the beginning of the 20th century, and later adopted biometrics in driving licenses, e-passports and automated border control (IriTech, inc., 2015). Companies have found budding markets for using fingerprint technology on ATM's all over South America (Hannah, 2005). About a half of all the countries in South America, including Brazil, use biometric voter registration in elections (International IDEA, 2017). Research is needed to explain, how the attitudes towards biometric technologies are formed in South America, and what cultural features have possibly allowed or contributed to the broad and pioneering adaption of biometric technologies in the continent. This study extends the user centered biometrics acceptance research to Brazil, which is the South American market leader of biometric technologies.

1.2 Motivation and objectives

To cross-culturally compare the acceptance of biometrics with Brazil, Finland was chosen as a country, which differs from Brazil in the name of history, geographical location, national identity development, cultural cluster and Hofstede's cultural dimensions. Finland belongs to Europe, where biometrics and their acceptance have already been extensively studied.

There is a need for a thorough research on the differences in biometrics attitudes between different cultures. The present empirical study will contribute to the field of user-oriented biometrics research by expanding the technology acceptance research to Brazil and conducting more research in Finland. It is the first step towards understanding the acceptance and use of biometric technologies in South America and builds to the overall understanding of the cultural and regional differences in the acceptance and use of biometrics. The study uses the most popular frameworks of culture and technology acceptance research, Hofstede's cultural dimension theory and the Technology Acceptance Model, in order to add comparable results to the existing knowledge of attitudes towards biometric authentication technologies in different parts of the world. The thesis wishes to answer the following research questions:

1. Is there a difference in familiarity and knowledge of biometrics between Finland and Brazil?
2. How is the acceptance of biometrics formed in Finland and in Brazil?
3. Is there a cultural difference in the biometrics acceptance between Finland and Brazil?

The results can contribute to the research of cultural differences in biometrics acceptance, and potentially to the organizational biometrics-related product development, implementation, marketing or communication in the studied countries.

1.3 Central concepts

The theoretical foundation of the present study can be divided into three important general categories. The study examines on technology acceptance between cultures, concentrating on biometric authentication as a specific area of technology. Biometric authentication technologies, technology acceptance and culture are therefore concepts that need to be defined.

1.3.1 Biometric authentication

Authentication is the process of confirming the correctness of the claimed identity (SANS Institute, 2018). Human-by-machine authentication, or user

authentication signifies the verifying of the validity of a claimed user (Gorman, 2003). Authentication is typically the first step toward confirming that a user is authorized to perform a requested action (Shay et al., 2010). User authentication is used to grant the user an access to a network or equipment that is tailored to the user or to make defined actions (Braz & Robert, 2006). The World Wide Web has added new complication to the once simple task of authentication by granting attackers an access to one's records without the need for physical presence (Gorman, 2003).

The classic division of authentication methods into something the user knows, something the user has and something the user is, includes some problems. For an example, passwords are not strictly known, but rather memorized, and thus can be forgotten in short or long periods of time (Gorman, 2003). Gorman (2003) suggests the use of a division between Knowledge-Based Authenticators, Object-Based Authenticators and ID-Based Authenticators. Gorman (2003) includes biometrics in the category of ID-Based Authenticators, since he does not believe biometric traits to signify one's true self any more than hair color or body build for an example.

Biometric authentication methods can be divided in physiological and behavioral methods. Physical methods involve physical parts of ones' body in the authentication, by utilizing fingerprints, iris of the eye or face for an example. Behavioral methods include methods such as recognition of gait, voice or signature. (Buciu & Gacsadi, 2016). However, for an example, a voice of a person is formed in addition to behavior by physical factors, and learned behavior affects how a finger is presented to a scanner and how a person looks at a camera, making this division quite artificial (Faundez-Zanuy, 2006). Biometrics can also be categorized based on other features, such as whether the signal produced by the biometric sample is alterable or stable over time (Gorman, 2003). Types of authenticators can be combined into multifactor authentication to enhance security (Gorman, 2003) and thus multiple biometric technologies can be combined into multifactor biometrics.

According to Clarke (1994), a desirable biometric characteristic should be universal, unique and exclusive, permanent through life, indispensable, collectable, digitally storable, precise, easy and efficient to record, and acceptable to contemporary social standards. For a biometric system and technology to be practically usable, Buciu & Gacsadi (2016) expect it to possess the characteristics of universality, uniqueness, permanence, collectability, simplicity, cost-efficiency, acceptability, scalability , resilience and for it to be able to detect attacks. The most popular biometric authentication technologies are based on fingerprint, eye iris and face. These and other methods, their application areas and the risks, benefits and impacts of applying biometric technologies in practice are discussed more in the literature review.

1.3.2 Technology acceptance

User attitude signifies the psychological state reflecting the affective or evaluating feelings towards a new system (Barki & Hartwick, 1994). Many different frameworks and models have been used to define and study the acceptance towards technical applications. From all the models proposed to explain and predict the use of a system, the Technology Acceptance Model (TAM) has captured the most attention in the information systems community (Chuttur, 2009). TAM has been selected as a more comprehensive user acceptance model to reflect real-world situations, in comparison to its alternatives, such as Theory of Reasoned Act, Unified Theory of Acceptance and Use of Technology (UTAUT), Technology Readiness and Acceptance Model (TRAM) or Diffusion of Innovation (DOI) (Kanak & Sogukpinar, 2017). TAM has been evaluated to have empirical advantage and to be easier to apply compared to for an example the Theory of Planner Behavior (TPB) (Mathieson, 1991).

TAM aims to provide a basis for tracing the impact of external variables on internal beliefs, attitudes and intentions (Legris, Ingham, & Collerette, 2003). It was first introduced by F. D. Davis (1986) and is used to measure and explain how users accept and use a technology. The original TAM is an adaptation of the principles of the Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975). It presents two key factors, perceived usefulness and perceived ease of use, affecting the attitude towards using a technology, which is a major determinant towards the actual system use. Later, a concept of behavioral intention was introduced to the model, as a precedent of actual use. In its final form, TAM also included external variables as an additional construct affecting the technology perceptions, and discarded the attitude-construct, suggesting a direct relationship between the main constructs and the behavioral intention to use a technology. The development of the model however did not end to this final form. TAM has been extended and applied into various fields of technology and different contexts of technology use. It has been used as a part of larger models and frameworks of technology acceptance and attitude research. Extensions of the model have been developed also in order to study the acceptance of biometric authentication technologies. TAM, its history, its various extensions and applications, and its utilization in biometrics acceptance research are presented in more depth later, in the literature review.

1.3.3 Culture

In cultural research, social environment, normally typified by country, is seen to define a person's learned patterns of thinking, feeling and potential acting, making culture a collective phenomenon (Hu, Chau, Liu Sheng, & Tam, 1999). In addition to the national culture, an individual's memberships in other professional, organizational, ethnic, religious and various other social groups also define the nature of their values (Straub, Loch, Evaristo, Karahanna, & Srite, 2002). Culture

is to a human collectivity what personality is to an individual (Hofstede, 1984, pp. 21).

Hofstede's (1984, pp. 21) view of culture is the collective programming of mind, which distinguishes the members of one group from people from another. Many differing definitions of culture also exist. A wide range of contradicting scholar opinions exist on the matter of which values, norms and beliefs should be used to measure the concept of culture (Straub, Keil, & Brenner, 1997).

Hofstede (1984, 2011) compares nations based on six cultural dimensions: Individualism vs. Collectivism, Power Distance, Uncertainty Avoidance, Masculinity vs. Femininity, Long Term Orientation vs. Short Term Orientation and in Indulgence vs. Restraint. His dimensions have been used to compare cultures in various contexts, and they have been associated to differences in technology acceptance between nations. The present study also utilizes this cultural dimension framework to compare Brazil and Finland, and hypothesizes certain relationships between the dimensions and the acceptance of biometrics. The cultural features specific to Finland and Brazil, their positioning on the Hofstede's cultural dimension scores, their comparability with South American and European culture, and other definitions of culture are also presented in more detail in the literature review, together with the technology acceptance differences accounted to cultural factors in earlier research.

1.4 Literature review

A comprehensive literature review was undertaken considering the topics of biometric authentication and technology acceptance, utilizing search engines such as Google Scholar, databases such as IEEE Xplore and ACM Digital Library, and the leading journals from the fields of Information Systems Sciences, Computer Sciences, Cognitive Sciences and Social Sciences. Earlier research on culture and national culture differences were also examined in order to clarify the concepts used in cross-cultural comparison of technology acceptance. The literature review aimed to shed light on backgrounds of the study field and to justify and adjust the final research questions and settings by answering the questions "How has the acceptance of biometric technologies been studied in earlier literature?" and "What kind of differences in attitudes towards biometric authentication have been found between geographical areas and cultures?". With this information, the research gaps could be identified, and the practices used in the empirical part defined better.

The literature review is a part of a student thesis, and as such some of its main goals are to synthesize the authors' understanding of the research subject and to justify future research on the topic, including the thesis in question (Okoli & Schabram, 2010). It started by looking into the current state of research on user authentication and biometric authentication technologies. Considerable amount of research was found on the usability and security of biometrics, but most of it was done with the focus on technical means and meters. The amount of user

centered biometrics research was found to be little, opening a possibility for filling a research gap on this field. The most important works were easy to identify quickly. These articles further offered valuable references from their literature reviews and theoretical foundations.

The search for a variety of geographical and cultural areas started from articles doing cross-cultural biometrics research in various geographical and cultural areas. Only few cross-cultural biometrics acceptance studies were found. The search was then done using the discovered biometrics attitude and acceptance -keywords, changing the additional keywords to consider different geographical and cultural areas each time.

The literature review categorized cultural differences in biometrics acceptance into categories of familiarity with biometrics, acceptance of biometrics and concerns and barriers to the use of biometrics. The research was found to be mostly conducted in Europe. Finland was represented only in few studies, but other Nordic countries were studied slightly more. Relatively a lot of research was also found to have been done in the North American context. In Asia, the Arab world was significantly represented. Not a lot of studies from other parts of Asia were found. The only study that mentioned biometrics attitudes or acceptance in Africa was the cross-cultural study by Riley et al. (2009). Not a single study inspecting attitudes towards biometric technologies in South or Latin American context was found, which is surprising, considering the substantial pioneering usage of biometric authentication methods in the area. The literature search was done in English, Finnish and Portuguese.

1.5 Outline of the thesis

Chapter two, the first chapter of the literature review, generally discusses biometric technologies, which is the main theme of the thesis. The chapter introduces different biometric technologies, the fields of application of biometrics and the impacts of the use of the technology. More specifically, the thesis considers the user acceptance of biometric technologies.

In chapter three, technology acceptance and the frameworks for its study are discussed, first generally and the considering biometrics specifically. The empirical part of the thesis commits a cross-cultural comparison of biometrics acceptance between Finland and Brazil, and thus clarifying cultural concepts and a review of worldwide technology acceptance literature is necessary.

In the fourth chapter, definitions of culture, and cultural traits of Finland and Brazil are introduced, followed by a review of literature considering technology acceptance in different parts of the world and the effects of cultural features on the acceptance. The models and frameworks for cross-culturally studying technology acceptance, validations of technology acceptance frameworks in different cultures, and the study of technology acceptance in Finland and Brazil are also presented. In the final parts of the literature review, the studies of biometrics acceptance in different cultural and geographical areas are presented, first

categorized by continent and then discussed under the topics of familiarity with biometrics, acceptance of biometrics and the concerns and barriers for the use of biometrics.

The empirical part of the thesis first presents the population samples used in data collection. The used research methods are then explained. Next, the results acquired from data analysis are first objectively presented and then the meanings are discussed in more detail, in the light of the research questions. The implications of the TAM-results and the impact of Hofstede's cultural dimension scores on technology acceptance are discussed separately. Further on, the research contributions and implications to practice are reflected, the limitations of the study considered, and based on this all, directions for future research are suggested. In the closing chapter, the final conclusions of the research are declared.

2 BIOMETRICS

This chapter will introduce biometric authentication and earlier research related to biometrics. The chapter is divided into the introduction to the types of biometric technologies and to the benefits, challenges and uses of biometrics. Most attention is paid to the methods that have gained the greatest attention in previous literature: fingerprint, eye iris and face recognition.

2.1 Biometric authentication methods

Among fingerprints, iris and face biometrics, other physiological methods are e.g. facial thermography, hand geometry, ear geometry, eye retina recognition and vascular pattern recognition (Buciu & Gacsadi, 2016). In addition to gait, voice and signature, behavioral methods can also include for an example keystroke analysis -based authentication or mouse dynamics (Buciu & Gacsadi, 2016). Fingerprint, iris and face recognition are the methods that are most used and that have gained most attention to in earlier literature (Jain, 2007; Kowtko, 2014).

Fingerprint recognition is the oldest, most widely used, and the first computer aided biometric authentication method (Faundez-Zanuy, 2006; Rathod, Iyer & Meena, 2015). A fingerprint sample can be gathered via various types of sensors or even digital cameras, and a finger-based sample can also be collected from e.g. its pattern of veins (Al-Alem, Alsmirat, & Al-Ayyoub, 2017; Kathuria, 2010). Previous research mentions as some of fingerprint authentication's limitations to be interference of environmental factors (e.g. too oily, wet or warm fingerprint), skin conditions and deformation, placement errors or sensor noise from worn surface coatings (Faundez-Zanuy, 2006; Ito et al., 2005; Zhou, Hu, Petersen, Wang, & Bennamoun, 2014). Security concerns have been raised as fingerprint systems have been spoofed by artificial fingerprints created of common materials (Yuan, Sun, & Lv, 2016). However, the sample coming from a living being can be assured by scanning the blood vessels in the sample, by liveness detection algorithms or by sensing capacitance and pulses from human fingers

(Kunnil, Pillai, & Milshtein, 2011; Marcialis & Roli, 2003; Sadasivuni, Houkan, Taha, & Cabibihan, 2017; Yuan, Sun, & Lv, 2016;). The deformation and smearing problems can be overcome by touchless live scan devices (Zhou, Hu, Petersen, Wang, & Bennamoun, 2014). Despite its problems, fingerprint authentication is seen as a useful method of authentication since fingerprint is one of the most unique biometric samples in a human body. The chance to find two equivalent fingerprints has been estimated as high as one in a billion or even as completely unique for every person (Faundez-Zanuy, 2006; Priya & Rajesh, 2011).

Eye iris as a biometric sample has been praised in earlier research as it is very predictable and a well-protected internal organ (Chabbra & Dutta, 2016). A single human iris contains a great amount of information, the characteristics of an iris do not change during a person's lifetime and there are hundreds of different variables that can be measured from an iris (Kapoor & Rawat, 2017). The interference of eye diseases in enrollment and comparison of iris samples has however been raised as a limitation in previous research (Trokielewicz, Czajka, & Maciejewicz, 2015). Iris recognition can also be spoofed by cosmetic contacted lenses, but this problem is being tackled by means of pattern-recognition and structured light protection (Bowyer & Doyle, 2014; Connell, Ratha, Gentile, & Bolle, 2013). The rate of false matches in eye iris recognition can be as low as one in 200 billion and the chance of two random eye iris samples to be equivalent is around one in 10^{35} (Daugman, 2005; Hallinan, 1991). Iris recognition has been claimed to be even more accurate than DNA in recognition of a person (Kapoor & Rawat, 2017).

In facial recognition, usability issues with screen reflection, alignment of the user, lighting conditions, quality of old images, aging, face occlusion, cosmetics and computing overhead can affect the recognition quality (Guo, Wen, & Yan, 2014; Shubhangi & Balbhim, 2017; Trewin, Swart, Koved, & Martino, 2012). Security of facial recognition systems has also been questioned since the face is constantly publicly displayed and because spoofing and replay attacks have been used to gain access to the systems (Smith et al., 2015). Such attacks are combated by liveness detection mechanisms and challenge/response-based methods, but these methods are challenging because of user motivation issues and the lack of intelligent enough sensors in consumer devices (Khan, Zhang, & Alghathbar, 2011; Li et al., 2015; Smith et al., 2015). Then again, face recognition has advantages over other biometric technologies, because it is non-intrusive, non-invasive, easy to use and can even be used to identify a person from distance without cooperation of the subject (Mandal, 2017). Facial recognition has no capture delay and the user can be entirely unaware of the whole process (Aly & Hassaballah, 2015). In addition, facial recognition systems have low technological costs (Karczmarek, Kiersztyn, Pedrycz, & Dolecki, 2017). Even though the performance of facial recognition always drops significantly in unconstrained environments, it has attracted much attention in the last decade due to its great potential value in real world applications (Zhu, Lei, Yan, Yi & Li, 2015). Face biometric have great potential in mobile devices, which already come equipped with a camera and other technology for utilizing facial recognition data (Feng, Zhou,

Dan, Peiyan, & Li, 2017). Facial recognition has also been suggested as a potential technology for long-distance bank account openings, issuing social insurances, mobile commerce payment management, access control, identity verification and video surveillance (Feng et al., 2017).

In addition to the most popular biometric authentication methods, countless of other biometric authentication schemes have been proposed. Some of them utilize similar techniques as the "top three" presented above, such as the use of palm veins or knuckle prints instead of fingerprint samples, or recognition of audio features from the user's breathing gestures instead of regular voice recognition (Chauhan et al., 2017; Jaswal, Kaul, & Nath, 2016; Raut, 2017). Other proposed methods come far from the traditional biometrics and vary from recording a person´s EEG brain waves to recognizing the body odor of the user (Gibbs, 2010; Thomas & Vinod, 2017).

Biometric authentication schemes have been developed to resemble ordinary actions performed on the secured devices and services, and some methods are even developed to perform authentication on a continuous basis. Methods such as the analysis of users keystroke dynamics on a computer, handwriting signature verification on ATM and hand pressure biometrics on firearms resemble the normal actions performed on the devices (Bergadano, Gunetti, & Picardi, 2002; Islam et al., 2017; Mondal, Deb, & Adnan, 2017). Continuous biometric authentication has been proposed based on e.g. touchscreen inputs or gait patterns on mobile devices (Derawi, Nickely, Bours, & Busch, 2010; Eberz et al., 2017).

2.2 Applications and impacts of biometric authentication technologies

Biometric authentication technologies are utilized in a wide variety of industries and contexts. Biometric authentication is used or planned to be used for example in access control, border control, banking, educational institutions, healthcare, national identity systems and passports (Bowyer & Doyle, 2014; Burge & Bowyer, 2013; Caldwell, 2014; Elliott, O'connor, Bartlow, Robertson & Guest, 2015; Maple ja Norrington, 2006; Meenakshi & Padmavathi, 2009; Prakash & Dhanalakshmi, 2016; Soniya, Sri, Titty, Ramakrishnan, & Sivakumar, 2017). In addition to the long history of use by government and law enforcement agencies, the use of biometrics has risen in consumer goods such as mobile phones and computers in recent years (Memon, 2017). In addition to the suggested security and usability advantages, earlier research notes that biometrics have brought services to new user segments, such as rural and illiterate masses, and even improved environmental pollution problems by reducing the amount of plastic ATM cards used in banking services (Bhosale & Sawant, 2012).

Despite their popularity, biometric technologies come with many problems and challenges. All biometric modalities have limitations, which can be related to e.g. noise in sensed data, insufficient distinctiveness across people, insufficient

universality across a group of users or vulnerability to spoof attacks and fake samples (El-fishawy, 2015). No such biometric authentication method exists, in which every person in the world would possess the biometric sample in question and be able to give a sample of good enough quality (Lassmann, 2002). Hairstyle, the absence or presence of eyeglasses, aging, cosmetic changes injuries are some examples of variations that can affect the level of biometric recognition accuracy (Akinnuwesi, Uzoka, Okwundu, & Fashoto, 2016) Health problems of elderly people have been emphasized as a limitation in earlier literature (Kowtko, 2014). Novel approached are however studied to overcome the limitations for certain user groups. For an example, vein technology has been suggested as an easier, faster and less stressful technology for elderly subjects and improved methods have been proposed to include blind people in iris and retina authentication (Riley, McCracken, & Buckner, 2007; Suliman & Ahmed, 2017).

The security threats can also be overcome. While biometrics open new doors to attackers, less traditional cyber-attacks are committed against biometrically secured targets compared to targets secured by traditional methods (Kowtko, 2014). The problem of biometrics credentials not being replaceable has been tackled by the means of cancelable biometrics. They can be used to create revocable and noninvertible biometric templates, which are cancelable and replaceable in a case of a security breach (Jenisch & Uhl, 2011; Patel et al., 2015; Ratha, Connell, Bolle, & Chikkerur, 2006).

In summary, the most popular biometric authentication technologies are based on fingerprint, eye iris and face recognition, but countless propositions for other types of biometric authentication and combinations of several methods exist in literature. Biometric authentication is being used in various commercial, organizational and governmental applications. At their best, biometric technologies provide highly usable and secure authentication, which utilizes physical or behavioral credentials, that are almost unique for each human being and which cannot be stolen, forgotten or lost. However, biometric authentication creates new security and privacy threats, any biometric feature always rules some user groups out and many external factors can affect the effectiveness and usability of biometrics. Biometrics are also not always accepted by users. In the next chapter, theories and models for explaining technology acceptance and biometrics acceptance are presented to help in explaining, how biometrics acceptance is formed.

3 TECHNOLOGY ACCEPTANCE

One objective of the literature review was to find out, how the acceptance of biometric technologies has been studied in earlier literature. Many models and frameworks have been presented and used to gain insights and perspectives on users' attitudes and acceptance towards technologies. TAM, which is the most frequently used method in Information Systems literature, is the model utilized also in the empirical part of this master's thesis. In this chapter, TAM, its many use contexts and extensions are presented. Then the user-centered biometrics research is examined in order to explain, how the acceptance of biometrics specifically can be measured in academic studies and to address the first objective of the literature review.

3.1 Technology Acceptance Model (TAM)

Davis (1986) defines perceived usefulness as the extent to which a person believes that using a particular technology will enhance his or her job performance and perceived ease of use as the degree to which a person believes that using a technology will be free from effort. In addition to perceived usefulness and perceived ease of use, a variable of behavioral intention to use was later added to the model (Davis, Bagozzi, & Warshaw, 1989). Davis et al. (1989) proposed that attitude toward using a technology affects the behavioral intention to use a technology, which determines the actual system use. They also suggested that the perceived usefulness can affect behavioral intention directly, without any attitude being formed. When testing the model, perceived ease of use was also found to influence the behavioral intention to use. In addition to the inclusion of behavioral intention, this version of TAM proposed external variables, such as system performance or accuracy, to affect the perceived usefulness and perceived ease of use of the technology.

Venkatesh & Davis (1996) updated TAM to its final version. In this version, the construct of attitude was eliminated, perceived usefulness and perceived ease

of use both directly affecting behavioral intention. They proposed the external variables, which affect the perceived usefulness and perceived ease of use, to consist of system characteristics, training, user involvement in design and the nature of the implementation process. Their final version of the first Technology Acceptance Model is presented in figure 1.

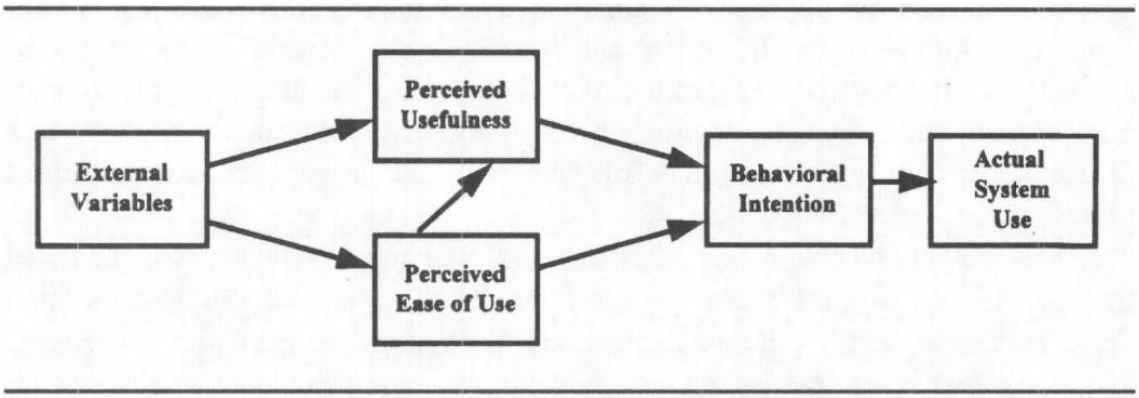

FIGURE 1 Technology Acceptance Model (Venkatesh & Davis, 1996)

Even though TAM reached its "final form" already in 1996, it has been constantly developed, extended and verified on various fields of technology, within different user groups and including many external constructs. Later Venkatesh & Davis (2000) extended TAM to include an explanation of perceived usefulness and usage intentions in terms of social influence and cognitive instrumental processes. Venkatesh (2000) has also extended the TAM to include determinants of system-specific perceived ease of use, based on adjustments and internal and external control, intrinsic motivation and emotion as anchors.

TAM has been utilized to study the part of social influence, gender differences and age differences in technology acceptance (Chung, Park, Wang, Fulk, & Mclaughlin, 2010; Malhotra & Galletta, 1999; Venkatesh & Morris, 2000). It has been applied to research technology acceptance in numerous contexts, such as e-commerce, organizational software implementation and social network adoption (Amoako-Gyampah & Salam, 2004; Carlos Martins Rodrigues Pinho & Soares, 2011; Gefen, Karahanna & Straub, 2003; Pavlou, 2003). Earlier research has also combined TAM with other models such as The Theory of Planned Behavior and the Diffusion of Innovation theory (Chen, Gillenson, & Sherrell, 2002; Fusilier & Durlabhji, 2005). UTAUT and TRAM are unified models based on TAM and additional models (Lin, Hsin-Yu, & Sher, 2007; Venkatesh, Morris, Davis & Davis, 2003).

Despite the popularity of TAM, it has also been criticized. Legris, Ingham, & Collerette (2003) argue that while TAM is a useful model, it seldom explains more than 40% of the variance in use and must be integrated into a broader model. They point out that TAM-studies often involve only students as study subjects. They belive the research would be better conducted in a business environment and that research would benefit from examining the introduction of business process applications instead of office automation software or systems development applications. In addition, they also see the self-reported use

problematic, as a non-precise measure which is used in many TAM studies, but cannot be analyzed rigorously.

3.2 Methods for measuring the acceptance of biometrics

A user's perception of a new technology, especially considering biometric devices and security applications, is influenced by psychological, social and contextual factors, that are related to the use of the technology in everyday applications (Biosec, 2005). The research on the user acceptance of biometrics in general is rather new (Kanak & Sogukpinar, 2017). Riley et al. (2009) mention, that according to prior literature, Technology Acceptance Models do not suit exploratory research, cross-cultural research or security and identification technology research very well. However, other studies show, that many successful replications of TAM and its extensions have been used both to measure biometrics acceptance, and to measure technology acceptance cross-culturally. The extended TAM by James, Pirim, Boswell, Reithel & Barkhi (2006) is the model utilized in the present study.

TAM has been used and extended into a biometrics-specific model for an example to measure the attitudes towards biometrics as a CAPTCHA replacement, to compare gender differences in the acceptance of a biometrics and to study biometric authentication acceptance in an e-banking context and in the use of hotel guests (Al-Harby et al., 2009; Gibbs, 2010; Krol et al., 2016; Morosan, 2012 Normalini & Ramayah, 2017; Tassabehji & Kamala, 2009). Breward, Hassanein, & Head (2017) have developed a framework for measuring consumer acceptance of controversial information technologies, using consumers' attitudes towards biometrics in ATM authentication as an example in model validation.

TAM, DOI, UTAUT and findings from the trust and privacy literature have been integrated to evaluate the acceptance of biometrics (Miltgen, Popovič, & Oliveira, 2013). According to Miltgen et al. (2013), the traditional models of user acceptance are not the best to explain the acceptance of biometrics, but that the drivers of biometric acceptance can be found from the trust and privacy literature instead. Kanak & Sogukpinar (2017) also stress the importance of including trust literature in a biometric acceptance model. However, they criticize the study of Miltgen et al. (2013) for not taking into account the users' security perceptions of biometrics. Their BioTAM presents an addition of a trust factor in Technology Acceptance Model (TAM) as a function of privacy-security tradeoff, public willingness and user confidence. The model addresses perceptions, attitudes and behavioral intentions by adding trust as a new construct to the Technology Acceptance Model.

James et al. (2006) have also created an extended application of the TAM framework to successfully predict the intention to use biometric devices. According to them, the barriers for the use of biometrics found in literature can be grouped into physical invasiveness, information invasiveness, ease of use, privacy, and the perceived level of benefit from the device. Their extended TAM

adds the constructs of perceived need for privacy, perceived need for security and perceived physical invasiveness to the model. They found perceived need for security to positively affect the perceived usefulness and negatively the perceived physical invasiveness of a device. Perceived physical invasiveness of the device affected negatively the perceived ease of use and the intention to use the technology. Perceived need for privacy affected perceived invasiveness positively. Contrary their hypothesis, perceived need for privacy did not affect perceived usefulness directly, but only indirectly through perceived need for security, on which it had a significant effect. Their model has been utilized in further research to study fingerprint biometrics on touchscreen devices, EEG biometrics and to compare user perceptions towards various authentication technologies (Jones, Antón, & Earp, 2007; Ponce, 2015; Rodriguez, 2015).

To sum it up, many models have been proposed and used to measure technology acceptance, but the Technology Acceptance Model has been the most represented in Information Systems literature. Despite its popularity, TAM has been criticized for low explanation power, leaning on users' own reports in measuring use and for the sample choices and application areas often associated to TAM studies. TAM has also been modified in many studies to suit the research of biometric technologies. Other models, such as Diffusion of Innovations -theory and UTAUT have been incorporated into TAM to measure the biometrics acceptance. Other authors have suggested, that instead of general technology acceptance models, the biggest drivers for acceptance of biometrics can be found from trust and privacy literature. None of these models however take cultural differences into consideration in measuring biometrics acceptance. In order to assess technology acceptance in different cultural contexts, culture needs to be defined. This definition is done in the next chapter, in order to understand better, what cultural differences are and how they can be compared across geographical areas.

4 CULTURE

Culture has many definitions. In presenting these definitions, most attention is paid to Hofstede's (1984) definition of culture and his theory of cultural dimensions, which is the framework used to compare cultures in this master's thesis. The cultural areas inspected in this study are Brazil from South America and Finland from Nordic Europe. The national and geographical characteristics and cultural backgrounds of Brazil and Finland need to be presented in order to proceed into a cross-cultural examination of the countries.

4.1 Definition of culture

Kluckhohn's (1951, p. 86, 5) anthropological definition of culture is "the patterned ways of thinking, feeling and reacting, acquired and transmitted mainly by symbols, constituting the distinctive achievements of human groups, including their embodiments in artifacts." Kluckhohn (1951) sees the essential core of culture to consist of traditional ideas and especially the values attached to them. Straub et al. (2002) present some early definitions of culture, such as Tylor's (1871, p.1) Primitive Culture which defines culture as "that complex whole which includes knowledge, beliefs, art, moral laws, customs and any other capabilities and habits acquired by man as a member of society", Kroeber's (1952) "the historically differentiated and variable mass of customary ways of functioning of human societies", Parson's and Shil's (1951) "set of values, norms and symbols that guide human behavior and Herskovit's definition (1955), which says that culture is "learned, allows man to adapt himself to his natural and social setting, is greatly variable and is manifested in institutions, thought patterns, and material objects". Straub et al. (2002) categorize the newer definitions of culture into three groups: definitions based on shared values, definitions based on problem solving and general all-encompassing definitions. Hofstede's theory of culture falls in the category of shared values.

The original cultural dimensions of Hofstede (1984) are Individualism/Collectivism, Power Distance, Uncertainty Avoidance and Masculinity/Femininity. Later, new dimensions of Long-Term Orientation/Short-Term Orientation and Indulgence/Restraint were added (Hofstede, 2011). The dimensions, their definitions and the abbreviations used in this study are summarized in table 1.

TABLE 1 Hofstede's dimensions, abbreviations and definitions (Hofstede, 2011)

Dimension	Definition
Power Distance (PDI)	The extent to which the less powerful members of organizations and institutions accept and expect that power is distributed unequally. Tends to be higher in East European, Latin, Asian and African countries and lower in Germanic and English-speaking Western countries.
Uncertainty Avoidance (UAI)	To what extent a culture programs its members to feel either uncomfortable or comfortable in unstructured situations. Usually higher in East and Central European countries, in Latin countries, in Japan and in German speaking countries. Lower in English speaking, Nordic and Chinese culture countries.
Individualism versus Collectivism (IDV)	The degree to which people in a society are integrated into groups. Tends to be high in developed and western countries, while less developed and Eastern countries are more collectivistic. Japan is found on the middle ground.
Masculinity versus Femininity (MAS)	The distribution of assertive versus modest and caring values between genders. High in Japan, German speaking countries and some Latin countries, moderately high in English speaking western countries, low in Nordic countries and the Netherlands and moderately low in some Latin and Asian countries.
Long Term versus Short Term Orientation (LTO)	The valorization of perseverance, thrift, ordering relationships by status, and having a sense of shame, versus valorization of reciprocating social obligations, respect for tradition, protecting one's 'face', and personal steadiness and stability. East Asian countries are the most long-term oriented, followed by Eastern- and Central Europe. South- and North-European and South Asian countries are the medium-term orientated countries and USA, Australia, Latin America, Africa and Muslim countries the short-term oriented countries.
Indulgence versus Restraint (IVR)	Allowing relatively free gratification of basic and natural human desires related to enjoying life and having fun versus controlling gratification of needs. South and North American countries, Western Europe and parts of Sub-Saharan Africa are countries of high indulgence, and Eastern Europe, Asia and the Muslim world countries of high restraint, Mediterranean Europe taking a middle position.

The original country scores of Hofstede (1984) are almost 40 years old and thus might be outdated today. Hofstede's dimensions have also been criticized for oversimplifying culture, equating culture to nation and not taking into account the flexible and changing nature of culture (Signorini, Wiesemes, & Murphy, 2009). Straub et al. (2002) argue the shortcoming of Hofstede's approach to be that there are recognized subcultures that span national geographic boundaries and nations that have strong internal cultural differences. As an example of the first shortcoming, Latin American culture is mentioned. Spector, Cooper, & Sparks (2001) also question the psychometric properties of the Values Survey Module (VSM) questionnaire, as their analysis could not establish a validity and reliability of the scales used in samples from 23 different countries and provinces.

Masculinity vs. Femininity is perhaps the most critiqued of all Hofstede's dimensions. Wu (2001) raises a point that the dimension is defined by stereotypical gender expectations in work context, such as advancement, earnings, training, and up-to-date qualities for men and friendly atmosphere, position security, physical conditions, and cooperation for women. The "masculine" and "feminine" items are criticized for having been consistent with attitudes of the 1960's and early 1970's but being less representative of newer understanding of gender issues and sex role identities (Erdener, 1998).

4.2 Brazil and South America

Brazil is a federation of 26 states and a Federal District around Brasilia, its capital. The country is divided into five administrative regions: The South, Southeast, Central West, Northeast and North. It is the fifth largest country in the world in terms of size and population. According to the National Household Sample Survey (PNAD) of 2015, the population of Brazil was 204 860 000 people, of which 51.5% women and 48.5% men (Instituto Brasileiro de Geografia e Estatística [IBGE], 2016). Brazil is a culturally diverse area, first inhabited by the native people, colonized by the Portuguese, receiving a large number of slaves from Africa and later immigrants from Europe and Asia (Hofstede, Garibaldi de Hilal, Malvezzi, Tanure, & Vinken, 2010).

In the beginning of the millennium, Brazil was considered a newly industrialized country and thus its IT diffusion was faster than in many other developing countries (Kim, 2002). For an example, the early diffusion of e-commerce in Brazil was relatively rapid compared to other developing countries (Tigre, 2003). In 2006, Brazil had 14 million internet users, having the largest online user population in Latin America (Singh, Fassott, Chao & Hoffmann, 2006). In 2015, 57.5% of the Brazilian population older than 10 years of age (102,1 million total users) 58% of women and 56.8% of men, had access to the internet (IBGE, 2015).

Some of Hofstede's dimensions can be seen as consistent in all Latin or Latin American countries. These include Power Distance and Uncertainty Avoidance, which are generally higher for all Latin countries, and Indulgence, which is said to be high in South America. Individualism is a dimension generally lower in all

developing and Eastern countries. However, the Latin countries differ from each other in the dimensions of masculinity. Earlier, Brazil has scored fairly high in Long Term Orientation (Hofstede et al., 2010, pp. 240), Hofstede & Hofstede (2005, p. 240) reporting a score of 65 for Brazil based on the Chinese Value Survey, a score above average. In a later study, the LTO score of Brazil has fallen to 44, taking it to the level of other Latin American countries (Hofstede & Minkov, 2010). All South American countries mentioned by Hofstede (2010) and their cultural dimension scores are presented in table 2. Not all South and Latin American countries had a score for each of the dimensions. The South American countries Bolivia, Guyana and Paraguay do not have any scores published by Hofstede (2010).

TABLE 2 South and Latin American countries and their scores on Hofstede's (2010) dimensions

Country	**PDI**	**IDV**	**MAS**	**UAI**	**LTO**	**IVR**
Argentina	49	46	56	86	32	40
Brazil	69	38	49	76	69	78
Chile	63	23	28	86	61	15
Colombia	67	13	64	80	26	32
Costa Rica	35	15	21	86	-	-
Ecuador	78	8	63	67	-	65
El Salvador	66	19	40	94	20	89
Guatemala	95	6	37	101	-	-
Mexico	81	30	69	82	23	34
Peru	64	16	42	87	20	62
Suriname	85	47	37	92	61	-
Uruguay	61	36	38	100	21	71
Venezuela	81	12	73	76	60	63

Hofstede et al. (2010) have explored the cultural diversity within Brazil in a business context based on three separate research projects utilizing Hofstede's VSM questionnaire in Brazil's different states. Based on the found cultural clusters of states, they found the Brazil's five administrative districts, counting the Federal District as Southeast, to work as a best-fitting framework for reporting regional differences in Brazil. The study found these regions to produce significantly distinct cultural profiles. However, evidence of a common Brazilian national culture was found as all the states were much more similar to each other than to other Latin American countries or countries worldwide. Their study suggested the following characteristics for the five regions: The South was found more hierarchical, less formal, more individualistic, and more masculine. The Southeast and Brasilia were less masculine and also shorter term oriented. The Central-West was found less formal. The Northeast was perceived to be less hierarchical, more formal, and less masculine. Finally, the North was found very informal, collectivist, and very masculine. Another study has found differences in motivational domains and business performance between regional subcultures in Brazil (Lenartowicz & Roth, 2001). However, Hofstede et al. (2010) criticizes these results

because the used questionnaire was created to evaluate mindsets of college students in the United states in the 1960's, but the samples were only collected from kiosk owners in Brazil.

Some papers speak of Brazil as a member of Latin America (e.g. Gupta, Hanges, & Dorfman, 2002). However, it is debatable if Brazil in fact belongs to the cultural cluster of Latin America. For more than a century after independence, Spanish American intellectuals and governments did not consider Brazil as a part of Latin America, and majority of Brazilian intellectuals and governments did not think of Brazil as an integral part of the region for even a longer period of time (Bethell, 2010). Hofstede (1976) has included Brazil in the cluster of Latin Europe and later in the Latin American cluster (Hofstede et al., 2010, pp. 259), but Brazil has also been seen as a completely independent cluster (Sirota & Greenwood, 1971). Lenartowicz, Johnson, & White (2003) also speak of Brazil as a part of Latin America but affirm that there can be significant differences in the relative importance of values among different subgroups within Latin American nations. They mention that subgroups in different Latin American countries can be culturally more coherent than subgroups within one country. Their results indicate that geography, a shared history and a common ethnic background might be as important in defining cultural subgroups as religion and language.

The present study is interested in Brazil and its national culture, Brazil as a member of the geographical area of South America, and the cultural cluster of Latin America, where majority of reviewed literature included it. However, it is important to note that South America and Latin America do not necessarily include the same countries and that South America might not be a culturally coherent area for all its cultural features, and that some of these features might vary a lot between countries in the area.

In conclusion, Brazil is a culturally rich nation, with its areas varying in cultural features. However, from the lens of Hofstede's dimensions, Brazil also seems to hold a unified national culture, distinct from other countries in the continent. This study does not aim to generalize its results to whole Brazil or Latin/South America, but to test its hypotheses within a limited sample of a Brazilian population, taking the first step into clarifying the characteristics of biometrics acceptance in the area.

4.3 Finland and Nordic Europe

After hundreds of years of being a part of Sweden, and 110 years being a part of Russia, Finland gained independence and became an established state in 1917 (Paasi, 1997). During the Swedish period and the first few decades of being an autonomous part of Russia, no clear national identities or widespread separatist tendencies existed in Finland (Paasi, 1997). In the beginning of Finland's political and social development, it remained as a part of Eastern Europe (Klinge, 1980). National feelings in Finland emerged later and slowly, mainly between the years 1860 and 1880 (Paasi, 1997). After the independence, the construction of Finnish

national integrity was concentrated on the "enemy image" towards Russia and in the post-war era, Finland was creating an image of being a neutral capitalist state between the east and the west, but involving an ideological link with the Western world (Paasi, 1997).

In the report by Tilastokeskus (2018) the population of Finland in 2017 was 5 513 130 with 49% men and 51% women. Seventy two percent of the households had access to a mobile broadband connection and 68% to a Wireless LAN -connection. Finland has been a pioneering force in the fields of technology and was for an example one of the first internet banking adopters along with the other Nordic countries (Mäenpää, Kale, Kuusela, & Mesiranta, 2008). Finland is one of the forerunners on new mobile services and has been considered for a long time as one of the most advanced and sophisticated test-markets for the industry (Bouwman, Carlsson, Walden, & Molina-Castillo, 2008). The Finnish mobile phone manufacturer Nokia is one of the reasons why the mobile industry has always been an important sector in Finland (Guhr, Loi, Wiegard, & Breitner, 2013).

Nishimura, Nevgi, & Tella (2008) describe Finnish culture as relatively homogenous and as a listening culture, where people are allowed to talk freely without being interrupted. They say that Finns tend to be punctual, non-hierarchical and individualistic. A characteristic feature of the Finnish sociocultural values is that inequalities between people should be minimized, and like other cultures on the low-end of the Power Distance -scale, Finland is characterized by equality and freedom of expression (Gyekye & Salminen, 2005).

In 1997, only 2% of Finland's population were born outside of Finland and traditionally Finland has indeed been a very closed state with respect to foreign refugees and immigrants and with the official policy. In 2018, the portion of people born outside of Finland had however grown to 7% of total population (Tilastokeskus, 2019). Hofstede, Hofstede, & Minkov (2010) also point out, that while scoring high on individualism, Finland is less exclusionist and more open to opt-out members than expected. Historically the Swedish-speaking minority elite has had a powerful role in Finnish politics and culture, and even today Finland is a bilingual state, with a Finnish-speaking majority and Swedish-speaking minority (Paasi, 1997). In 2017, the Swedish-speaking population of Finland was 289 052 people (Tilastokeskus, 2018). Besides the Finnish Swedish, another national minority existing in Finland are the Sámi people living in the Northern Finland (Paasi, 1997). In 2016, the population speaking the Sami-language was 1 992 people (Tilastokeskus, 2018).

The Swedish language has been a key element in the inclusion of Finland among the cultural and political co-operation of the Nordic countries (Paasi, 1995). All the reviewed literature grouped Finland to the cultural cluster of the Nordic or Nordic European countries (Gupta et al., 2002; Hofstede et al., 2010, pp.60; Ronen & Shenkar, 1985). In this master's thesis, the Nordic countries are therefore considered the cultural cluster of Finland.

As seen from the table 3, the Nordic countries share somewhat similar scores on Hofstede's cultural dimensions. Finland differs from them in the

uncertainty avoidance -scores, where Denmark and Sweden clearly position in the lower end, Norway in the middle and Finland a little above the middle. Also, while Finland is one of the six most feminine countries, it scores a bit higher than the other Nordic countries in the Masculinity-dimension (Hofstede et al., 2010, pp. 140). In Long Term Orientation, Finland together with Denmark and Norway differ from Sweden, which positions a little over the middle. Finland has been researched with the lens of Hofstede´s dimensions for an example in the contexts of construction sector, international reward management, productivity of R&D units and forestry education (Arevalo, Mola-Yudego, Pelkonen, & Qu, 2012; Chiang, 2005; Jullan, 1992; Kedia, Keller, & Nummelin, 2007).

TABLE 3 Nordic countries and their scores on Hofstede's (2010) dimensions

Country	**PDI**	**IDV**	**MAS**	**UAI**	**LTO**	**IVR**
Denmark	18	74	16	23	35	70
Finland	33	63	26	59	38	57
Norway	31	69	8	50	35	55
Sweden	31	71	5	29	53	78

All in all, Finland has a history of being a part of different countries and cultures before its independence. Finland's national identity has been constructed based on different cornerstones in its history. It is a bilingual country of Finnish and Swedish speakers, and also includes the Sámi minority living in the northern parts of the country. Finland has developed a homogenous culture, which is also similar with the Nordic European culture cluster, into which Finland has been unanimously categorized in earlier literature.

Culture, to sum it up, can be a related to social groups or it can refer to the national culture of a country. Many definitions of culture exist, but the most popular theory for explaining national culture in the Information Systems literary is the cultural dimension theory of Hofstede (1984). He sees culture as a collective programming of minds, distinguishing members between different groups. Brazil and Finland differ from each other in some of Hofstede's dimensions. For an example, Hofstede´s (1984) scores suggests that Brazil has a higher Power Distance than Finland and that Finland is a more feminine and individualistic country than Brazil. Next, culture and technology acceptance are united. The following chapter concentrates on theories and frameworks aimed at studying technology acceptance in different cultural contexts and in a cross-cultural manner.

5 CULTURAL TECHNOLOGY ACCEPTANCE

The aim of this chapter is to bring together technology acceptance and culture, and to compare the features of biometrics acceptance between cultures. To do this, the earlier technology acceptance research across countries, especially considering biometrics, needs to be examined. The studies of biometrics acceptance around the world are first presented by continent in order to categorize the results of biometrics acceptance literature, and to finally compare the familiarity, acceptance and barriers of biometrics use between regions.

5.1 Cultural study of technology acceptance

National culture is a macro-level phenomenon, but technology acceptance is an individual concern (Srite & Karahanna, 2006). Nationality, religion, history, political views and socio-economic conditions are all examples of potential cultures which may come in different combinations in every individual (Viberg & Grönlund, 2013). Culture is a critical variable in explaining how social groups interact with IT (Leidner & Kayworth, 2006). In addition to initial technology adoption choices, the post-adoption beliefs, and thus indirectly behaviors, have been found to be significantly affected by cultural lenses (Lee, Choi, Kim, & Hong, 2007). Comparing the acceptance of technology between cultures is therefore a more complicated matter than only comparing levels of acceptance between two regions. Not all differences between countries have been explainable for an example by Hofstede's dimensions, and there are problems related to equating culture with a country or a continent. TAM was the most widely used framework for measuring and predicting the adoption and use of technology outside western contexts in the examined literature. Another model that was validated in diverse cultures and used in many cross-cultural studies was UTAUT (Al-Gahtani, Hubona, & Wang, 2007; Im, Hong, & Kang, 2011; Nistor, Göğüş, & Lerche, 2013; Oshlyansky, Cairns, & Thimbleby, 2007; Yoo & Huang, 2011).

5.1.1 Technology acceptance and Hofstede's dimensions

Riley et al. (2009) explain, that in previous research considering technology acceptance and Hofstede's dimensions, cultures of high Power Distance have been found to have centralized decision making structures, which affect the acceptance negatively They add, that individualism has been found to positively affect technology acceptance, possibly because in collectivist societies, it is more rare to go against prevailing norms and attitudes, while members in individualistic societies are more willing to adopt technologies which others are not using. According to them, cultural technology acceptance studies have found uncertainty avoidance to negatively influence technology adoption, because new technologies create an unknown territory, with which people from these cultures tend not to want to get involved. They also note some earlier attempts that tried to associate masculinity with positive attitudes towards technology, but that there are contradictory evidences considering this claim.

In cross-national studies, the Hofstede´s dimensions have been shown to affect technology acceptance between nations at least to some extent (e.g. Srite, 2006). Simon (2001) has adapted Hofstede's dimensions to explore the perception and satisfaction levels of websites and claims that differences exist between cultural clusters. Asian and Latin/South American perceptions were found to be similar, and the perceptions of Europeans and North Americans to be similar. In the masculine and collectivist cultures, such as Asia and South/Latin America, there were less differences between genders in technology acceptance, possibly because of more uniformity in the thought process across genders. The European and North American cultures have more contrast between genders in perceptions and levels of satisfaction. Straub, Keil, & Brenner (1997) studied the acceptance of email between Japan, Switzerland and the US together with Hofstede's dimensions and suggested that in high PDI societies, the leveling effect of computer-based media might not be seen or felt as a desirable feature, and that especially UAI could influence choices between computer-based and traditional media. However, not all studies have found Hofstede's cultural dimensions to explain cross-cultural technology acceptance differences. Viberg & Grönlund (2013) have compared the use of mobile devices in second and foreign language learning in Sweden and China, claiming Hofstede's cultural dimensions not being able to explain the differences in mobile-assisted language learning attitudes between the countries, suggesting gender to be a stronger predictor of attitudes than cultural dimensions.

Srite & Karahanna (2006) perceived from previous research that behavioral models do not universally hold across cultures. They argue, that while country-level analysis of Hofstede's dimensions should not be used to explain individual behavior, the individual level of analysis can be treated as an individual difference variable of an espoused cultural value, and because the effect of culture is dependent to the extent to which the individual subscribes to cultural values, assessing each individual's espoused cultural values is appropriate and meaningful for predicting individual level behavior. They posit that national culture

impacts the cultural values that an individual holds, affecting the level of technology acceptance. Their extended technology acceptance model includes espoused national cultural value moderators of Masculinity vs. Femininity, Individualism vs. Collectivism, Power Distance and Uncertainty Avoidance. Social norms were found to be stronger determinants of intended behavior for those individuals who espouse cultural values of femininity, low power distance and high uncertainty avoidance. Contrary to what was hypothesized, values of masculinity/femininity did not moderate the relationship between perceived usefulness and behavioral intention but did the relationship between perceived ease of use and behavioral intention. The present study will also utilize Hofstede´s cultural dimensions as variables of espoused values in order to compare biometrics perceptions between Finland and Brazil.

5.1.2 TAM

In addition to being validated in many fields of technology, TAM has also been extended and successfully used in many different cultural and national contexts, for example in Europe, North America, Asia, Middle East and Africa (Asmah, Ofoeda, & Gyapong, 2016; Chitungo & Munongo, 2013; Faqih, 2013; Fusilier & Durlabhji, 2005; Kripanont, 2007; Lee, Yoon, & Lee, 2009; Lin, Fofanah, & Liang, 2011; Teo, Lee, Chai, & Wong, 2009; Tong, 2010). TAM has also been extended to specifically suit the developing country context (Sharif Abbasi, Hussain Chandio, Fatah Soomro & Shah, 2011). Cross-cultural studies have been performed utilizing TAM and though being successful, the models have revealed some differences in how technology is accepted between cultures and nations (e.g. Evers & Day, 1997; Rose & Straub, 1998; Tarhini, Hone, & Liu, 2015).

However, not all agree with TAM's universality between cultural contexts. In Straub et al.´s (1997) email-study, the results indicated TAM holding for U.S and Switzerland, but not for Japan, suggesting that TAM might not predict technology use across all cultures. Some TAM-studies claim the model not to fit well cultures outside North America or the Western world (Anandarajan, Igbaria, & Anakwe, 2002; Schepers & Wetzels, 2007).

5.2 Technology acceptance in Brazil and South America

Unlike biometrics, the acceptance of other technologies has already been studied in South America and Brazil, utilizing diverse models. UTAUT has been validated in the context of e-learning acceptance in Peru (Maldonado, Khan, Moon, & Rho, 2011). Many Latin American countries have been included in cross-cultural TAM-studies before (McCoy, Everard, & Jones, 2005; Park, Roman, Lee & Chung, 2009).

Cruz, Barretto Filgueiras Neto, Muñoz-Gallego, & Laukkanen (2010) have studied the adoption of mobile banking in Brazil by utilizing TAM, TRA, DOI

and theory of resistance to innovation. They found the majority of respondents not to use any kind of mobile banking services, and the major barriers of use being the perception of cost, risk, low perceived relative advantage and complexity. TAM has also been extended to study e-learning adoption in Brazil (Okazaki & dos Santos, (2012). TAM was replicable in the Brazilian context, but unlike in the original model, perceived usefulness was not found to be a direct driver of intention to use e-learning applications. Singh, Fassott, Chao & Hoffmann (2006) have used an extended TAM to study international websites customized for consumers from Germany, Brazil and Taiwan. They found the cultural adaptation on a website to be a less important determinant for ease of use and attitude toward an international website for Brazilian than for Taiwanese consumers.

Brazilians consumers' cognitive and affective evaluations and the acceptance of new technologies have been found in earlier research to be significantly influenced by their technology readiness, the natural willingness to adopt new technologies, possibly because of the Brazilian or Latin American culture, being a more emotive one (Ferreira, da Rocha, & da Silva, 2014). Avgerou, Ganzaroli, Poulymenakou, & Reinhard (2009) have studied the citizen's perceived trustworthiness towards electronic voting in Brazil. They found Brazilians to perceive the system positively, total trustworthiness being affected by the citizens' perception of trustworthiness of the electronic voting system, trustworthiness and reputation of the election authorities and citizens' general positive attitudes towards ICT.

TAM has been repeatedly validated in Brazil, in various fields of technology. While some relationships of the model have differed from the original, it could be said that replicating a TAM-study in Brazil might likely work. However, the functioning of a biometrics-specific TAM-study in Brazil cannot be taken for granted. Technology acceptance in Brazil has not been explained by Hofstede´s cultural dimensions in earlier research, but other details, such as being an emotive culture, and nationally high levels of trust towards technology have been suggested as factors affecting the Brazilian technology perceptions.

5.3 Technology acceptance in Finland

In Finland, biometrics are used for an example in biometric passports, that according to the Finnish Ministry of Internal Affairs, protect the Finnish citizens from international terrorism, illegal immigrants and international criminals (Heimo, Hakkala, & Kimppa, 2012). Heimo et al. (2012) have however brought up the problems with such systems, and mention them to possibly generate inequality, insecurity and erosion of privacy amongst the society. The acceptance of biometrics in Finland has been studied only in one research paper (Biosec, 2005). Europe, however, is overrepresented in the biometrics acceptance studies and some studies were also found regarding other Nordic countries. For non-biometric technologies, the field of technology acceptance study in Finland is ample. In addition to many TAM-replications, UTAUT is another notable model which

has been validated in Finland (Brown, Dennis, & Venkatesh, 2010; Louho & Kallioja, 2006).

Online banking has been a focus of attitude research in many Finnish studies, of which most use TAM, and a typical online banking user in Finland has been stated to be a relatively young, well-educated family man with a good job and high income-level (Karjaluoto, Mattila, & Pento, 2002; Mäenpää et al., 2008; Pikkarainen, Pikkarainen, Karjaluoto, & Pahnila, 2004). One of the early TAM-validations in Finland found self-efficacy and technology readiness to affect computer usage in Finland (Igbaria & Iivari, 1995). Other TAM-studies have examined Finnish technology acceptance in contexts such as mobile payments and application based mobile services (Ervasti & Helaakoski, 2010; Guhr et al., 2013).

Finland has been subject to cross-cultural technology acceptance studies, where cultural differences have been found between internet banking consumption of Finland and Portugal and mobile service use between Finland, Netherlands and Greece (Bouwman et al., 2008; Kivijärvi, Laukkanen, & Cruz, 2008). The studies inspected countries differing on Hofstede´s dimensions, but no relationships between the dimensions and technology acceptance differences were shown. Sánchez-Franco, Martínez-López, & Martín-Velicia (2009) have studied the acceptance of e-learning applications in the Nordic culture (Finland, Norway, Sweden and Denmark) and the Mediterranean culture (Portugal, Spain and Greece), by utilizing TAM and comparing the countries on Hofstede's cultural dimensions. In their study, cultural differences did have a significant impact on attitude and behaviors towards the applications, the Nordic culture being driven more by instrumental factors and intrinsic enjoyment-based factors, whereas the Mediterranean countries seemed to regard the web as a means to a social end.

The multiple validations of TAM in Finland suggest that applying TAM in the present study would be without problems, but again, the functioning of the biometrics-specific TAM in Finland is yet to be tested. Finland has been shown to differ from other countries in the ways how technology is perceived, and some specific demographic and other features have been noted as affecting technology acceptance. Hofstede´s dimensions have also been used to successfully explain technology acceptance differences between the Nordic countries and Mediterranean countries.

5.4 Cultural study of attitudes towards biometrics

Among other factors, cultural background has been identified to have significant influence on attitudes towards biometric devices and their perceived ease of use (Biosec, 2005). The results of earlier studies considering attitudes and acceptance towards biometrics in different cultural contexts are now presented. Studies from the field of biometrics acceptance have been conducted in Europe, North America, Africa and Asia.

5.4.1 Europe

In an early study of biometrics acceptance, using a mainly European sample, all biometric systems were found to be perceived as less acceptable than traditional password systems and behavioral systems were perceived as less acceptable than physiologic systems (Deane, Barrelle, Henderson & Mahar, 1995). The acceptation of keystroke verification increased when the perceived sensitivity of information increased, and fingerprint verification was perceived as more acceptable when organizational information was perceived as more sensitive. In a newer study, two in three Europeans were ready to use biometric authentication in a payment situation (Visa, 2006). Two thirds of the respondents found it secure to use a two-factor authentication, where biometrics were involved. Half of the respondents found biometrics to speed up and facilitate payments. Fingerprint authentication was the preferred mean of biometric authentication of the respondents. A high level of approval among European citizens has been supported in another study, even though the Spanish respondents accepted biometrics slightly less (Biosec, 2005). Minor concerns regarding the physical harmfulness of biometric sensors emerged, German and Spanish subjects being more concerned than the Finnish respondents. The trust in biometric technologies was found to be limited and the knowledge of biometric technologies very low. The acceptance was also found to be moderated heavily based on fear, instead of knowledge.

In the UK, biometric methods have been seen as possible alternatives for traditional methods such as passwords or PIN-codes in mobile phones (Clarke & Furnell, 2005; Furnell, Dowland, Illingworth, & Reynolds, 2000; Furnell & Evangelatos, 2007). While UK-based respondents think that they would perceive face biometrics as more trustworthy if they saw enough people using them, they have been concerned about the protection and discarding of their face image after verification, and see face biometrics as more suitable for high-security applications (Krol et al., 2016). Biometrics in the UK have been studied in the context of e-banking, where especially the user's perceptions of biometric security influence positively the attitude and intention to use the technology (Tassabehji & Kamala, 2009).

Riley et al. (2009) have studied regional differences in the perception of biometric authentication technologies. They collected and compared data from India, South Africa and the UK. Only 24% of the British respondents had used biometrics before. The British respondents were the least likely to have positive opinions about biometrics. British respondents favored password-based authentication over biometric technologies and token-based authentication. The British subjects were the least willing to use biometrics. A weak positive relationship was found between the willingness to use biometrics and the knowledge of biometrics the subjects rated for themselves. The major concerns towards biometrics were the security of biometric information and fears of health and safety implications of using biometrics. The biometric information security was a bigger concern in the UK compared to the other countries.

In Sweden, iris scan and fingerprint technologies have been rated the most accepted and most security expectations fulfilling biometric methods for mobile units (Giarimi & Magnusson, 2002). While German people prefer passwords as an authentication method and up to 25% might not accept biometrics at all, fingerprint and iris recognition are the most accepted biometric methods in Germany (Krupp et al, 2013; Zimmerman & Gerber, 2017). Krupp et al. (2013) claim that their German subjects did not generally find biometrics too personal, intimate or frightening, but Zimmerman & Gerber (2017) have found some privacy concerns regarding the use of personal information in authentication.

5.4.2 North America

The acceptance of biometrics in the USA has varied in earlier research from higher than passwords to not strongly supported, but the acceptance seems to depend on the context of use between domains such as financial and healthcare or between personal and corporate use (Clodfelter, 2010; Heckle et al, 2007; Jones, Antón, & Earp, 2007). The level of familiarity has been reported very low in the US with only 6% having used biometrics before (Moody, 2004). Respondents in Moody´s (2004) study rated fingerprint as the most likely and iris and retina as the least likely biometric methods to use and they were concerned the most about privacy and identity theft, followed by cost associated with biometrics, lack of trust in the reliability of devices, fear of body parts being stolen and safety concerns considering eye biometrics. The acceptance of biometrics in the US has also been studied in contexts such as workplace tracking systems, airport security control and implanting an identifying RFID-chip into one´s body (Carpenter, Mcleod, Hicks, & Maasberg, 2018; Perakslis & Wolk, 2006; Summer, 2007).

In Canada, the acceptance of biometric authentication has been studied in the financial sector, where human-problems and legislation-related problems have been suggested to emerge more likely than technical problems in biometrics adoption (Assadi, Hassanein, Breward, & Head, 2009; Gatali, Lee, Park, & Kang, 2016). In the context of book store purchases, application contexts with obvious, apparent benefits to the user tend to lead to greater perception of usability and higher level of acceptance than contexts with only system or corporate benefits among the Canadian citizens (Heckle, Patrick, & Ozok, 2007).

5.4.3 Africa and Asia

Sabena et al. (2010) note that according to Unisys Security Index (Blue Bell PA, 2008) majority of consumers are willing to provide biometric identifiers to banks, government agencies and other organization for identification, but that in Asia, this willingness is under 50% for newer methods such as voice and several other physical characteristics.

In the study of Riley et al. (2009), there was no significant difference of familiarity between Indian and South African subjects, the percentage of previous use being 36% for South Africa and 39% for India. The Indian respondents

viewed biometrics more positively. Indian and South African subjects rated biometrics as a more acceptable authentication method than traditional systems.

Biometrics have been studied in the Malaysian banking applications, where trust in internet banking improved as perceived effectiveness of biometric technology improved and gait was ranked the most important method for biometrics in ATM, followed by palm, voice and signature-based methods (Normalini & Ramayah, 2017; Rasiah & Yen , 2016).

In Saudi-Arabia, users have been found to accept biometrics in e-commerce settings when they are already familiar with biometric technologies and internet (AL-Harby et al., 2010). In a workplace context, Saudi-Arabian government workers had mixed feeling about the importance of biometrics on a workplace and whether fingerprint technology on a workplace means mistrust towards employees, majority being unsure about these questions (Alhussain & Drew, 2009). They however saw notification, information and education of employees about such systems as important. The managers of the workers saw digital and technological culture and change resistance by employees to be barriers for applying biometric technologies in their organizations. Alhussain & Drew (2009) point out that in Saudi-Arabia, fingerprint technologies cause fear of radiation risks associated with the use of the technology, as well as health concerns of disease transfer through many people touching the same points in the readers.

While some security concerns and inability to share biometrically secured devices with family members cause worry in Yemen, biometrics have been rated in the country as a faster, more secure and as an option with better privacy than password-based techniques, fingerprint and iris scan being perceived as the most secure methods for ATM use (Rashed et al., 2013).

5.5 Cultural differences in biometrics

The second objective of the literature review was to discover what kind of differences in attitudes towards biometric authentication have been found between geographical areas and cultures. This question is now answered within three categories, that were identified from earlier research: Familiarity with biometrics, acceptance of biometrics and the concerns and barriers for the use of biometrics.

5.5.1 Familiarity with biometrics

The familiarity with a technology might play a part on the acceptance of biometrics. Users have difficulties in comparing familiar authentication methods with biometrics and have been found more likely to accept a biometric authentication method that seems more familiar to them, than what is best performance-wise (Brockly et al., 2014; Krol et al., 2016).

In Finland, Germany and Spain, the general knowledge of biometrics has been found to be quite low (Biosec, 2005). In another German study, under a half

of the subjects were found to have used biometrics before (Krupp et al., 2013). Riley et al. (2009) found biometrics to be little familiar within India, South Africa and United Kingdom. The British respondents were less familiar with biometric technologies than Indian and South African respondents with 24% having previously used biometrics. In an earlier UK-based study, up to 93% of respondents claimed to be aware of biometric technologies (Furnell & Evangelatos, 2007). However, the percentage of respondents claiming to have used these technologies before was significantly lower, 2% for iris and 16% for fingerprint.

In a research on a U.S workplace context, only 6% had used biometrics before (Moody, 2004). Canadian respondents have stated being ready to try biometrics as they saw it becoming a social norm and used by a lot of businesses in the future, making familiarity and knowledge of biometrics factors affecting the decision to use the technology (Heckle, Patrick, & Ozok, 2007).

Familiarity with biometrics was found to vary between countries, but also between different studies in the same country. Overall, the research of differences in the knowledge of biometrics in a cross-cultural manner was found to be low. The users' familiarity with biometrics between countries has been found to affect the acceptance and adoption decisions and thus might explain the differences between acceptance in different countries. Therefore, the following is hypothesized:

H1: The users who are already familiar with biometrics will have a higher intention to use the technology.

5.5.2 Acceptance of biometrics

European biometrics acceptance has been stated to be very high, but also lower than acceptance of knowledge-based authentication (Biosec, 2005; Deane et al., 1995). The Biosec (2005) study found the acceptance to vary across different scenarios, the use of biometrics being supported in sectors of high security requirements and in applications, that normally require the user to remember passwords and PIN-codes. The respondents were less accepting about the use of biometrics in private areas, such as in personal computers or email. The European acceptance of biometrics is also closely related to the political and societal environment (Biosec, 2005).

In Germany, up to 25% have been found not to accept biometrics at all (Krupp et al., 2013). Ninety three percent of young Swedish students could consider using biometrics in a mobile unit, 43% preferring biometrics over knowledge-based methods (Giarimi & Magnusson, 2002). In the UK, the acceptance of biometrics has been relatively high, especially in the contexts of mobile devices, high-security applications, prevention of terrorism and fraud and, to some extent, identification documents (Clarke & Furnell, 2005; Furnell & Evangelatos, 2007; Krol et al, 2016).

Riley et al. (2009) found British respondents to be less accepting of biometrics than Indian and South African respondents. British, Indian and South

African respondents were all willing to use biometrics, but the Britons less than South Africans or Indians. The Indian and South African respondents viewed biometric technologies as a more accepted authentication method than knowledge- and token-based methods.

In previous study, Yemeni people have been found to perceive biometrics as faster and more secure than password-based systems (Rashed et al., 2013). In Saudi-Arabia, people have been found to accept biometrics in an e-commerce setting, as long as they have already been familiar with biometric technologies and internet before (Al-Harby, 2010). In Asia generally, the willingness to use biometrics has been under 50% for some biometric methods (Blue Bell PA, 2008).

In the United States, consumers have been found both to and not to accept biometrics as an authentication method in personal shopping, but in workplace contexts the acceptance has been consistently lower (Clodfelter, 2010; Heckle et al., 2007; Moody, 2004). University students in the US have rated biometrics as the most popular authentication method, especially in healthcare organizations and the financial domain, but biometrics in passports, airplanes and government buildings have also gained some support (Jones, Antón, & Earp, 2007; Perakslis & Wolk, 2006). In Canada, convenience and high security are seen as attributes of biometric technologies, but context and the status of biometrics as a social norm were found to affect the perception of benefits and level of comfort in using biometric technologies (Heckle et al., 2007).

Despite the critique towards TAM, the model has been used successfully in various contexts, outside western cultures, in cross-cultural studies and also considering biometrics. TAM has been validated in Brazil and in Finland. The biometrics-specific TAM of James et al. (2006) has been repeated successfully multiple times. The James et al.'s (2006) model is therefore believed to be replicable in Finland and in Brazil to successfully explain acceptance of biometrics. Based on the model the following is hypothesized:

H2a: The perceived usefulness of the security technology will have a significant positive effect on an individual's intention to use the technology.
H2b: The perceived ease of use of the security technology will have a significant positive effect on an individual's intention to use the technology.
H2c: The perceived physical invasiveness of the security technology will have a significant negative effect on an individual's intention to use the technology.
H3a: The perceived ease of use of the security technology will have a significant positive effect on the perceived usefulness of the technology.
H3b: An individual's desire for the security of their person and his/her personal information will have a significant positive effect on the perceived usefulness of the technology.
H3c: An individual's perceived need for privacy will have a significant positive effect on the perceived usefulness of the technology.
H4: The perceived physical invasiveness of the security technology will have a significant negative effect on the perceived ease of use of the technology.

H5a: An individual's desire for the security of their person and his/her personal information will have a significant negative effect on the perceived physical invasiveness of the technology.
H5b: An individual's desire for privacy will have a significant positive effect on the perceived physical invasiveness of the technology.
H6: An individual's perceived need for privacy will have a significant positive effect on his/her need for security.

The levels of acceptance found in literature differ between countries, but also between studies within the same country. Therefore, cultural differences alone might not explain all the differences in the acceptance of biometrics. The context where biometrics are used, seems to affect the level of acceptance. The acceptance of biometrics was found generally difficult to compare between studies, because of varying research methods, reporting styles, sample populations, contexts and biometric technologies across studies.

Some cross-cultural studies have used TAM together with Hofstede's dimensions, but not all found support for the dimensions as an explanation for differences in technology acceptance. Making connections to the present study based on these results is difficult because none of such studies considered biometrics. The claims of Hofstede's dimension's unsuitability for biometrics research are only few, but Hofstede's theory is widely used and accepted in earlier research. Despite the shortcomings of Hofstede's cultural dimension theory, it was decided to expand the commonly used model of combining TAM and Hofstede's cultural dimensions to this study, first of its kind to consider the acceptance of biometrics in Brazil and South America. This study does not claim Hofstede's dimensions to exactly represent culture but uses them as a vehicle to gain insights on certain differences that occur between the researched areas and to possibly explain some of these differences. In the field of biometrics acceptance, Riley (2009) and Al-Harby (2010) have found relationships between the acceptance of biometrics and Hofstede's dimensions, but they were contradictory with earlier theories. Based on Riley et al. (2009) and Al-Harby (2010), it is hypothesized that:

H7a: Individualism versus Collectivism score will have a significant negative effect on the intention to use biometrics.
H7b: Power Distance score will have a significant positive effect on the intention to use biometrics.
H7c: Masculinity versus Femininity score will have significant positive effect on the intention to use biometrics.

The research model based on all the hypotheses is presented in the figure 2.

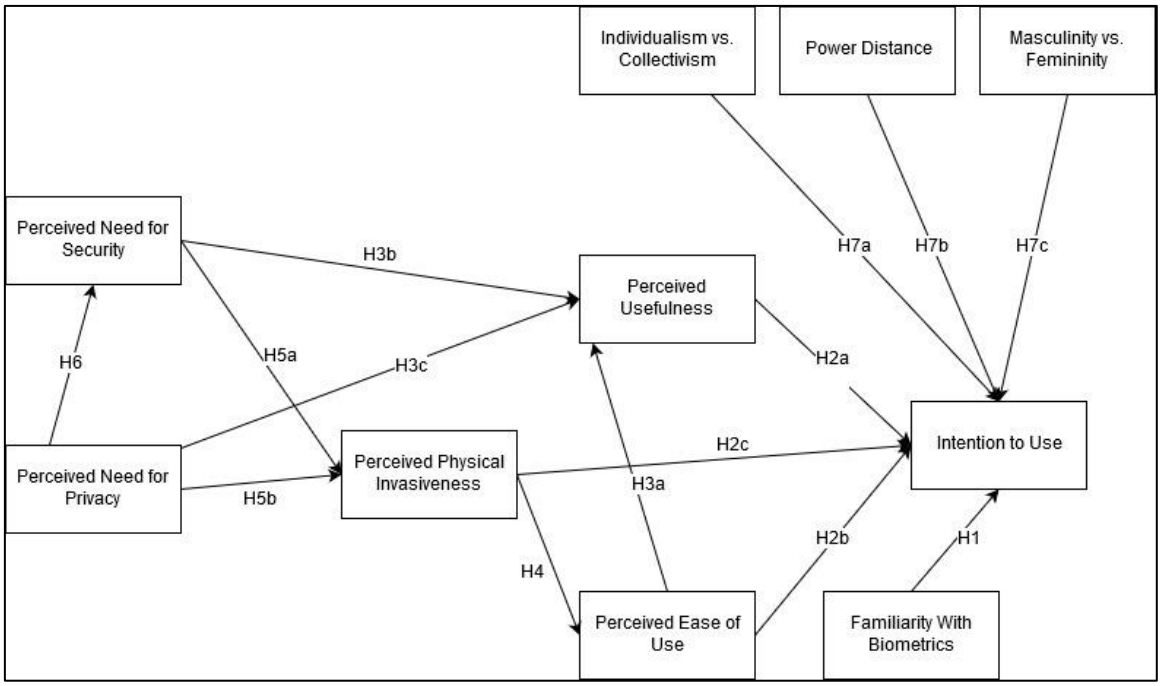

FIGURE 2 The research model

5.5.3 Concerns and barriers for the use of biometrics

Riley et al. (2009) found the security and health and safety issue fears to be major concerns related to using biometrics in UK, India and South Africa. Information security concerns were bigger in the UK, than in South Africa and India. Perceived health risks involved in some biometric technologies and the potential loss, theft and misuse of biometric data have also emerged in the UK (Furnell & Evangelatos, 2007). Considering face biometric as a CAPTCHA replacement, privacy concerns and assurance of only intended use of their facial details were the biggest concerns in the use of the technology for British respondents (Krol et al., 2016). The subjects also mentioned the inability to share the protected devices with other people and concerns of harvesting details from the pictures for advertising purposes.

Giarimi & Magnusson (2002) found 77% of the 16-18-year-old Swedish students ready to use biometrics if the sample was stored in their mobile unit, but only 51% if the sample was stored outside the mobile unit, indicating a privacy concern. Privacy concerns towards the use of personal information in authentication have emerged also in Germany (Zimmerman & Gerber, 2017). In Europe generally, minor concerns about the physical harmfulness of biometrics have emerged (Biosec, 2005).

In the United States, the biggest concerns have been privacy and identity theft concerns, the cost associated with biometrics, lack of trust in the reliability of biometric devices, fear of body parts being stolen and safety concerns considering eye biometrics (Moody, 2004). Jones, Antón, & Earp (2007) however claim the U.S population to not be very concerned about the impact of biometric authentication technologies on their privacy.

In Canada, privacy and security concerns were found to cause significant negative influence on the consumer acceptance of biometrics (Assadi et al., 2009). The concerns included inadvertent scenarios, such as a security breach, and intentional scenarios, such as financial institutions sharing information with other entities. Consumers were found to accept biometrics in financial transactions better, if they had more control over their biometric data. Also Gatali, Lee, Park, & Kang (2016) report the possible public concerns and privacy to be the biggest issues of biometrics adoption in Canada. Other noted issues include lack of education on the easiness and perceived security of biometrics, unclear privacy laws considering biometrics in banking and highly coordinated industry members and regulatory boards in the government. Insufficient knowledge of biometrics has caused hesitation to use biometrics in Canada as well (Heckle et al., 2007).

In Yemen, users have been concerned about the security of biometric technologies, and not being able to share biometrically secured devices with family members (Rashed et al., 2013). Saudi-Arabian managers have perceived digital and technological culture, employee resistance, system failures and the inability for a system to take fingerprints from some users to be barriers for applying fingerprint scanning on workplaces (Alhussain & Drew, 2009). In Saudi-Arabia, fingerprint technologies are also feared to cause radiation-risks and disease transfer among employees (Alhussain & Drew, 2009).

Only few concerns considering the technical functioning of the biometric devices were identified. Most studies mentioned concerns of information security and privacy, misuse, loss and theft of data, control over own data, safety of physical health and body parts being stolen. Most of the concerns can roughly be categorized under privacy and security issues, which are addressed in the extended TAM of James et al. (2006). Some other concerns also emerged, such as social concerns of not being able to share biometric password with close people. Once again, there were contradicting results between different studies considering the same countries.

This chapter concludes the first part of the study. Next part conducts the empirical study, which examines cultural differences in biometrics acceptance between Brazil and Finland. The empirical part begins by presenting the research methods of the study.

6 RESEARCH METHODS

In this chapter, the research methods of the empirical study are presented. The aim of the study was to clarify, how the acceptance of biometrics is formed in different cultures, by expanding the cultural biometrics acceptance research to Brazil from South America, comparing it with Finland from Nordic Europe. The study in question is a descriptive study, because it uses survey data to describe the state of affairs as they exist at present, using variables that cannot be controlled (Kothari, 2009, pp. 2-3). The research is quantitative in nature, as the survey collects Likert-scaled data, which can be expressed in terms of quantity and analyzed in a formal and rigid fashion (Kothari, 2009, pp. 3-5). Kothari (2009, pp. 4) explains empirical research to be data-based research, which comes up with conclusions that can be verified by observation or experiment.

6.1 Participants

The questionnaire was targeted to Finnish and Brazilian university students. By targeting university students, costs could be minimized and the results from the survey compared to previous and future studies utilizing a similar population. Using a student sample also allowed to gather and examine a similar sample across two different cultures. The Finnish survey was sent to the biggest faculties and subjects associations in one Finnish university. The Brazilian version was sent to the biggest faculties and student organizations in one Brazilian university. Thus, a random sample from this university student population was acquired. Random sampling should be the method of choice in most researches, in order to minimize bias and to estimate sampling error (Kothari, 2009, pp. 15).

A total of 815 people opened the questionnaire, 563 started answering and 312 completed it as a whole. A total of 150 Finnish responses and 152 Brazilian responses were collected. Hofstede (2013) suggest an ideal size for a homogenous sample for the Values Survey Module 2013 (VSM13) to be 50 for each country, while samples below 20 respondents should be avoided. A sample size of 125

from each country is enough for multiple regression analyses, achieving a power of .80 at medium effect size and α = .05, according to the sample size requirements calculated by Cohen (1992). Hence, the sample size is enough to use VSM13 and to run the intended regression analyses. The respondents to the survey were distributed by nationality, gender and age groups. The distributions can be seen from the table 4 and table 5.

TABLE 4 Distribution of the survey respondents by nationality and gender

Gender	Finnish	Brazilian	Total
Male	64	57	121
Female	61	68	129
Total	125	125	250

TABLE 5 Distribution of the survey respondents by nationality and age

Age	Finnish	Brazilian	Total
Under 20	5	5	10
20-29	88	88	176
30-39	21	21	42
40-49	7	7	14
Over 50	4	4	8
Total	125	125	250

6.2 Measures: Survey design

Following various examples from the reviewed literature, a quantitative questionnaire was decided to be the method of choice for this study. Majority of the studies used questionnaires with Likert-scaled variables to measure various aspects of attitudes and perceptions of biometrics (e.g. James et al., 2006; Kanak & Sogukpinar, 2017). Most commonly, extensions and modifications of the Technology Acceptance Model were used. Some studies asked open-ended interview questions to attain qualitative data and responses about the opinions, problems and barriers considering the use and applying of biometric technologies (e.g. Gatali et al., 2006). Some exceptions to the questionnaire- and interview-research were found in a form of laboratory researches (e.g. Heckle, Patrick, & Ozok, 2007; Zimmerman & Gerber, 2017).

6.2.1 The initial questionnaire

From the technology acceptance models focusing especially on biometric technologies, the model of James et al. (2006) was selected. The questionnaire has been successfully used in earlier research more than once. Their model includes the constructs for perceived need for privacy, perceived need for security and perceived physical invasiveness, which were factors identified in the literature review to affect biometrics acceptance. Based on the model, they developed a questionnaire which includes vignettes to represent several different biometrics use cases, which will help in determining the general acceptance of biometrics in Finland and in Brazil, free of situational bias. The used biometric devices, their behavioral or physiological nature, the context of use, compulsion of use and the required time for authentication in each vignette are specified in table 6.

TABLE 6 Biometric technologies used in the vignettes

	Biometric device	**Behavioral / Physiological**	**Use context**	**Compulsory / Voluntary**	**Time required for authentication**
Vignette 1	Hand geometry scanner	Physiological	Physical access, employed as individual choice	Voluntary	A few seconds
Vignette 2	Facial scanner	Physiological	Physical access in organization	Compulsory	A few seconds
Vignette 3	Retinal scanner	Physiological	Physical access in organization	Compulsory	A few seconds
Vignette 4	Fingerprint scanner	Physiological	Virtual access in organization	Voluntary	Instantaneous
Vignette 5	Hand geometry scanner	Physiological	Physical access in organization	Compulsory	A few seconds
Vignette 6	Fingerprint scanner	Physiological	Virtual access in organization	Compulsory	Instantaneous
Vignette 7	Retinal scanner	Physiological	Virtual access in organization	Compulsory	A few seconds
Vignette 8	Signature biometrics	Behavioral	E-commerce	Compulsory	Not informed

Questionnaire items measuring cultural values are taken from VSM13 (Hofstede & Minkov, 2013), which is the newest official questionnaire measuring Hofstede's cultural dimensions. Because Hofstede's original dimension scores are

already decades old and thus might already be outdated, new data to calculate the dimension scores was collected. This way, the applicability of Hofstede's dimensions to the samples in question could be verified.

The awareness of and familiarity with biometrics is measured by asking, whether the respondents have heard of or used biometrics, as done e.g. in Furnell & Evangelatos (2007). The items measuring demographic details of the respondents were combined from James et al. (2006), the VSM13 (Hofstede, 2013) and the reports by IBGE (2016), which were utilized in the literature review. The choice of the demographic questions was based on the literature review, where for an example gender and age were found to affect technology acceptance, and profiles such as "relatively young, well-educated family man with a good job and high income-level" were identified for typical technology users.

According to Mackenzie, Podsakoff & Podsakoff (2011), the first step in a scale development procedure is to develop a conceptual definition of the used constructs. The questionnaire is based on TAM and thus important constructs to measure are perceived usefulness, perceived ease of use and behavioral intention to use a technology. These constructs have been defined in the chapter 3.1 of the literature review. As suggested by Mackenzie et al. (2011), the type of property the construct represent, and the entity to which it applies should be defined. Perceived usefulness and perceived ease of use refer to a perception of a person about the use of a technology. Behavioral intention refers to the actual intention of a person to use a specified technological solution.

In the literature review, security and privacy factors were found to affect the adaption and attitudes towards biometrics and to differ between nations and cultures. Therefore, security and privacy perceptions are points of interest in this study. The additional constructs presented by James et al. (2006), perceived need for security and perceived need for privacy, refer to a person's level of need regarding security and privacy. James et al. (2006) define security as the protection of physical and digital assets and perceived need for security as one's perceived need for the safekeeping of physical or informational assets. Their definition of privacy is from Westin (1967, pp.7), who defines it as the ability of an individual to control the terms under which personal information is acquired and used. Therefore James et al. (2006) define perceived need for privacy as the importance to an individual of being able to control the acquisition and usage of personal information.

The literature review also found certain health and safety concerns to act as barriers to the use of biometrics, indicating and issue with physical invasiveness of biometric authentication. The model of James et al. (2006) includes perceived physical invasiveness of a biometric device as a factor affecting the intention to use. Perceived physical invasiveness refers to a person's perception about the level of invasiveness of a biometric device on their physical being. James et al. (2006) define invasiveness as an intrusion or encroachment to one physically and/or from a privacy standpoint. Perceived physical invasiveness therefore is the perception of discomfort or fear from the physicality of the device use (James et al., 2006).

The constructs considering Hofstede's dimensions have been defined in the chapter 4.1 of the literature review. The constructs in Hofstede's theory refer to the collective cultural values of a nation, or to the espoused cultural values of an individual, as used by Srite & Karahanna (2006).

The demographics used for the Finnish and Brazilian versions of the study were equal, apart from the question asking ethnicity information. In Finland, Statistics Finland (Tilastokeskus), the national statistical institution, classifies people based on nationality, language and birth country instead of ethnicity or race (Nieminen, 2013). No established scale of classifying a person's race or ethnicity exists in Finland or in Finnish academic literature and thus the background details of nationality, nationality at birth and native language were used instead. This approach is however not ideal, since asking for a native language does not reveal for an example the members of the Roma minority, of which majority are registered in Finnish civil registry as Finnish or Swedish speaking (Nieminen, 2013).

In Brazil however, the standard classification of the official government census is based on color and race. Including this statistical information in a research conducted in Brazil is important in order to compare the sample population to the actual, diverse population, and to capture differences between groups of different racial and ethnic cultural identities. For these reasons, the racial classification was included in the study, while acknowledging that using such classification could be considered inappropriate or offensive in Finland and in the English language. According to Statistics Finland, a respondent should also have a chance to define their ethnicity in an open response, and choose not to answer (Nieminen, 2013). These principles were decided to be applied on the Brazilian questionnaire version, too.

The rest of the questionnaire items were equal in the Finnish and Brazilian versions. Respondents from both countries could choose to see all the questions in their local language or in English. Changing the language of the survey was also possible at any moment while responding the survey.

An example of a questionnaire item measuring each of the examined constructs in the first pilot version can be seen in a table 7. The table includes the reference to the original studies, where the items were used. If no reference is provided, the question is original to this study. The final questionnaire and its translations can be found in appendix 1.

Some changes were made to the original survey questions of James et al. (2006) and Hofstede's and Minkov's (2013) VSM13. The question "How proud are you to be a citizen of your country?" was changed to "How proud are you to be a citizen of Finland?" and "How proud are you to be a citizen of Brazil?" to make it easier to translate into Finnish while maintaining the original meaning of asking about current citizenship. Some wordings in the demographic questions were changed from the original questions.

In one of the questions measuring perceived need of security by James et al. (2006), references to the Olympics and Super Bowl were changed to "big sports competitions" to make the question more internationally applicable, as the Super

Bowl is only hosted in the United States. Some wordings in the responding instructions were changed from James et al. (2006) to make the scales and instructions match with the rest of the questionnaire. These wordings were changed without changing the meaning of the questions or scales. In addition, the names in the original Vignettes were changed to popular Finnish and Brazilian names.

TABLE 7 Questionnaire item examples for the pilot survey

Construct	**Questionnaire item**	**Originally used in**
Perceived Need for Security	I feel that my personal security at my home or in my vehicle is important to me.	James, Pirim, Boswell, Reithel, & Barkhi (2006)
Perceived Need for Privacy	I feel that my control over my personal information is very important to me.	James, Pirim, Boswell, Reithel, & Barkhi (2006)
Perceived Usefulness	I think this biometric device is useful.	James, Pirim, Boswell, Reithel, & Barkhi (2006)
Perceived Ease of Use	I think this biometric device is easy to use.	James, Pirim, Boswell, Reithel, & Barkhi (2006)
Perceived Physical Invasiveness	I think that this device would be physically invasive.	James, Pirim, Boswell, Reithel, & Barkhi (2006)
Intention to Use	I think I would use this device.	James, Pirim, Boswell, Reithel, & Barkhi (2006)
Knowledge of Biometrics	Have you heard of biometrics? 1. Yes 2. No	
Familiarity With Biometrics	Have you used biometrics? 1. Yes 2. No	
Individualism versus Collectivism	have sufficient time for your personal or home life	Hofstede & Minkov (2013)
Power Distance	have a boss (direct superior) you can respect	Hofstede & Minkov (2013)
Masculinity versus Femininity	get recognition for good performance	Hofstede & Minkov (2013)
Indulgence Versus Restraint	moderation: having few desires	Hofstede & Minkov (2013)
Long Term Orientation	thrift (not spending more than needed)	Hofstede & Minkov (2013)
Uncertainty Avoidance	One can be a good manager without having a precise answer to every question that a subordinate may raise about his or her work	Hofstede & Minkov (2013)

The questionnaire was given to experts in information security and social sciences in Finland and in Brazil. The questionnaire items were adjusted according to their comments.

6.2.2 The Finnish version

After the initial version of the questionnaire was completed in English, a translation into Finnish took place. The translation was done separately by two native Finnish speakers. The two translations were compared and searched for differences. The two translators then arranged a meeting to discuss the differences found and agreed on which version to use for each question. The final translation, approved by both translators, was used for a pilot test in Finland. The respondents had a choice to display each question in English or in Finnish. They could also change the language during the survey. In addition to the actual survey questions, the pilot study subjects were asked to give comments about the survey items and the survey in general.

As suggested by the pilot survey respondents, the order of the privacy- and security -related questions was randomized, in order to avoid very similar questions being asked right after each other. Some respondents also reported, that they answered not being familiar or aware of biometrics, but after reading the vignettes, they realized what biometric technologies actually include, and that in fact they were more aware and familiar with biometrics than what they initially responded. A small paragraph presenting biometric technologies and their use was therefore added in the introduction of the survey.

Based on the pilot survey results, Cronbach's alpha was calculated in IBM SPSS for each of the constructs to evaluate their reliability and internal consistency. All the TAM-constructs were found reliable with a Cronbach's alpha of >.700 (Nunnally, 1978). An analysis was run to see, how the reliability would change if some of the questionnaire items were deleted, but the differences were so small, that no action was taken. The constructs consisting of items measuring Hofstede's dimensions were not found reliable based on Cronbach's alpha. This was expected, because Hofstede's dimensions do not necessarily correlate on an individual level in the manner as they correlate on country-level (Hofstede, 2013). Hofstede (2013) explains, that as the questions are used to measure country-level dimensions, the answers do not necessarily correlate across individuals, and thus a reliability-test such as Cronbach's alpha should be done based on country mean scores. Because this study generated a country mean score for only two countries, Cronbach's alpha could not be counted on a country-level. Hofstede (2013) however suggests, that the reliability can be indirectly shown through the validity of the scores in predicting dependent variables. He has calculated Cronbach's alphas for the original four dimensions, based on the original IBM-study database. These values are presented in table 8.

TABLE 8 Cronbach´s alphas for Hofstede´s original dimensions based on the IBM-database

	PDI	**IDV**	**MAS**	**UAI**
α	0.84	0.77	0.76	0.72

Despite the high scores on Cronbach's alphas on the TAM-constructs, some changes were made from the pilot questionnaire to the final version. A commonly

known translation of the word "invasive" does not exist in the Finnish language. Many pilot test subjects reported not to understand the word and thus they could not answer the questions related to physical invasiveness well. The translation for the word was changed to a translation of the word "intrusive", which is not an exact equivalent of "invasive", but which is better understood in this context in the Finnish language. Other, small changes to the Finnish translation were made, to make the used language more understandable, without changing the meanings of the questions. All the changes to the Finnish translations were verified by the two original, native translators.

After collecting the final data, a Confirmatory Factor Analysis (CFA) was run in SmartPLS for the translated questionnaire items and Cronbach's alphas were calculated again for each construct. The final Cronbach´s alphas in table 9 show that all the TAM-constructs were reliable, but none of the Hofstede´s dimension constructs crossed the reliable threshold, as expected. Because the Technology Acceptance Model by James et al. (2006) and Hofstede's theory of cultural dimensions are separate models, they were analyzed by separate CFA´s. Both models were also tested separately for each country sample.

TABLE 9 Cronbach´s alphas for the final constructs in Finnish sample

	P	**S**	**PU**	**PEOU**	**PI**	**IU**	**PDI**	**IDV**	**MAS**	**UAI**	**LTO**	**IVR**
α	0.79	0.83	0.82	0.80	0.92	0.86	0.06	0.21	0.21	0.35	-0.03	-0.00

P = Perceived Need For Privacy, S = Perceived Need For Security, PU = Perceived Usefulness, PEU = Perceived Ease of Use, PI = Perceived Physical Invasiveness, IU = Intention to Use, PDI = Power Distance, IDV = Individualism vs. Collectivism, MAS = Masculinity vs. Femininity, UAI = Uncertainty Avoidance, LTO = Long vs. Short Term Orientation, IVR = Indulgence vs. Restraint

CFA was run for the Perceived Need for Security and Perceived Need for Privacy -constructs. The items measuring the original TAM-construct all had equal questions after eight vignettes, considering different situations and contexts of biometrics use. Following the example of James et al. (2006), factor analysis did not consider the other TAM-constructs, because the analysis would actually measure the vignettes instead of the survey items.

The model fit assessment guide of SmartPLS considers the root mean square residual (SRMR) less than 0.10 to be a sufficient fit (SmartPLS GmbH, 2019). In this model, the value was 0.128. By deleting some items with low factor loadings, a good fit of the data was reached while maintaining the Cronbach's alphas and Composite Reliability over their significant thresholds. After deleting the items S3, S4, S6, P7 and P8 (see appendix 1 for content of each item), the SRMR-value fell to 0.093.

Average Variance Extracted (AVE) was not sufficient on the >.50 level for neither construct, indicating weak convergent validity (Hair, Black, Babin & Anderson, 2009). Malhotra (2010) however argues, that an adequate convergent validity can be shown based on Composite Reliability alone. Composite Reliability was found sufficient, >.70, for both constructs in the Finnish sample (Hair et al.,

2009). The Composite Reliability and AVE for the TAM-constructs in the Finnish sample are presented in table 10.

TABLE 10 Composite Reliability and Average Variance Extracted of the TAM-constructs in the Finnish sample

	Composite Reliability	**Average Variance Extracted (AVE)**
Perceived need for privacy	0.784	0.348
Perceived need for security	0.744	0.343

To achieve discriminant validity, items should have higher factor loadings in their corresponding constructs than in the other constructs, and the square root of AVE should be higher than the inter-construct correlations (Chin, 1998). As can be seen from table 11, all items loaded more strongly to their corresponding constructs than the other construct. The Fornell-Larcker criterion also showed higher AVE square root values than inter-construct correlations for the constructs. The inter-construct correlations are presented in table 12.

TABLE 11 Factor loadings for the TAM-constructs in the Finnish sample

	Perceived Need for Privacy	**Perceived Need for Security**
P1	**0.748**	0.675
P2	**0.688**	0.620
P3	**0.551**	0.496
P4	**0.495**	0.446
P5	**0.489**	0.441
P6	**0.626**	0.564
P9	**0.474**	0.428
S1	0.350	**0.389**
S2	0.412	**0.457**
S5	0.375	**0.416**
S7	0.676	**0.750**
S8	0.534	**0.592**
S9	0.704	**0.781**

TABLE 12 Inter-construct correlations for the TAM-constructs in the Finnish sample

	Intention to use	Perceived ease of use
Perceived need for privacy	0.590	
Perceived need for security	0.901	0.585

While acknowledging that the items considering Hofstede´s dimensions do not necessarily correlate across individual responses and that the reliability of the constructs should be taken for granted according to Hofstede (2013), a CFA was run in order to evaluate the reliability and validity across our specific samples. None of the Hofstede's dimension constructs had their convergent validity supported based on AVE nor Composite Reliability, as seen from table 13. The SRMR was 0.100, reaching the lower end of sufficient model fit threshold. No improvement to construct reliability or convergent validity could be achieved by removing the items with lowest factor loadings.

TABLE 13 Composite Reliability and Average Variance Extracted of the Hofstede's constructs in the Finnish sample

	Composite Reliability	Average Variance Extracted (AVE)
Individualism	0.107	0.099
Indulgence	0.073	0.100
Long Term Orientation	0.022	0.158
Mascilinity	0.026	0.053
Power Distance	0.017	0.160
Uncertainty Avoidance	0.421	0.210

Discriminant validity was not supported for any of the culture constructs in Finland based on the item cross-loadings, as the factors cross-loaded to other dimensions against the theorized factor structure. The cross-loadings for the cultural constructs in Finland are presented in table 14. The Fornell-Larcker criterion supported the discriminant validity with higher inter-construct correlations than the AVE square root values for all the constructs, except for Uncertainty Avoidance. These inter-construct correlations in Finnish data can be seen in table 15.

TABLE 14 Factor loadings for the Hofstede's constructs in the Finnish sample

	Individualism	Power Distance	Masculinity	Indulgence	Long Term Orientation	Uncertainty Avoidance

(to be continued)

Table 14 (to be continued)

IDV1	**0.020**	-0.136	0.129	-0.256	0.027	0.102
IDV2	**0.314**	-0.328	-0.575	0.014	0.285	-0.266
IDV3	**-0.187**	0.149	0.318	0.280	-0.255	-0.068
IDV4	**0.510**	-0.450	-1.094	-0.177	0.485	-0.120
PDI1	-0.517	**0.553**	0.641	0.145	-0.498	-0.015
PDI2	0.427	**-0.543**	-0.661	-0.384	0.350	0.285
PDI3	-0.044	**0.032**	0.180	-0.224	-0.041	0.088
PDI4	-0.361	**0.198**	0.364	-0.122	-0.066	0.214
MAS1	-0.522	0.185	**0.237**	0.052	-0.267	0.266
MAS2	0.345	-0.275	**-0.174**	-0.027	0.102	-0.139
MAS3	0.137	-0.198	**-0.091**	-0.041	-0.068	-0.226
MAS4	-0.682	0.446	**0.345**	0.373	-0.356	-0.044
IVR1	-0.277	-0.050	0.228	**0.005**	0.011	0.078
IVR2	0.474	-0.234	-0.373	**-0.229**	0.331	-0.042
IVR3	-0.163	0.200	0.390	**0.552**	-0.525	-0.554
IVR4	0.263	-0.018	-0.109	**0.207**	-0.114	-0.430
LTO1	0.393	-0.325	-0.351	-0.418	**0.408**	0.070
LTO2	-0.354	0.274	0.465	0.331	**-0.344**	0.123
LTO3	0.561	-0.382	-0.526	-0.387	**0.509**	0.181
LTO4	-0.170	0.175	0.046	0.451	**-0.297**	-0.333
UAI1	-0.166	-0.138	0.372	-0.688	0.177	**0.704**
UAI2	-0.204	-0.048	0.129	-0.530	0.256	**0.553**
UAI3	-0.015	-0.190	-0.011	-0.203	-0.047	**0.179**
UAI4	-0.557	0.039	0.421	0.070	-0.270	**0.080**

TABLE 15 Inter-construct correlations for Hofstede's dimensions in the Finnish sample

	Individualism	**Indulgence**	**Long Term Orientation**	**Masculinity**	**Power Distance**	**Uncertainty Avoidance**
Individualism	0.314					
Indulgence	-0.363	0.316				
Long Term Orientation	0.978	-0.973	0.397			
Mascilinity	-2.019	0.699	-0.925	0.231		
Power Distance	-0.921	0.401	-0.749	1.234	0.401	
Uncertainty Avoidance	-0.329	-0.962	0.281	0.434	-0.184	0.458

6.2.3 The Brazilian version

Based on the final version of the questionnaire, a Portuguese translation was also made. To examine demographics more accurately, a question for annual household income for Brazil was presented in the local currency and taking into condition the lower income and purchasing power in the country (NationMaster.com, 2014; The World Bank Group, 2019). The question asked the income in

monthly basis, as opposed to the yearly scale in the Finnish version, since all the official governmental sources and other Brazilian surveys examined in the literature review asked and reported household income on a monthly basis.

A Brazilian Portuguese version of the VSM13 was already available on the Values Survey Module -website (Hofstede, Chueke, Pavan, & Avrichir, 2014). This translation was slightly changed to match better the original English version and the Finnish translation. The correctness of the translation was verified by one native and one fluent Brazilian Portuguese speaker. For the rest of the questionnaire, one native and one fluent Brazilian Portuguese speaker made separate translations, like in the Finnish version. The two translations were again compared, and in a meeting, the final versions of the translated questions were agreed upon. A pilot study was made also for the Brazilian version of the survey.

Cronbach's alphas were calculated again for the final data. The values generally fell a little, but most of the TAM-constructs were found reliable with Cronbach's alphas >.700. Perceived need for privacy, however, fell to α = .627. The analysis found out, that if the question "I feel that the use of personal information that has been released by me but is used in a manner not intended by me is unacceptable." was deleted, Cronbach's alpha would rise to α = .700. One reason for this could be, that the Portuguese translation might not capture the same message as the English and Finnish versions. However, several native speakers were consulted in addition to the original translators, and they all confirmed, that the translation is correct. Another possible explanation is, that Brazilians, or the subjects of the pilot sample do not see this type of use of their data as such a privacy infringement as the issues in other items. As the translation was confirmed to reflect the same message as the original questionnaire item, it was decided to be left in the final questionnaire. Only small spelling changes were done to the final survey, without changing any meanings of the questions.

All TAM-constructs were found reliable based on Cronbach's alpha also in the Brazilian data, but again none of the Hofstede´s dimension constructs crossed the reliable level. The Cronbach´s alphas are presented in table 16.

TABLE 16 Cronbach´s alphas for the final constructs in Brazilian sample

	P	**S**	**PU**	**PEOU**	**PI**	**IU**	**PDI**	**IDV**	**MAS**	**UAI**	**LTO**	**IVR**
α	0.69	0.86	0.87	0.86	0.90	0.85	-0.07	0.16	0.13	0.12	-0.21	0.13

P = Perceived Need For Privacy, S = Perceived Need For Security, PU = Perceived Usefulness, PEU = Perceived Ease of Use, PI = Perceived Physical Invasiveness, IU = Intention to Use, PDI = Power Distance, IDV = Individualism vs. Collectivism, MAS = Masculinity vs. Femininity, UAI = Uncertainty Avoidance, LTO = Long vs. Short Term Orientation, IVR = Indulgence vs. Restraint

In the Brazilian data, Composite Reliability indicated convergent validity for Perceived Need for Security, but not for Perceived Need for Privacy. AVE showed no convergent validity for neither construct . The Composite Reliabilities and AVE´s for TAM-constructs in the Brazilian data are presented in table 17. The data was not found to fit the model, SRMR being 0.160. By deleting items starting

from the lowest factor loadings, the Cronbach's alphas, Composite Reliabilities and AVE's weakened without any significant improvements to the SRMR-value.

TABLE 17 Composite Reliability and Average Variance Extracted of the TAM-constructs in the Brazilian sample

	Composite Reliability	**Average Variance Extracted (AVE)**
Perceived need for privacy	0.63	0.19
Perceived need for security	0.86	0.35

Discriminant validity was supported based on the factor loadings, which loaded more strongly to their corresponding constructs than the others, as shown in the table 18. The Fornell-Larcker criterion also supported the discriminant validity and showed higher AVE square root values than inter-construct correlations for the constructs, as seen in table 19.

TABLE 18 Factor loadings for the TAM-constructs in the Brazilian sample

	Perceived Need for Privacy	**Perceived Need for Security**
P1	**0.460**	0.352
P2	**0.849**	0.649
P3	**0.436**	0.333
P4	**0.259**	0.198
P5	**0.521**	0.398
P6	**0.213**	0.163
P7	**0.176**	0.134
P8	**0.258**	0.197
P9	**0.368**	0.281
S1	0.303	**0.396**
S2	0.308	**0.403**
S3	0.382	**0.501**
S4	0.281	**0.368**
S5	0.292	**0.382**
S6	0.347	**0.454**

(to be continued)

Table 18 (to be continued)

S7	0.563	**0.737**
S8	0.611	**0.800**
S9	0.713	**0.933**

TABLE 19 Inter-construct correlations for the TAM-constructs in the Brazilian sample

	Intention to use	**Perceived ease of use**
Perceived need for privacy	0.440	
Perceived need for security	0.764	0.588

None of the Hofstede's dimension constructs reached convergent validity based on AVE nor Composite Reliability in Brazil, as seen from table 20. The SRMR was 0.105, so the data did not fit the model. No improvement to model fit, construct reliability and convergent validity could be achieved by removing the items with lowest factor loadings in Finland either.

TABLE 20 Composite Reliability and Average Variance Extracted of the Hofstede's constructs in the Brazilian sample

	Composite Reliability	**Average Variance Extracted (AVE)**
Individualism	0.001	0.064
Indulgence	0.001	0.081
Long Term Orientation	0.001	0.161
Mascilinity	0.020	0.158
Power Distance	0.008	0.062
Uncertainty Avoidance	0.060	0.082

The factors cross-loaded to other cultural dimensions against the theorized factor structure, not supporting discriminant validity. The cross-loadings for the Hofstede's constructs are presented in table 21. The Fornell-Larcker criterion however supported discriminant validity with higher inter-construct correlations than the AVE square root values for all the constructs. The inter-construct correlations for Brazil can be seen in table 22.

TABLE 21 Factor loadings for the Hofstede's constructs in the Brazilian sample

	Individualism	**Power Distance**	**Masculinity**	**Indulgence**	**Long Term Orientation**	**Uncertainty Avoidance**
IDV1	**-0.162**	0.531	0.172	0.398	0.028	0.287
IDV2	**0.247**	-0.508	-0.523	-0.290	0.075	0.126
IDV3	**-0.303**	0.290	0.538	0.550	-0.374	-0.023
IDV4	**0.281**	-0.447	-0.537	-0.294	0.336	-0.041
PDI1	-0.487	**0.281**	0.365	0.309	-0.092	0.310
PDI2	0.525	**-0.369**	-0.598	-0.341	0.254	-0.235
PDI3	-0.290	**0.119**	0.162	0.151	0.044	0.058
PDI4	-0.322	**0.140**	0.046	0.064	-0.094	0.409
MAS1	-0.676	0.693	**0.289**	0.118	-0.132	0.110
MAS2	0.624	-0.669	**-0.479**	-0.851	0.477	0.002
MAS3	0.860	-0.408	**-0.435**	-0.693	0.321	-0.269
MAS4	-0.792	0.522	**0.360**	0.455	-0.191	0.001
IVR1	-0.617	0.388	0.553	**0.309**	-0.105	0.251
IVR2	0.583	-0.421	-0.545	**-0.449**	0.710	-0.054
IVR3	-0.213	-0.064	0.349	**0.154**	-0.188	-0.344
IVR4	0.010	-0.209	0.037	**-0.069**	0.132	-0.708
LTO1	0.497	-0.336	-0.451	-0.803	**0.626**	-0.081
LTO2	-0.183	0.188	0.395	0.492	**-0.407**	0.150
LTO3	0.170	-0.118	-0.052	-0.125	**0.108**	0.128
LTO4	-0.548	0.111	0.131	0.200	**-0.273**	0.231
UAI1	-0.192	0.293	0.107	0.193	-0.144	**0.389**
UAI2	0.033	0.112	-0.148	-0.026	0.151	**-0.045**
UAI3	-0.225	-0.307	0.083	-0.068	0.022	**-0.215**
UAI4	0.008	0.385	0.129	0.019	-0.039	**0.357**

TABLE 22 Inter-construct correlations for Hofstede's dimensions in the Brazilian sample

	Individualism	**Indulgence**	**Long Term Orientation**	**Masculinity**	**Power Distance**	**Uncertainty Avoidance**
Individualism	0.254					
Indulgence	-1.493	0.285				
Long Term Orientation	0.860	-1.197	0.401			
Masculinity	-1.826	1.436	-0.752	0.397		
Power Distance	-1.647	0.963	-0.513	1.402	0.249	
Uncertainty Avoidance	-0.077	0.298	-0.250	0.235	0.956	0.286

All in all, Composite Reliability was found sufficient for all TAM-constructs except for perceived need for privacy in Brazil. AVE, however, was not meaningful

for any of those constructs. The discriminant validity was supported by Fornell-Larcker criterion and factor cross-loadings for privacy- and security-constructs in both countries. A good fit of data for the TAM-constructs was achieved in the Finnish data after deletion of some items with low factor loadings, but no good fit was possible to establish for the Brazilian data. The Brazilian data will be analyzed while including all the TAM-items, but the security- and privacy-constructs will include less items in Finland. The CFA for Hofstede's dimension constructs can be considered failed. No clear factor structures could be established, except very weakly for Uncertainty Avoidance in Finland, and no reliability or validity for the constructs could be shown. Data analysis will include all the culture-items in both countries.

6.3 Procedure

Web surveys were used for data collection. The link to the Finnish survey was distributed via emails and Facebook groups. The emails were sent out by the faculty staff, but it was clearly mentioned, that the email content was written, and the study conducted by the author of the thesis. Majority of the Facebook posts were written by the author, but one Brazilian student also shared the same message in some Facebook groups, which had a large member bases of students, but where the author had no access.

The covering note for the emails and Facebook posts mentioned, that the questionnaire examines the societal views, attitudes towards biometrics authentication technologies and security and privacy perceptions of Finnish and Brazilian respondents. It was explained, that responding the questionnaire does not require any previous knowledge of biometrics or any other technology, and that any citizen of Finland or Brazil could participate. The recipients were also informed, that responding was completely anonymous.

Filling out the survey was done completely online. The survey was applied by utilizing the survey-software Webropol. First the subjects were presented a welcome message, which consisted of an ethical disclaimer, information about the content and motivation of the study, and a short explanation of what biometric authentication technologies are.

The subjects were also informed in the welcome page, that they could stop answering at any time and not have their answers included in the final report. Based on the comments from pilot test subjects, the whole process of answering the questionnaire had an approximate duration of 15-20 minutes.

When proceeding with the survey, the subjects were first asked for demographic information, including age, gender, employment and education backgrounds. The subjects were also asked whether they were of Brazilian or Finnish nationality, and were redirected to the right questionnaire, if the nationality did not match with the current page. Next, the participants were asked questions related to the studied constructs. This was followed by a page thanking the participants and giving them instructions for addressing any additional questions.

7 RESULTS

Data from 250 respondents to the questionnaire was used to measure 14 constructs. Data considering cultural dimension- and TAM-constructs was measured to predict technology acceptance in Finland and Brazil. SPSS was used to assess the normal distribution of each of the studied construct and to do parametric and non-parametric t-tests and regression analyses accordingly. The results from testing the research model are summarized in figure 3.

7.1 Descriptive statistics

The mean and standard deviations, minimum values and maximum values for each construct in both countries are presented in table 23. All the constructs were composed out of the total 125 respondents' answers in each country. All the standard deviations were low (<1), indicating that the individual scores were close to the mean scores.

TABLE 23 Minimum score, maximum score, mean and standard deviation of studied constructs per country

		Minimum	Maximum	Mean	Std. Deviation
Perceived Need for Security	Finland	3.17	5.00	4.52	0.41
	Brazil	3.00	5.00	4.60	0.40
Perceived Need for Privacy	Finland	3.00	5.00	4.48	0.48
	Brazil	3.11	5.00	4.28	0.43
Perceived Usefulness	Finland	1.38	5.00	3.81	0.69
	Brazil	2.13	5.00	4.32	0.59
Perceived Ease of Use	Finland	1.38	5.00	3.84	0.60
	Brazil	1.75	5.00	4.10	0.67
Perceived Physical Invasiveness	Finland	1.00	4.75	2.65	0.93
	Brazil	1.00	4.63	2.47	0.86
Intention to Use	Finland	1.38	5.00	3.42	0.86

(to be continued)

Table 23 (to be continued)

	Brazil	2.00	5.00	4.03	0.70
Power Distance	Finland	2.00	4.25	3.17	0.41
	Brazil	2.25	4.25	3.26	0.42
Individualism vs Collectivism	Finland	2.50	4.75	3.56	0.46
	Brazil	2.50	4.75	3.50	0.42
Masculinity vs. Femininity	Finland	1.50	4.25	2.76	0.48
	Brazil	2.00	4.00	3.01	0.39
Uncertainty Avoidance	Finland	1.25	3.75	2.42	0.49
	Brazil	1.25	3.75	2.59	0.47
Long vs. Short Term Orientation	Finland	2.00	4.00	2.88	0.44
	Brazil	1.75	4.25	3.04	0.42
Indulgence vs Restraint	Finland	2.25	4.25	3.37	0.42
	Brazil	2.50	4.25	3.27	0.38

7.2 Intention to use between groups

To test the effect of familiarity on intention to use, the respondents were divided into groups based on the fact whether they had or had not used biometrics before. In Finland, 57.6% and in Brazil 98.4% of respondents had used biometrics before. Independent samples t-test was run to examine the differences in intention to use between familiarity-groups. The independent samples t-test showed a statistically significant difference in the intention to use biometrics between respondents who had and had not used biometrics before. Those who had used biometrics before had a higher intention to use them in the future too, supporting H1. However, there was no significant effect in the Finnish or Brazilian samples when tested separately.

The respondents were also divided to groups based on whether they had or had not heard of biometrics before. In Finland 80% and in Brazil 97.6% reported to have heard about biometric technologies before. Independent samples t-tests were run to test the differences of intention to use between the formed groups. The independent samples t -test showed no statistically significant difference in the intention to use biometrics between respondents who had and had not heard about biometrics before. There was no significant effect in the Finnish or Brazilian samples when tested separately either.

In further analysis, the intention to use between country samples was compared. Overall, Brazil had a higher mean intention to use than Finland. An independent samples t-test showed a statistically significant difference between Finnish and Brazilian intention to use biometrics, Brazilians having a higher intention. The results from t-test related to intention to use biometrics between nationality-, familiarity- and knowledge-groups are presented in table 24.

TABLE 24 Results of t-tests measuring intention to use between familiarity, nationality and knowledge groups

	Familiarity with biometrics						
	Familiar (N = 195)		Not familiar (N = 55)				
	M	**SD**	**M**	**SD**	***t***	**df**	***p***
Intention to Use*	3.85	0.77	3.31	0.93	3.90	76.05	<0.001**

*Homogeneity of variance was observed by Levene's Test for Equality of Variances and thus a Welch's unequal variances t-test was used;**one-tailed sig.

	Familiarity with biometrics						
	Familiar (N (Fin) = 72) (N (Br) = 123)		Not familiar (N (Fin) = 53) (N (Br) = 2)				
	M	**SD**	**M**	**SD**	***t***	**df**	***p***
Intention to Use in Finland (Fin)*	3.51	0.78	3.30	0.95	1.35	99	0.090**
Intention to Use in Brazil (Br)*	4.04	0.70	3.63	0.53	0.84	123	0.202**

*Homogeneity of variance was observed by Levene's Test for Equality of Variances and thus a Welch's unequal variances t-test was used;**one-tailed sig.

	Nationality						
	Finnish (N = 125)		Brazilian (N = 125)				
	M	**SD**	**M**	**SD**	***t***	**df**	***p***
Intention to Use	3.42	0.86	4.03	0.70	-6.20	248	<0.001

	Knowledge of biometrics						
	Knowledge (N = 222)		No knowledge (N = 28)				
	M	**SD**	**M**	**SD**	***t***	**df**	***p***
Intention to Use	3.75	0.84	3.56	0.83	1.14	248	0.257

	Knowledge of biometrics						
	Knowledge (N (Fin) = 100) (N (Br) = 122)		No knowledge (N (Fin) = 25) (N (Br) = 3)				
	M	**SD**	**M**	**SD**	***t***	**df**	***p***
Intention to Use in Finland (Fin)	3.38	0.86	3.59	0.86	1.07	123	0.287
Intention to Use in Brazil (Br)	4.05	0.69	3.33	0.63	1.78	123	0.078

7.3 Results from testing TAM

An average score of each TAM-construct was calculated for each respondent to test the relationships of the constructs. The Brazilian averages included all the items analyzed in the CFA. The Finnish data on the other hand, was analyzed based on six security-questions and seven privacy-questions. This is not an issue in the TAM-analysis because the model and its applicability in the specific cultural context was tested and reported separately for both countries.

A series of multiple stepwise linear regressions and enter-method regressions were undertaken in IBM SPSS to analyze the model. The explanation of variance, regression coefficients, t-values, and significance levels for all the regressions analyses including only TAM-constructs in the separate country samples are presented in table 25.

A stepwise regression analysis was used to examine the effect of perceived usefulness, perceived ease of use and perceived physical invasiveness on intention to use. Perceived usefulness had a significant effect on intention to use in Finland ($\beta = 0.56$) and in Brazil ($\beta = 0.64$). H2a was therefore supported in both countries. A significant positive effect of perceived ease of use on intention to use was shown significant in Brazil ($\beta = 0.19$), but not in Finland, thus H2b being supported in Brazil, but not in Finland. The perceived physical invasiveness of biometrics also had a negative effect on the intention to use. The relationship was significant in Finland ($\beta = -0.38$) and in Brazil ($\beta = -0.14$), and thus H2c was supported in both countries.

The effect of perceived ease of use, perceived need for security and perceived need for privacy on perceived usefulness was examined via stepwise regression model. The perceived ease of use had a significant effect on the perceived usefulness in Finland ($\beta = 0.60$) and in Brazil ($\beta = 0.64$), supporting H3a in both countries. The hypothesized effect of perceived need for security on the perceived usefulness was found significant in Brazil ($\beta = 0.34$), but the relationship was excluded from the model in the Finnish data. H3b was thus supported in Brazil, but not in Finland. A significant negative effect of perceived need for privacy on perceived usefulness was found in Finland ($\beta = -0.17$) and in Brazil ($\beta = -0.14$), H3c not being supported in either of the countries.

An enter-method regression analysis showed physical invasiveness to have a significant negative effect on the perceived ease of use in Finland ($\beta = -0.47$) and in Brazil ($\beta = -0.40$). H4 was therefore supported in both countries.

When tested for the effect of perceived need for privacy and perceived need for security on perceived physical invasiveness of biometrics, the stepwise regression model showed perceived need for security to influence the perceived physical invasiveness negatively and significantly in Finland ($\beta = -0.34$), but the construct was excluded from the model in Brazilian data. Therefore, H5a was supported in Finland, but not in Brazil. Perceived need for privacy had a significant positive effect on perceived physical invasiveness in Finland ($\beta = 0.66$), but

also this construct was excluded from the model in Brazilian data. Again, H5b was supported in Finland, but not in Brazil.

Finally, an enter-method regression showed a significant positive effect of perceived need for privacy on perceived need for security in Finland (β = 0.65) and in Brazil (β = 0.39), supporting H6 in both countries.

TABLE 25 Regression analysis results for TAM

Country	Dependent Variable	Significant Independent Variables	Std. β	Sig.
Brazil	Intention to Use	Usefulness	0.64	<0.001
	R^2 = 0.748; F = 119.82, p < .001	Ease of Use	0.19	0.004
		Invasiveness	-0.14	0.008
Finland	Intention to Use	Usefulness	0.56	<0.001
	R^2 = 0.716; F = 153.81, p < .001	Invasiveness	-0.38	<0.001
Brazil	Usefulness	Ease of Use	0.64	<0.001
	R^2 = 0.597; F = 59.83, p < .001	Security	0.34	<0.001
		Privacy	-0.14	0.033
Finland	Usefulness	Ease of Use	0.56	<0.001
	R^2 = 0.394; F = 39.74, p < .001	Privacy	-0.17	0.025
Brazil	Ease of Use			
	R^2 = 0.163; F = 34.06, p < .001	Invasiveness	-0.40	<0.001
Finland	Ease of Use			
	R^2 = 0.217; F = 34.06, p < .001	Invasiveness	-0.47	<0.001
Brazil	Security			
	R2 = 0.152; F = 22.03, p < .001	Privacy	0.39	<0.001
Finland	Security			
	R^2 = 0.420; F = 89.05, p < .001	Privacy	0.65	<0.001
Finland	Invasiveness	Security	-0.34	0.001
	R^2 = 0.262; F = 21.64, p < .001	Privacy	0.66	<0.001

7.4 Results from testing Hofstede's dimensions

The cultural dimension scores were calculated based on the weighted equations provided by Hofstede (2013). According to Hofstede (2011), Brazil should score higher than Finland on Power Distance, Masculinity, Uncertainty Avoidance and Long Term Orientation, Finland should score higher than Brazil on Individualism and Indulgence should be close to the same score in both countries. Independent samples t-tests were run to see, if there were significant differences in the scores for Hofstede's dimensions between countries. The results from t-test considering the differences in cultural dimension scores between the nationalities are presented in table 26. A statistically significant difference in dimension scores between Brazil and Finland was found for MAS, UAI and LTO. Brazil scored higher than Finland on all these three dimensions.

All the regression analyses performed in the previous chapter were repeated in SPSS as stepwise models, including also each of the cultural constructs. The explanation of variance, regression coefficients, t-values, and significance levels for all the significant stepwise models including Hofstede's dimensions in the total sample are presented in table 27. When entered into a stepwise regression model together with ease of use, usefulness and invasiveness, all the cultural dimensions (including IDV, PDI and MAS) were excluded from the model and thus H7a, H7b and H7c were not directly supported.

Some relationships between the cultural dimensions and TAM-constructs were however found. A stepwise regression testing the influence of perceived need for privacy and Hofstede's dimensions on perceived need for security found Individualism vs. Collectivism to have a significant negative effect (β = -0.14) on perceived need for security. Lower perceived need for security contributed to lower perceived usefulness in Brazil and higher perceived invasiveness in Finland, contributing further on to lower intention to use. H7a was therefore partially supported. Other cultural constructs were excluded from the model. All the hypotheses and their support are presented in table 28.

A stepwise regression testing the effect of perceived need for privacy, perceived need for security, perceived ease of use and Hofstede's dimensions on perceived usefulness, together with the TAM-constructs showed a significant positive effect (β = 0.11) of Uncertainty Avoidance on the perceived usefulness and a significant negative effect (β = -0.11) of Power Distance on perceived usefulness. As perceived usefulness was found to have a positive effect on intention to use, power distance had an indirect negative relationship with intention to use, further opposing H7b. Other cultural constructs were excluded from the stepwise model.

A stepwise regression testing the effect of perceived physical invasiveness and Hofstede's dimensions on perceived ease of use showed a significant negative effect (β = -0.16) of Uncertainty Avoidance on perceived ease of use. Other cultural constructs were excluded in the stepwise analysis.

When tested for effect of perceived need for privacy, perceived need for security and Hofstede´s dimensions on perceived physical invasiveness with a stepwise regression, only the relationships between Perceived Need for Privacy and Perceived Physical Invasiveness, and Perceived Need for Security and Perceived Physical Invasiveness were found. All the cultural constructs were excluded from the model.

In further analysis, when the same tests were run with regular averages from the questionnaire items of each dimension, without Hofstede's (2013) dimension specific equations, only a significant negative effect of Individualism versus Collectivism on perceived need for security (β = -0.14) and a barely significant positive effect of Long versus Short Term Orientation on perceived need for privacy (β = 0.13) emerged.

TABLE 26 Results of t-tests measuring Hofstede's cultural dimension scores between Finland and Brazil

	Nationality						
	Finnish (N = 125)		Brazilian (N = 125)				
	M	SD	M	SD	*t*	df	*p*
Power Distance	3.17	0.41	3.26	0.42	-1.76	248	0.080
Individualism vs. Collectivism	3.56	0.46	3.50	0.42	1.07	248	0.285
Masculinity vs. Femininity*	2.76	0.48	3.01	0.39	-4.60	239.34	<0.001
Uncertainty Avoidance	2.42	0.49	2.59	0.47	-2.87	248	0.005
Long vs. Short Term Orientation	2.88	0.44	3.04	0.42	-2.93	248	0.004
Indulgence vs. Restraint	3.37	0.42	3.27	0.38	1.94	248	0.054

*Homogeneity of variance was observed by Levene's Test for Equality of Variances and thus a Welch's unequal variances t-test was used

TABLE 27 Stepwise regression analysis models including Hofstede´s dimensions

Dependent Variable	Significant Independent Variables	Std. β	Sig.
Usefulness			
$R^2 = 0.534$; $F = 56.03$, $p < .001$	Ease of Use	0.62	<0.001
	Privacy	-0.27	<0.001
	Security	0.263	<0.001
	Uncertainty Avoidance	0.11	0.012
	Power Distance	-0.11	0.018
Ease of Use			
$R^2 = 0.219$; $F = 34.67$, $p < .001$	Invasiveness	-0.45	<0.001
	Uncertainty Avoidance	-0.16	0.006
Security			
$R^2 = 0.261$; $F = 43.60$, $p < .001$	Privacy	0.49	<0.001
	Individualism vs. Collectivism	-0.14	0.014
Security*			
$R^2 = 0.261$; $F = 43.60$, $p < .001$	Privacy	0.49	<0.001
	Individualism vs. Collectivism	-0.14	0.014
Privacy*			
$R^2 = 0.016$; $F = 4.00$, $p = .047$	Long Term Orientation	0.13	0.047

*Calculated with regular averages instead of Hofstede´s (2013) weighed equations

TABLE 28 The hypotheses and their support in Finland and in Brazil

Hypothesis	**Supported**
H1: The users who are already familiar with biometrics will have a higher intention to use the technology.	Yes
H2a: The perceived usefulness of the security technology will have a significant positive effect on an individual's intention to use the technology.	Yes
H2b: The perceived ease of use of the security technology will have a significant positive effect on an individual's intention to use the technology.	Only in Brazil
H2c: The perceived physical invasiveness of the security technology will have a significant negative effect on an individual's intention to use the technology.	Yes
H3a: The perceived ease of use of the security technology will have a significant positive effect on the perceived usefulness of the technology.	Yes
H3b: An individual's desire for the security of their person and his/her personal information will have a significant positive effect on the perceived usefulness of the technology.	Only in Brazil
H3c: An individual's perceived need for privacy will have a significant positive effect on the perceived usefulness of the technology.	No
H4: The perceived physical invasiveness of the security technology will have a significant negative effect on the perceived ease of use of the technology.	Yes
H5a: An individual's desire for the security of their person and his/her personal information will have a significant negative effect on the perceived physical invasiveness of the technology.	Only in Finland
H5b: An individual's desire for privacy will have a significant positive effect on the perceived physical invasiveness of the technology.	Only in Finland
H6: An individual's perceived need for privacy will have a significant positive effect on his/her need for security.	Yes
H7a: Individualism versus Collectivism score will have a significant negative effect on the intention to use biometrics.	Partially
H7b: Power Distance score will have a significant positive effect on the intention to use biometrics.	No
H7c: Masculinity versus Femininity score will have significant positive effect on the intention to use biometrics.	No

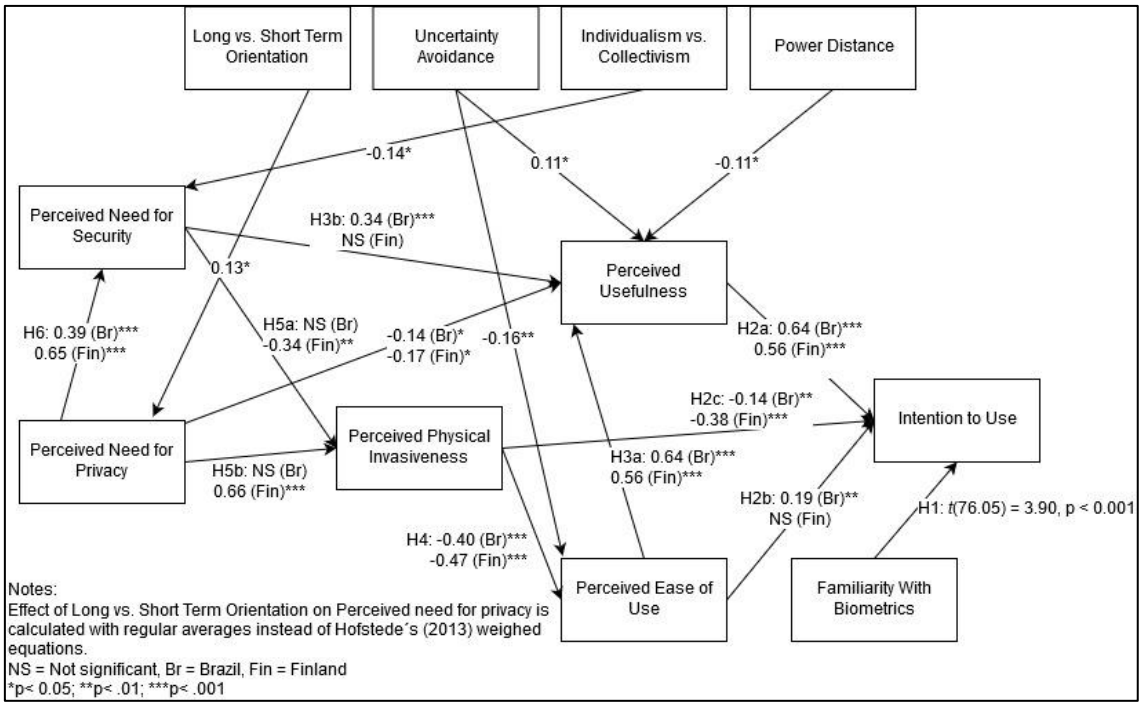

FIGURE 3 Supported results from testing the research model

8 DISCUSSION

The objective of this chapter is to discuss the applicability of the biometrics-specific Technology Acceptance Model on our samples, the differences between acceptance formation in Finland and Brazil and the impact of Hofstede's cultural dimensions on the model relationships. The relationships that emerged in the data analysis are compared to previous studies and the implications of results for both theory and practice are presented. Finally, the chapter also discusses the limitations of the study and suggests directions for future research.

8.1 Acceptance of biometrics

This research wished to firstly respond, whether there is a difference in familiarity and knowledge of biometrics between Brazil and Finland. In addition to higher intention to use, the higher familiarity and knowledge of biometrics in Brazil were expected results, since Brazil was shown in the literature review to be the leader of South American biometrics markets, and South America in general to be a pioneering area in the use of various biometrics applications (Hannah, 2005; IriTech, inc., 2015; International IDEA, 2017; Onin.com, 2017). Finnish respondents knew about and had used biometrics less than their Brazilian counterparts. The familiarity with biometrics in Brazil seems to be higher than what most of earlier literature considering European, North American, African and Asian countries report (e.g. Biosec, 2005; Moody, 2004; Riley et al., 2009). The response to the first research question therefore is: yes, there is a difference in familiarity and knowledge of biometrics between Finland and Brazil.

The second research question asked, how the acceptance of biometrics is formed in Brazil and in Finland. The effect of earlier use of biometrics on acceptance was examined to understand the acceptance formation better. The results in total sample suggest that the users who have previously used biometrics, and thus are familiar with biometrics, have a greater intention to use them in the future. This is in line with earlier literature that suggests familiarity to

influence acceptance (e.g. Brockly et al., 2014; Krol et al., 2016). The results might however be biased by cultural or other country-specific factors, since the results from testing the countries separately suggested that an individual's choice of using a biometrics is not different between those who have used some biometric technology before and those who have not. Therefore, one should take caution when making conclusions on technology acceptance based solely on self-reported anterior use or intention to use. Between those who had and had not heard of biometrics before, the results suggested no significant differences of intention to use in the total sample and neither in separate country samples. Therefore, whether the respondents already had knowledge of biometrics or not, had no difference on their intention to use biometrics. All in all, intention to use biometrics does not seem to differ between the knowledge groups, and the difference of intention between familiarity-groups emerges only when disregarding nationality in the analysis.

Further on, a Technology Acceptance Model was used to inspect the acceptance formation. Some of the relationships that were found between technology acceptance constructs in statistical testing followed the findings by James et al. (2006) both in Finland and in Brazil. They explain these results as follows: An individual is more likely to use a biometric technology, if they find the device useful in a particular situation and less likely if they perceive the biometric as more invasive. The ease of a device's use affects significantly, whether the device is perceived as useful. When the biometric technology is perceived more invasive, it will be seen as less easy to use. Finally, an individual who has a high perceived need for privacy, will also have a high perceived need for security.

Some relationships followed the original model in only one of the countries. Based on James et al.´s (2006) explanations, a technology is viewed as less invasive in Finland, when the user feels more need for their security and that the higher level of privacy that a Finnish individual thinks they require, the more invasive the biometric device is perceived. James et al. (2006) explain, that biometric devices may be seen to invade one's privacy due to the physical nature of their use. Therefore, Finnish people might see biometric technologies as an invasion to their privacy, while the Brazilian subjects might be less worried about involving their body in the authentication process. Neither the need for personal security seems to affect the perceptions of invasiveness among Brazilian users, which is understandable if they do not see biometrics as physically invasive to begin with. These result suggest that Brazil differs from many countries in Europe, North America, Africa and Asia, where fears of physical health issues have been found to be major barriers for the use of biometrics (e.g. Alhussain & Drew, 2009; Furnell & Evangelatos, 2007; Moody, 2004; Riley et al., 2009).

According to the relationships that emerged only in the Brazilian data, an individual who feels that a device is easy to use, is more likely to actually use it and an individual's perceived need for security will positively affect how useful they feel the biometric device will be (James et al., 2006). In Finland, however, biometrics might not be seen as a useful way of increasing one's personal security

and while ease of use might be a driver for the willingness of an individual to use biometric devices in Brazil (and in the United States according to James et al. (2006)), the Finnish subjects might not see ease of use as a strong enough factor to affect their use decision. However, the perceived ease of use was found to positively affect perceived usefulness in both countries, showing an indirect impact of perceived ease of use on the intention to use biometric devices also in Finland.

Finally, James et al. (2006) hypothesized a positive effect of an individual's perceived need for privacy on the perceived usefulness of the technology. The hypothesis was not supported in their study, and they only found an indirect relationship through perceived need for security. In the present study, the higher an individual in either country perceived their needed level of privacy, the less useful they found the biometric technology. This result is contradictory both with James et al.'s (2006) hypothesized model and their actual results. The Finnish and Brazilian users might not believe biometric technologies to be a useful way of protecting their privacy, or they might even see the use of biometric authentication as negatively affecting their privacy.

All in all, the extended TAM by James et al. (2006) was supported in this study by most parts. The answer to the second research question is for Finland´s part that the acceptance follows James et al.´s (2006) model, except for 1) the positive effect of perceived ease of use on intention to use, 2) the positive effect of perceived need for security on perceived usefulness and 3) the positive effect of perceived need for privacy on perceived usefulness. For Brazil, acceptance followed the model except for 1) the positive effect of perceived need for privacy on perceived usefulness, 2) the negative effect of perceived need for security on perceived physical invasiveness and 3) the positive effect of perceived need for privacy on perceived physical invasiveness. Familiarity with biometrics might also affect the intention to use biometrics between the countries. Since all the hypothesized relationships were not supported in neither Brazil nor Finland, James et al.´s (2006) model might not work completely as intended when taken from the United States to other countries. There might be differences, cultural or other, in the applicability.

8.2 Impact of Hofstede's dimensions

The third and final research question was set to discover, whether there are cultural differences in the acceptance of biometrics between Brazil and Finland. Like most of the earlier cross-cultural technology acceptance studies, the present study utilized Hofstede´s cultural dimension theory to search for such differences. Even though Riley (2009) and Al-Harby (2010) suggest that Hofstede's dimensions do not explain differences in the acceptance of biometrics, they did not study the effects of the dimensions in relation to the TAM-constructs. They also did not study the individual level effects of espoused national cultural values as demonstrated by Srite & Karahanna (2006).

The results suggest that an individual, who has espoused more individualist cultural values, will feel less need for his or her personal security. This could further mean that in individualist cultures, citizens generally feel less need for security of their physical being. The finding of an indirect negative relationship with intention to use is in line with Riley et al. (2009) and Al-Harby (2010), but contradictory with previous research considering Hofstede's dimensions and technology acceptance in general. The explanation by Erumban and Jong (2006), that in collectivist societies people are less willing to adopt new technologies that are not used by their peers, might not apply to biometrics, which in some countries, including Brazil, is required to be used by law in applications such as national ID's, driving licenses, passports and election voting (IriTech, inc., 2015). However, it needs to be remembered that the effect of Individualism versus Collectivism on intention to use biometrics was only an indirect relationship through perceived need for security, usefulness and invasiveness.

Those who have espoused more power distance allowing cultural values, perceived biometrics as less useful. The results mean that in cultures which accept larger differences of power, biometrics might be seen as a less useful technology. The findings related to Power Distance were more in line with the previous findings of non-biometric cultural technology acceptance literature, than with the findings of Riley et al. (2009) and Al-Harby (2010). Al-Gahtani (2002) and Van Everdingen and Waarts (2004) have explained the negative relationship between power distance and technology acceptance by high power distance societies having centralized decision-making structures, which negatively affect technology adoption. However, power distance was only related to the perceived usefulness of the technology and therefore only indirectly to the intention to use biometrics, and thus this explanation does not necessarily hold. In the other hand, it is possible that in cultures of high Power Distance, a new technology such as biometric authentication is not seen as a useful alternative to the traditional authentication technologies because centralized decision-making structures considering technology use have already been established.

Within our sample, individuals who have espoused more uncertainty avoiding cultural values were more likely to perceive biometric devices as hard to use, but useful. This could be a sign, that while seeing biometrics as a useful technology, uncertainty avoiding cultures prefer to keep on using traditional authentication schemes and are less willing to change into less known methods, which would require practice to use. Uncertainty Avoidance did not have effect on technology acceptance on Riley et al.'s (2009) study but did in earlier non-biometrics technology acceptance research. The negative relationship between Uncertainty Avoidance and technology acceptance has been argued to be a possible consequence of people being less willing to be involved with the "unknown territories" of new technologies (Erumban & Jong, 2006; Van Everdingen & Waarts, 2004). This explanation is possibly applicable to the finding of the present study. Uncertainty Avoidance, however, was also positively related to perceived usefulness, and therefore indirectly to intention to use.

The positive effect of espoused values of Long Term Orientation on perceived need for privacy was found when calculating regular averages for the dimension constructs instead of using Hofstede's equations for dimension calculation. This relationship could mean that people in long-term oriented cultures generally think that they need a higher level of privacy. As a higher perceived need for privacy contributes to the perceived usefulness of biometric devices, and therefore indirectly to the intention to use biometrics, Long vs. Short Term Orientation might play a part in the formation of the acceptance of biometrics.

The findings indicate that Hofstede's dimensions do not provide a clear explanation for the differences found in the biometrics acceptance between Finland and Brazil. The answer to the third research question therefore is, that cultural differences can explain only a small part of differences in biometrics acceptance between the countries, but there are some cultural differences. Riley et al. (2009) saw their results interpreting two possible explanations. Firstly, it is possible that the theories considering the relationship between culture and technology acceptance might be overstated or that the previously presented theories about the relationship of cultural differences and technology acceptance might not apply to biometrics due to it being a special or unique type of technology. They however remind that almost any technology has specific contextual or historical issues that have an effect on its perception in different cultures and communities. They therefore believed a more plausible explanation to be, that specific contextual factors of the different countries, such as media attention of biometrics and crime rates, and differences in the underlying familiarity with biometrics provide a better explanation for the difference in attitudes between the observed countries. The effect of familiarity was examined in the current study, but the other specific contextual factors might have influenced the results too.

8.3 Research contributions and implications for practice

The results of the study offer numerous contributions for research. Firstly, the study tested the replicability of James et al.'s (2006) Technology Acceptance Model in new cultural contexts in Finland and Brazil. This will give insights about whether and with what modifications the model should be taken into further cultural and geographical areas. Secondly, such insights can also be gained regarding the applicability of a model combining the biometrics-TAM and Hofstede's cultural dimensions for cross-cultural research purposes. In relation, another contribution was the translation of the James et al.'s (2006) Technology Acceptance Model questionnaire into Finnish and Portuguese, and the VSM13-survey into Finnish.

Further on, the study was a first of its kind to address the acceptance of biometric technologies in Brazil and in the whole South America. The research therefore contributed to the existing knowledge of cross-cultural technology acceptance and biometrics acceptance by highlighting differences in the levels of biometrics acceptance, the ways how the acceptance of biometric technologies of

Finnish and Brazilian citizens is formed, and what cultural dimensions might play part in the attitude formation. In addition, it revealed differences in the ways how security and privacy needs differ between the citizens of the countries, and how these differences are related to attitudes towards biometrics. The results can help to direction future research efforts into the right areas and constructs of biometric technology acceptance, in order to effectively measure the differences in acceptance and the reasons leading to them in Finland, Brazil and other countries.

There were also some practical implications. Firstly, the results can be applied by organizations and businesses interested in developing and distributing products with biometric features for the Finnish and Brazilian markets. The discovered levels of biometrics acceptance and the factors affecting the acceptance can aid in the decisions about including certain biometrics-enhanced products in the studied areas. Also, the findings of this research could contribute to planning the advertising, marketing, instructions, support and other communication required when introducing a biometric product to a new market. Finally, the findings point out the problematic areas, such as privacy and security issues in Finland, and can contribute to the improvement of the total acceptance of biometrics in the country. The results from Brazil on the other hand can help biometrics actors to repeat elsewhere the actions that might have positively affected the acceptance of biometrics in the country.

8.4 Limitations and directions for future research

The study had some limitations, which should be taken into account when analyzing the results and conducting further related research. Despite the critique towards utilizing population consisting of students, using a student sample is a common practice in academic research (Carlos Martins Rodrigues Pinho & Soares, 2011). However, a university student sample does not represent the whole population of Brazil and Finland. The use of students can be considered a convenience sampling method, because the easily acquirable sample was partially chosen because of the limited time and financial resources (Kothari, 2009, pp. 15). According to Kothari (2009, pp. 15), using convenience sampling may give very biased results, especially when the population is not homogenous. The university student sample used in this study can therefore be considered a limitation. Future research should present the questionnaire to a more diverse sample in Finland and Brazil to better generalize the results to the whole populations.

Caution should be taken in the interpretation of results including the TAM-constructs in Brazil, since the model fit, reliability and validity could not be shown for the model, indicating another limitation. However, this limitation seems to stem from differences in the privacy-related phenomena. The fact that there were differences in the privacy-related items and constructs both in the CFA and the regression analysis, would indicate cultural differences in privacy perceptions, and the influence of such differences on the acceptance of biometrics to be interesting points to study in further research.

Caution should also be taken in the analysis of the impact of Hofstede's dimensions on the TAM-constructs. Some tests were run on the whole datasets at once with Perceived Need for Security and Perceived Need for Privacy as inspected variables. The Finnish data includes less items for these constructs than the Brazilian data, and thus the same constructs measure partially different privacy- and security-issues in the two countries. Also, order of Brazil´s and Finland´s dimension scores did not follow Hofstede´s (2011) observations for all the dimensions, suggesting that his theory is not fully applicable to our sample. Further on, no reliability or validity could be shown for the cultural constructs. The results considering the impact of Hofstede's cultural dimensions should therefore be generally interpreted with caution. The low reliability was however expected, as the VSM13 was developed to measure country-level effects and the individual-level correlations of the items may differ a lot from the country-level. Even though Srite & Karahanna (2006) argue that the Hofstede's cultural dimensions can be considered as individual-level espoused cultural values, Hofstede (2013) advises against using the dimensions for an individual level analysis, making this approach a limitation to the study.

Nonetheless, there are clearly some statistically significant relationships between the individual dimension scores and the TAM-constructs, but since the Hofstede's dimensions and the VSM 2013 were not created for analysis between individuals, future research should collect data from more countries in order to see if such results emerge also on country-level. This way the reliability of the dimension constructs could also be calculated as intended on a country level. However, as other reports suggest (e.g. Spector et al., 2001), not even country-level analysis might support the reliability and validity of the VSM-items. A researcher wanting to establish reliability and validity while using cultural dimension constructs might therefore want to consider other options of cultural dimension frameworks in future works.

The results may also have been affected by errors in translation. A more rigorous translation process should be created in future research to make sure that the questionnaire items ask exactly the same thing in all of the studied countries. Focus groups should be created in order to qualitatively assess the questionnaire items, constructs and translations. Another option is to hire a professional translator to verify the correctness of the translated items based on back translations.

Another interesting idea for future research would be to measure how the different types of biometric technologies, personal and organizational contexts, forced and voluntary use, and other characteristics presented in the vignettes affect the perceptions between countries and cultures. Even though the vignettes featured various biometric technologies and use situations in the present study, the model was not designed to measure the differences between them, but rather to create a generalizable measure of biometrics acceptance independent of context. Thus, the differences of responses between vignettes were not tested in the present study.

Finally, instead of or in addition to cultural differences, other contextual, historical, situational, political, legislative, social etc. differences might have affected the differences in the perceptions of biometrics between the Finnish and Brazilian respondents and should be studied in further research. To evaluate better the underlying reasons in the differences of biometrics acceptance, a qualitative assessment, such as an interview approach would be truly helpful in taking cross-regional user-centered biometrics research forward. This would also help to dig deeper into the underlying reasons, that affect the regional differences that emerged in this study, such as perceptions of privacy and security, and the relationship of privacy and security needs, biometrics and their physical invasiveness between countries.

9 CONCLUSION

Biometric technologies can improve usability and security of authentication but are prone to new types of problems. Biometrics differ from traditional authentication technologies, because they involve the human body in the user authentication process. User acceptance can be a problem for widescale adoption of biometrics, and the acceptance often differs between geographical areas. Most of the user-centered biometrics research has been done in European and North American contexts, and the study of attitudes towards biometric technologies in general is low. No earlier research has examined the acceptance of biometric technologies in South America, despite the continent being a pioneering area of biometrics markets.

Previous research has found the acceptance of biometrics to differ a lot between, and even within studied regions. Some cross-cultural research exists, but most studies have examined the acceptance of biometrics within only one cultural area, making it less reliable to compare the results between studies. Many barriers and issues in the adoption of biometrics have also been reported, but neither they can be conveniently compared between geographical areas only by the means of a literature review. To resolve these problems, more cross-cultural studies should be conducted, especially outside Europe.

Because the present study took the first step into measuring acceptance of biometrics in South America, the most popular models were picked from literature to make the results as comparable with previous studies as possible. An online survey was employed in Finland and in the leader of South American biometrics markets, Brazil, in their local languages. The survey utilized the extended Technology Acceptance Model of James et al. (2006) to examine the ways how biometrics acceptance is formed in the countries, and Hofstede's theory of cultural dimensions to discover possible cultural differences affecting the acceptance. In addition, the users were asked about their knowledge of and their familiarity with biometrics.

The intention to use, familiarity and knowledge of biometrics were higher in Brazil than in Finland. Familiarity was shown to positively influence intention to use in the total sample, but not in Finland nor Brazil when examined separately.

Most of the TAM-relationships found by James et al. (2006) were supported in at least one of the studied countries, but neither country followed the model completely. In Brazil, an individual´s perceived need for security influenced positively the perceived usefulness of biometrics and higher ease of use of biometrics led to a higher intention to use, while the Finnish respondents did not see biometrics to increase their personal security nor had their intention to use biometrics increased due to ease of use. The results showed Finnish people to see biometrics as an invasion to their privacy, as opposed to the Brazilian respondents. In Finland, biometrics were however seen as less invasive when the user felt more need for their personal security, while there was no such effect among Brazilians. In addition, biometrics were not seen as a useful way of protecting one´s privacy in neither country, as opposed to the original model.

Considering the cultural differences, one´s more individualistic cultural values seemed to cause less need for their personal security, thus indirectly leading to lower intention to use biometrics. Also, the acceptance of larger power distances in society seemed to be related to perceiving biometrics as less useful and therefore to lower intention to use biometrics. Those with more uncertainty avoiding values, on the other hand, perceived biometrics as harder to use, but more useful. Finally, some results suggested those with espoused values of Long Term Orientation to require a higher level of personal privacy, leading to higher perceived usefulness of biometrics, and thus possibly to higher intention to use.

Main limitations of the present study were the use of a university student population, lack of model fit, reliability and validity of the Technology Acceptance Model in Brazil and the use of individual-level analysis of Hofstede´s cultural dimension theory. In addition to using a more diverse population from a greater number of countries, future research should examine more closely the differences that emerged in the present study and their underlying causes by utilizing frameworks that in addition to culture, consider the specific contextual and situational reasons that affect technology acceptance in the studied countries.

In conclusion, the present study tested the applicability of a unified model of James et al.´s (2006) biometrics-TAM and Hofstede´s cultural dimension theory in Finland and in Brazil, being the first study to examine the acceptance of biometrics in South America. The results pointed out differences in the intention to use, familiarity and knowledge of biometrics between Finland and Brazil, and clarified the process of biometrics acceptance formation in the countries. The results can assist future research to decide whether, where and with what modifications to utilize these two models in other cultural and geographical areas. Future research can also examine further the differences that emerged between Brazil and Finland in this study, such as security and privacy needs and their relation to the acceptance of biometrics. Businesses and organizations can apply the findings in decision-making about introducing biometric products in Brazil and Finland and in planning the communication regarding such decisions.

REFERENCES

Aboelmaged, M. G., & Gebba, T. R. (2013). Mobile Banking Adoption : An Examination of Technology Acceptance Model and Theory of Planned Behavior. *International Journal of Business Research and Development*, *2*(1), 35–50.

AbuShanab, E., & Pearson, J. M. (2007). Internet banking in Jordan. *Journal of Systems and Information Technology*, *9*(1), 78–97.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 41-46.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39). Springer, Berlin, Heidelberg.

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211.

Akinnuwesi, B. A., Uzoka, F. M. E., Okwundu, O. S., & Fashoto, G. (2016). Exploring biometric technology adoption in a developing country context using the modified UTAUT. *International Journal of Business Information Systems*, *23*(4), 482.

Al-Adwan, a, Adwan, A. A.-, & Smedley, J. (2013). Exploring students acceptance of e-learning using technology acceptance model in jordanian universities. *International Journal of Education and Development Using Information and Communication Technology*, *9*(2), 4–18. Retrieved from http://ijedict.dec.uwi.edu/viewarticle.php?id=1617

Al-Alem, F., Alsmirat, M. A., & Al-Ayyoub, M. (2017). On the road to the Internet of Biometric Things: A survey of fingerprint acquisition technologies and fingerprint databases. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, (20150348), 0–5.

Al-Gahtani, S. S. (2002). Extending the technology acceptance model beyond its country of origin: a cultural test in Western Europe. In *Advanced Topics in Information Resources Management, Volume 1* (pp. 158-183). IGI Global.

Al-Gahtani, S. S., Hubona, G. S., & Wang, J. (2007). Information technology (IT) in Saudi Arabia: Culture and the acceptance and use of IT. *Information and Management*, *44*(8), 681–691.

Al-Harby, F. M. (2010). BIOMETRIC AUTHENTICATION SYSTEMS FOR SECURED E-TRANSACTIONS IN SAUDI ARABIA. University of Bradford.

Al-Harby, F., Qahwaji, R., & Kamala, M. (2009). The effects of gender differences in the acceptance of biometrics authentication systems within online transaction. *2009 International Conference on CyberWorlds, CW '09*, 203–210.

Alhussain, T., & Drew, S. (2009). Towards User Acceptance of Biometric Technology in E-Government: A Survey Study in the Kingdom of Saudi Arabia. *IFIP Advances in Information and Communication Technology*, *305*, 26–38.

Aly, S., & Hassaballah, M. (2015). Face recognition: challenges, achievements and future directions. *IET Computer Vision*, *9*(4), 614–626.

Amoako-Gyampah, K., & Salam, A. F. (2004). An extension of the technology acceptance model in an ERP implementation environment. *Information and Management*, *41*(6), 731–745.

Anandarajan, M., Igbaria, M., & Anakwe, U. P. (2002). IT acceptance in a less-developed country: A motivational factor perspective. *International Journal of Information Management*, *22*(1), 47–65.

Ap Rasiah, D., & Yen, Y. Y. (2016). User Acceptance of Biometric Authentication in Malaysian ATMs. *International Business Management*, *10*(16), 3607-3610.

Arevalo, J., Mola-Yudego, B., Pelkonen, P., & Qu, M. (2012). Students' views on forestry education: A cross-national comparison across three universities in Brazil, China and Finland. *Forest Policy and Economics*, *25*, 123–131.

Asmah, A. E., Ofoeda, J., & Gyapong, K. (2016). Factors that affect banks??? acceptance of electronic cheque clearing system: Evidence from Ghana. *Journal of Internet Banking and Commerce*, *21*(2).

Assadi, V., Hassanein, K., Breward, M., & Head, M. (2009). Consumer acceptance of biometrics for identity verification in financial transactions. *ECIS 2009 Proceedings*, Paper 294.

Avgerou, C., Ganzaroli, A., Poulymenakou, A., & Reinhard, N. (2009). Interpreting the trustworthiness of government mediated by information and communication technology: Lessons from electronic voting in Brazil. *Information Technology for Development*, *15*(2), 133–148.

Barki, H., & Hartwick, J. (1994). Measuring User Participation, User Involvement, and User Attitude. *MIS Quarterly*, *18*(1), 59.

Bergadano, F., Gunetti, D., & Picardi, C. (2002). User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*, *5*(4), 367–397.

Bethell, L. (2010). Brazil and 'Latin America'. *Journal of Latin American Studies*, *42*(3), 457-485.

Bharadwaj, S., Vatsa, M., & Singh, R. (2014). Biometric quality: a review of fingerprint, iris, and face. *Eurasip Journal on Image and Video Processing*, *2014*(1), 1–28.

Bhosale, S. T., & Sawant, B. S. (2012). S Ecurity I N E-B Anking Via Card Less Biometric Atms, *2*(4), 9–12.

Biosec, E. (2005). User acceptance: The BioSec approach. *Biometric Technology Today*, *13*(7), 8–10.

Blue Bell PA (2008). Unisys Study: Consumers Overwhelming Trust Biometrics to Protect Data, & Americans concerned about ID theft.

Bouwman, H., Carlsson, C., Walden, P., & Molina-Castillo, F. J. (2008). Trends in mobile services in Finland 2004-2006: From ringtones to mobile internet. *Info*, *10*(2), 75–93.

Bowyer, K. W., & Doyle, J. S. (2014). Cosmetic contact lenses and iris recognition spoofing. *Computer*, *47*(5), 96–98.

Braz, C., & Robert, J. (2006). Security and Usability : The Case of the User Authentication Methods. *Proceedings of the 18th International Conference of the Association - IHM '06*, 199–203.

Breward, M., Hassanein, K., & Head, M. (2017). Understanding consumers' attitudes toward controversial information technologies: A contextualization approach. *Information Systems Research*, *28*(4), 760-774.

Brockly, M., Elliott, S., Burdine, J., Frost, M., Riedle, M., & Guest, R. (2014, October). An investigation into biometric signature capture device performance and user acceptance. In *2014 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-5). IEEE.

Brosnan, M., & Lee, W. (1998). A Cross-Cultural Comparison of Gender Differences in Computer Attitudes and Anxieties: The United Kingdom and Hong Kong. *Computers in Human Behavior*, *14*(4), 559–577.

Brown, S. A., Dennis, A. R., & Venkatesh, V. (2010). Predicting Collaboration Technology Use: Integrating Technology Adoption and Collaboration Research. *Journal of Management Information Systems*, *27*(2), 9–54.

Buciu, I., & Gacsadi, A. (2016). Biometrics systems and technologies: A survey. *International Journal of Computers, Communications and Control*, *11*(3), 315–330.

Caldwell, T. (2014). 2014 – a Year in Biometrics. *Biometric Technology Today*, *2014*(11), 9–11.

Carlos Martins Rodrigues Pinho, J., & Soares, A. M. (2011). Examining the technology acceptance model in the adoption of social networks. *Journal of Research in Interactive Marketing*, *5*(2/3), 116–129.

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2018). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers*, *20*(1), 91-110.

Castiglione, A., Choo, K. K. R., Nappi, M., & Narducci, F. (2017). Biometrics in the Cloud: Challenges and Research Opportunities. *IEEE Cloud Computing*, *4*(4), 12–17.

Chabbra, N., & Dutta, R. (2016). Low Quality Iris Detection in Smart Phone : A Survey. *International Journal of Computer Science and Mobile Computing*, *5*(4), 271–276.

Chauhan, J., Hu, Y., Seneviratne, S., Misra, A., Seneviratne, A., & Lee, Y. (2017). BreathPrint. *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '17*, 278–291.

Chen, L. da, Gillenson, M. L., & Sherrell, D. L. (2002). Enticing online consumers: An extended technology acceptance perspective. *Information and Management*, *39*(8), 705–719.

Chiang, F. (2005). A critical examination of Hofstede's thesis and its application to international reward management. *International Journal of Human Resource Management*, *16*(9), 1545–1563.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, *295*(2), 295-336.

Chitungo, S., & Munongo, S. (2013). Extending the Technology Acceptance Model to Mobile Banking Adoption in Rural Zimbabwe. *Journal of Business Administration and Education*, *3*(1), 51–79.

Chung, J. E., Park, N., Wang, H., Fulk, J., & Mclaughlin, M. (2010). Age differences in perceptions of online community participation among non-

users: An extension of the Technology Acceptance Model. *Computers in Human Behavior*, *26*(6), 1674–1684.

Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins , Developments and Future Directions. *Sprouts: Working Papers on Information Systems*, *9*(2009), 1–23.

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones - A survey of attitudes and practices. *Computers and Security*, *24*(7), 519–527.

Clarke, R. (1994). *Human Identification in Information Systems: Management Challenges and Public Policy Issues*. *Information Technology and People* (Vol. 7).

Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, *17*(3), 181–188.

Cohen, J. (1992). QUANTITATIVE METHODS IN PSYCHOLOGY. *Psychological Bulletin*, *112*(1), 155–159.

Comrey, A. L., & Lee, H. B. (1992). Interpretation and application of factor analytic results. *Comrey AL, Lee HB. A first course in factor analysis*, *2*, 1992.

Connaughton, R., Bowyer, K. W., & Flynn, P. J. (2016). Handbook of Iris Recognition.

Connell, J., Ratha, N., Gentile, J., & Bolle, R. (2013). Fake Iris Detection Using Structured Light, 8692–8696.

Cruz, P., Barretto Filgueiras Neto, L., Muñoz-Gallego, P., & Laukkanen, T. (2010). *Mobile banking rollout in emerging markets: evidence from Brazil*. *International Journal of Bank Marketing* (Vol. 28).

Blair, J., Czaja, R. F., & Blair, E. A. (2013). *Designing surveys: A guide to decisions and procedures*. Sage Publications.

Davis, F D. (1986). A technology acceptance model for empirically testing new end-user information systems: Theory and results. *Management*, *Ph.D.*(April), 291.

Davis, Fred D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, *35*(8), 982–1003.

Deane, F., Barrelle, K., Henderson, R., & Mahar, D. (1995). Perceived acceptability of biometric security systems. *Computers and Security*, *14*(3), 225–231.

De Grada, E., Ercolani, A. P., Areni, A., & Sensales, G. (1987). La rappresentazione del computer in gruppi diversi della popolazione italiana. *Rassegna di psicologia*, *4*(2), 3.

Derawi, M. O., Nickely, C., Bours, P., & Busch, C. (2010). Unobtrusive user-authentication on mobile phones using biometric gait recognition. *Proceedings - 2010 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2010*, 306–311.

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security - ASIA CCS '17*, 386–399.

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. *Proceedings - International Carnahan Conference on Security Technology*, 170–178.

El-fishawy, N. (2015). Multi-Biometric Systems : A State of the Art Survey and Research Directions. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *6*(6), 128–138.

Elliott, S. J., O'connor, K., Bartlow, E., Robertson, J. J., & Guest, R. M. (2015). Expanding the human-biometric sensor interaction model to identity claim scenarios. *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*, 1–6.

Erdener, C. B. (1998). *Hofstede's Mas/Fem Dimension of National Culture and Work-related Values: Rethinking the Model*. Business Research Centre, School of Business, Hong Kong Baptist University.

Erumban, A. A., & De Jong, S. B. (2006). Cross-country differences in ICT adoption: A consequence of Culture?. *Journal of world business*, *41*(4), 302-314.

Ervasti, M., & Helaakoski, H. (2010). Case study of application-based mobile service acceptance and development in Finland. *International Journal of Information Technology and Management*, *9*(3), 243.

Evers, V., & Day, D. (1997). The Role of Culture in Interface Acceptance. *Proceedings Human Computer Interaction, Interact'97*, (1993), 260–267.

Faraj, S. & Sambamurthy, V. (2006). Leadership of Information Systems Development Projects. *IEEE Transactions on Engineering Management, 53*(2), 238–249.

Faqih, K. M. S. (2013). Exploring the influence of perceived risk and internet self-efficacy on consumer online shopping intentions : Perspective of technology acceptance model. *International Management Review*, *9*(1), 67–78.

Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, *21*(6), 15–26.

Feng, W., Zhou, J., Dan, C., Peiyan, Z., & Li, Z. (2017). Research on mobile commerce payment management based on the face biometric authentication. *International Journal of Mobile Communications*, *15*(3), 278.

Ferreira, J. B., da Rocha, A., & da Silva, J. F. (2014). Impacts of technology readiness on emotions and cognition in Brazil. *Journal of Business Research*, *67*(5), 865–873.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research.

Frischholz, R. W., & Werner, a. (2003). Avoiding replay-attacks in a face recognition system using head-pose estimation. *2003 IEEE International SOI Conference. Proceedings (Cat. No.03CH37443)*.

Furnell, S., & Evangelatos, K. (2007). Public awareness and perceptions of biometrics. *Computer Fraud and Security*, *2007*(1), 8–13.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and Supervision: A Survey of User Attitudes. *Computers & Security*, *19*(6), 529–539.

Fusilier, M., & Durlabhji, S. (2005). An exploration of student internet use in India. *Campus-Wide Information Systems*, *22*(4), 233–246.

Gatali, I. F., Lee, K. Y., Park, S. U., & Kang, J. (2016). A Qualitative Study on Adoption of Biometrics Technologies: Canadian Banking Industry. *Proceedings of the 18th Annual International Conference on Electronic Commerce: E-Commerce in Smart Connected World*, 20:1--20:8.

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

Geerthofstede.nl. (2015). *Dimension data matrix* [Data file]. Retrieved from https://geerthofstede.com/research-and-vsm/dimension-data-matrix/

Giarimi, S., & Magnusson, H. (2002). Investigation of user acceptance for biometric verification/identification methods in mobile units. *Master of Computer and Systems Sciences, Department of Computer Systems Sciences, Stockholm University*.

Gibbs, M. (2010). Biometrics: body odor authentication perception and acceptance. *ACM SIGCAS Computers and Society*, *40*(4), 16–24.

Gorman, L. (2003). Comparingpasswords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2020–2021.

Gorsuch, R. (1983). Factor analysis (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Guhr, N., Loi, T., Wiegard, R., & Breitner, M. H. (2013). Technology Readiness in Customers' Perception and Acceptance of M(obile)-Payment: An Empirical Study in Finland, Germany, the USA and Japan. *11th International Conference on Wirtschaftsinformatik*, 119–133.

Guo, G., Wen, L., & Yan, S. (2014). Face authentication with makeup changes. *IEEE Transactions on Circuits and Systems for Video Technology*, *24*(5), 814–825.

Gupta, V., Hanges, P. J., & Dorfman, P. (2002). Cultural clusters: Methodology and findings. *Journal of world business*, *37*(1), 11-15.

Gyekye, S. A., & Salminen, S. (2005). Responsibility assignment at the workplace: A Finnish and Ghanaian perspective. *Scandinavian Journal of Psychology*, *46*(1), 43–48.

Hallinan, P. W. (1991). Recognizing human eyes. In *Geometric Methods in Computer Vision* (Vol. 1570, pp. 214-227). International Society for Optics and Photonics.

Hamid, L. (2015). Biometric technology: not a password replacement, but a complement. *Biometric Technology Today*, *2015*(6), 7–10.

Hannah, J. (2005). Privacy concerns, expense keep biometrics out of US ATMs. *Information Week October*, *12*.

Heckle, R. R., Patrick, A. S., & Ozok, A. (2007). Perception and acceptance of fingerprint biometric technology. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 153-154). ACM.

Heimo, O. I., Hakkala, A., & Kimppa, K. K. (2012). How to abuse biometric passport systems. *Journal of Information, Communication and Ethics in Society*, *10*(2), 68–81.

Herskovits, M. J. (1955). Cultural anthropology.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2009). Tutki ja kirjoita. 15. painos. *Helsinki: Tammi*, 202-204.

Hofstede, G. (1976). Nationality and espoused values of managers. *Journal of Applied Psychology*, *61*(2), 148.

Hofstede, G. (1984). Culture's consequences: International differences in work-related values. Beverly Hills, CA: Sage.

Hofstede, G., Hofstede, G. J., Minkov, M. (2010). Cultures and Organizations: Software of the Mind, Third Edition (0071664181 / 9780071664189) McGraw-Hill Education: Professional Books.

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, *2*(1), 1–26.

Hofstede, G., & Hofstede, G. J. (2005). Cultures and organizations: Software of the mind (Revised and expanded 2nd ed.). New York: McGraw-Hill

Hofstede, G., & Minkov, M. (2013). VSM 2013. *Values survey module*.

Hofstede, G., Chueke, G. V., Pavan, K., & Avrichir, I. (2014). VALUES SURVEY MODULE 2013 Versão Português (Brasil). Retrieved from https://geerthofstede.com/wp-content/uploads/2016/08/VSM-2013-Portuguese-Brazil-New-Spelling-Agreement-2013-2014-11-07.doc

Hofstede, G., Garibaldi de Hilal, A. V., Malvezzi, S., Tanure, B., & Vinken, H. (2010). Comparing regional cultures within a country: Lessons from Brazil. *Journal of Cross-Cultural Psychology*, *41*(3), 336–352.

Hofstede, G., & Minkov, M. (2010). Long- versus short-term orientation : new perspectives, *2381*.

Hu, C., Yin, J., Zhu, E., Chen, H., & Li, Y. (2010). A composite fingerprint segmentation based on Log-Gabor filter and orientation reliability. *Proceedings - International Conference on Image Processing, ICIP*, *1*, 3097–3100.

Hu, P. J., Chau, P. Y. K., Liu Sheng, O. R., & Tam, K. Y. (1999). Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology. *Journal of Management Information Systems*, *16*(2), 91–112.

Igbaria, M., & Iivari, J. (1995). The effects of self-efficacy on computer usage. *Omega*, *23*(6), 587–605.

Igbaria, Magid, Iivari, J., & Maragahh, H. (1995). Why do individuals use computer technology? A Finnish case study. *Information and Management*, *29*(5), 227–238.

Im, I., Hong, S., & Kang, M. S. (2011). An international comparison of technology adoption: Testing the UTAUT model. *Information and Management*, *48*(1), 1–8.

Imura, S., & Hosobe, H. (2016). Biometric Authentication Using the Motion of a Hand. In *Proceedings of the 2016 Symposium on Spatial User Interaction* (pp. 221-221). ACM.

Instituto Brasileiro de Geografia e Estatística - IBGE. (2015). Acesso à Internet e à Televisão e Posse de Telefone Móvel Celular para Uso Pessoal.

Instituto Brasileiro de Geografia e Estatística - IBGE. (2016). Pesquisa Nacional por Amostra de Domicílios. Síntese de indicadores 2015.

International IDEA. (2017). If the EMB uses technology to collect voter registration data, is biometric data captured and used during registration?. Retrieved from https://www.idea.int/data-tools/question-view/738

Islam, M. S., Ali, M., Zubaer, K. H., Sarmin, S., Islam, M. T., Islam, B., … Sadri, A. M. (2017). Trusted Worrier: A low-cost and high-accuracy user authentication system for firearm exploiting dynamic hand pressure biometrics. *Proceedings of 2017 International Conference on Networking, Systems and Security, NSysS 2017*, 87–95.

Ito, K., Morita, A., Aoki, T., Higuchi, T., Nakajima, H., & Kobayashi, K. (2005). A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints.pdf, 33–36.

IriTech, inc. (2015). Key Drivers for Biometrics in South America in next 5 years. Retrieved from https://www.iritech.com/blog/biometric-south-america/

Jain, A. K. (2007). Technology: Biometric recognition. *Nature*.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing*, *18*(3), 1–23. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-33749373316&partnerID=40&md5=7a32b5a02e5d4d6922cca3ccaa256f4a

Jaswal, G., Kaul, A., & Nath, R. (2016). Knuckle Print Biometrics and Fusion Schemes -- Overview, Challenges, and Solutions. *ACM Computing Surveys*, *49*(2), 1–46.

Jayarathne, I., Cohen, M., & Amarakeerthi, S. (2017, November). Survey of EEG-based biometric authentication. In *2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST)* (pp. 324-329). IEEE.

Jenisch, S., & Uhl, A. (2011). Security analysis of a cancelable iris recognition system based on block remapping. *2011 18th IEEE International Conference on Image Processing*, 3213–3216.

Jones, L. A., Antón, A. I., & Earp, J. B. (2007). Towards understanding user perceptions of authentication technologies. *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society - WPES '07*, 91.

Kanak, A., & Sogukpinar, I. (2017). BioTAM: a technology acceptance model for biometric authentication systems. *IET Biometrics*, *6*(6), 457–467.

Kapoor, P., & Rawat, P. (2017). Biometric Quality : Analysis of Iris Recognition Techniques with other Biometric Authentication Systems, *162*(4), 31–36.

Karczmarek, P., Kiersztyn, A., Pedrycz, W., & Dolecki, M. (2017). An application of chain code-based local descriptor and its extension to face recognition. *Pattern Recognition*, *65*(July 2016), 26–34.

Karjaluoto, H., Mattila, M., & Pento, T. (2002). Factors underlying attitude formation towards online banking in Finland. *International Journal of Bank Marketing*, *20*(6), 261–272.

Kathuria, M. (2010). Design of a Vein Based Personal Identification System. *2010 International Conference on Advances in Recent Technologies in Communication and Computing*, 284–286.

Kedia, B. L., Keller, R. T., & Jullan, S. D. (1992). Dimensions of national culture and the productivity of R&D units. *Journal of High Technology Management Research*, *3*(1), 1–18.

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Journal of conflict resolution*, *2*(1), 51-60.

Khan, M. K., Zhang, J., & Alghathbar, K. (2011). Challenge-response-based biometric image scrambling for secure personal identification. *Future Generation Computer Systems*, *27*(4), 411–418.

Kim, Y. H. (2002). Financing Information Technology diffusion in low–income Asian developing countries. *Journal of Asian development*, 115-133.

Kivijärvi, M., Laukkanen, T., & Cruz, P. (2008). Consumer Trust in Electronic Service Consumption: A Cross-Cultural Comparison Between Finland and Portugal. *Journal of Euromarketing*, *16*(3), 51–65.

Klinge, M.: Poliittisen ja kulttuurisen Suomen muotoutuminen. In: Tommila, P. et al. (eds.): Suomen kulttuurihistoria II, WSOY, Porvoo 1980.

Kluckholn, C. (1951). The Study of Culture. In D. Lerner, & H. D. Lasswell (Eds.), The Policy Sciences. Stanford, CA: Stanford University Press.

Kothari, C. . (2009). *Research Methodology: Methods and Techniques* (Second Rev). New Age Publications (Academic).

Kowtko, M. A. (2014). Biometric Authentication for Older Adults.

Kripanont, N. (2007). Examining a Technology Acceptance Model of Internet Usage by Academic within Thai Business Schools. *School of Information Systems*.

Kroeber, A. L., & Kluckhohn, C. (1952). Culture: A critical review of concepts and definitions. *Papers. Peabody Museum of Archaeology & Ethnology, Harvard University*.

Krol, K., Parkin, S., & Sasse, M. A. (2016). "I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement. *ISBA 2016 - IEEE International Conference on Identity, Security and Behavior Analysis*.

Krupp, A., Rathgeb, C., & Busch, C. (2013). Social acceptance of biometric technologies in Germany: A survey. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *P-212*, 193–200. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84887983920&partnerID=tZOtx3y1

Kunnil, V. O., Pillai, A., & Milshtein, S. (2011). Biometrics assisted secure network transactions. *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, 69–74.

Miltgen, C., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decision Support Systems*, *56*(1), 103–114.

Lassmann, G. (2002). Some results on robustness, security and usability of biometric systems. *Proceedings. IEEE International Conference on Multimedia and Expo*, *2*, 577–580.

Lee, B. C., Yoon, J. O., & Lee, I. (2009). Learners' acceptance of e-learning in South Korea: Theories and results. *Computers and Education*, *53*(4), 1320–1329.

Lee, I., Choi, B., Kim, J., & Hong, S.-J. (2007). Culture-Technology Fit: Effects of Cultural Characteristics on the Post-Adoption Beliefs of Mobile Internet Users. *International Journal of Electronic Commerce*, *11*(4), 11–51.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management*, *40*(3), 191–204.

Leidner, D. E., & Kayworth, T. (2006). Review: a review of culture in information systems research: toward a theory of information technology culture conflict. *MIS Quarterly*, *30*(2), 357–399.

Lenartowicz, T., Johnson, J. P., & White, C. T. (2003). The neglect of intracountry cultural variation in international management research. *Journal of Business Research*, *56*(12), 999–1008.

Lenartowicz, T., & Roth, K. (2001). Does subculture within a Country matter? a cross-cultural study of motivational domains and business performance in Brazil. *Journal of International Business Studies*, *32*(2), 305–325.

Li, N., & Kirkup, G. (2007). Gender and cultural differences in Internet use: A study of China and the UK. *Computers and Education*, *48*(2), 301–317.

Li, Y., Li, Y., Yan, Q., Kong, H., & Deng, R. H. (2015). Seeing Your Face Is Not Enough : An Inertial Sensor-Based Liveness Detection for Face Authentication. *ACM SIGSAC Conference on Computer and Communications Security*, 1558–1569.

Liang, H.-N., Fleming, C., & Wang, W. (2014). User Authentication Interfaces in Mobile Devices: Some Design Considerations. *2014 IEEE 17th International Conference on Computational Science and Engineering*, 754–757.

Lin, C.-H., Hsin-Yu, S., & Sher, P. J. (2007). Integrating Technology Readiness into Technology Acceptance: The TRAM Model. *Psychology & Marketing*, *24*(7), 641–657.

Lin, F., Fofanah, S. S., & Liang, D. (2011). Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success. *Government Information Quarterly*, *28*(2), 271–279.

Liu, S., & Silverman, M. (2001). Practical guide to biometric security technology. *IT Professional*, *3*(1), 27–32.

Louho, R., & Kallioja, M. (2006). Factors affecting the use of hybrid media applications. *Graphic Arts in Finland*, *35*(3), 11–21. Retrieved from http://media.tkk.fi/GTTS/GAiF/GAiF_PDF/GAiF2006_3-2.pdf

Lu, D., Xu, K., & Huang, D. (2017). A Data Driven In-Air-Handwriting Biometric Authentication System, 531–537.

M. J. Burge, & Bowyer, K. W. (2013). *Handbook of Iris Recognition*. *Igarss 2014*. Springer Publishing Company, Incorporated.

Mackenzie, S. B., Podsakoff, P. M., Podsakoff, N. P., & Mackenzie, S. B. (2019). Linked references are available on JSTOR for this article : Construct

Measurement and Validation Procedures in MIS and Behavioral Research : Integrating New and Existing Techniques1, *35*(2), 293–334.

Mäenpää, K., Kale, S. H., Kuusela, H., & Mesiranta, N. (2008). Consumer perceptions of Internet banking in Finland: The moderating role of familiarity. *Journal of Retailing and Consumer Services*, *15*(4), 266–276.

Makrakis, V. (1992). Cross-cultural Comparison of Gender Differences in Attitude towards Computers in Japan and Sweden [1]. *Scandinavian Journal of Educational Research*, *36*(4), 275–287.

Maldonado, U., Khan, G., Moon, J., & Rho, J. (2011). E-learning motivation and educational portal acceptance in developing countries. *Online Information Review*, *35*(1), 66–85.

Malhotra, Y., & Galletta, D. F. (1999). Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation. *Proceedings of the 32nd Hawaii International Conference on System Sciences*, *00*(c), 1–11.

Mandal, B. (2017). Face recognition: Perspectives from the real world. *2016 14th International Conference on Control, Automation, Robotics and Vision, ICARCV 2016*, *2016*(November), 13–15.

Maple, C., & Norrington, P. (2006). The Usability and Practicality of Biometric Authentication in the Workplace. *First International Conference on Availability, Reliability and Security (ARES'06)*, 958–964.

Marcialis, G. L., & Roli, F. (2003). Experimental Results on Fusion of Multiple Fingerprint Matchers Fusion of Multiple Fingerprint Matchers, 814–820.

Maruoka, T., Kambe, K., Harada, H., & Nakanishi, I. (2017). A Study on Evoked Potential by Inaudible Auditory Stimulation toward Continuous Biometric Authentication, 1171–1174.

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, *2*(3), 173–191.

McCoy, S., Everard, A., & Jones, B. M. (2005). An examination of the technology acceptance model in Uruguay and the us: A focus on culture. *Journal of Global Information Technology Management*, *8*(2), 27–45.

Meenakshi, V. S., & Padmavathi, G. (2009). Security Analysis of Hardened Retina Based Fuzzy Vault. *2009 International Conference on Advances in Recent Technologies in Communication and Computing*, 926–930.

Memon, N. (2017). How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight]. *IEEE Signal Processing Magazine*, *34*(4), 194–196.

Mondal, P. C., Deb, R., & Adnan, M. N. (2017). On reinforcing automatic teller machine (ATM) transaction authentication security process by imposing behavioral biometrics. *2017 4th International Conference on Advances in Electrical Engineering (ICAEE)*, 369–372.

Moody, J. (2004). Public Perceptions of Biometric Devices : The Effect of Misinformation on Acceptance and Use. *Issues in Informing Science and Information Technology*, *1*, 753–761.

Morosan, C. (2012). Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *Journal of Hospitality and Tourism Research*, *36*(1), 52–84.

Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, *42*(21), 8198–8211.

NationMaster.com (2014). Local purchasing power: Countries Compared. Retrieved from https://www.nationmaster.com/country-info/stats/Cost-of-living/Local-purchasing-power

Nieminen, J. (2013). Etnisyystiedon merkitys kasvaa maahanmuuton lisääntyessä. Retrieved from https://www.stat.fi/artikkelit/2013/art_2013-09-23_003.html?s=0

Nigam, I., Vatsa, M., & Singh, R. (2015). Ocular biometrics: A survey of modalities and fusion approaches. *Information Fusion*, *26*, 1–35.

Nishimura, S., Nevgi, A., & Tella, S. (2008). Communication Style and Cultural Features in High/Low Context Communication Cultures: A Case Study of Finland, Japan and India. *Teoksessa A. Kallioniemi (Toim.), Uudistuva Ja Kehittyvä Ainedidaktiikka. Ainedidaktinen Symposiumi*, *8*(Lc), 783–386.

Nistor, N., Göğüş, A., & Lerche, T. (2013). Educational technology acceptance across national and professional cultures: A European study. *Educational Technology Research and Development*, *61*(4), 733–749.

Normalini, M. K., & Ramayah, T. (2017). Trust in Internet Banking in Malaysia and the Moderating Influence of Perceived Effectiveness of Biometrics Technology on Perceived Privacy and Security. *Journal of Management Sciences*, *4*(1), 3–26.

Nummelin, J. (2007). Measuring Organizational Culture in Construction Sector - Finnish Sample. *VTT Technical Research Centre of Finland*, (1980), 1–10.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). New York: McGraw-Hill.

Okazaki, S. (2012). Understanding e-learning adoption in brazil: Major determinants and gender effects. *International Review of Research in Open and Distance Learning*, *13*(4), 91–106.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Working Papers on Information Systems*, *10*(26), 1–51.

Omar, M. H. (1992). Attitudes of college students towards computers: A comparative study in the United States and the Middle East. *Computers in Human Behavior*, *8*(2–3), 249–257.

Onin.com (2017). *The History of Fingerprints.* Retrieved from http://onin.com/fp/fphistory.html

Oshlyansky, L., Cairns, P., & Thimbleby, H. (2007). Validating the Unified Theory of Acceptance and Use of Technology (UTAUT) tool cross-culturally. *Proceedings British Computer Society HCI 2007 Conference*, *2*, 83–86. Retrieved from http://portal.acm.org/citation.cfm?id=1531429

Overturf, G. D. (2000). Technical Report. *Pediatrics*, *106*(2), 367. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=3449077&site=ehost-live

Paasi, A. (1995). The social construction of peripherality: the case of Finland and the Finnish-Russian border area. In Competitive European Peripheries (pp. 235-258). Springer, Berlin, Heidelberg.

Paasi, A. (1997). Geographical perspectives on Finnish national identity. *GeoJournal*, *43*(1994), 41–50.

Park, N., Roman, R., Lee, S., & Chung, J. E. (2009). User acceptance of a digital library system in developing countries: An application of the Technology Acceptance Model. *International Journal of Information Management*, *29*(3), 196–209.

Parkavi, R., Babu, K. R. C., & Kumar, J. A. (2017). Multimodal Biometrics for user authentication. *Proceedings of 2017 11th International Conference on Intelligent Systems and Control, ISCO 2017*, 501–505.

Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep Face Recognition. *Procedings of the British Machine Vision Conference 2015*, (Section 3), 41.1-41.12.

Parsons, T., & Shils, E. E. (1951). Toward a General Theory of Action. New York, NY: Harper & Row Publishers.

Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, *33*(4), 49–61.

Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, *32*(5), 54–65.

Pavlou, A. P. (2003). Consumer Acceptance of Electronic Commerce : Integrating Trust and Risk with the Technology Acceptance Model Consumer Acceptance of Electronic Commerce : Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce ISSN:*, *7*(3), 101–134.

Perakslis, C., & Wolk, R. (2005, June). Social acceptance of RFID as a biometric security method. In *Proceedings. 2005 International Symposium on Technology and Society, 2005. Weapons and Wires: Prevention and Safety in a Time of Fear. ISTAS 2005*. (pp. 79-87). IEEE.

Phillips, T., Zou, X., & Li, F. (2017). A Cancellable and Privacy-Preserving Facial Biometric Authentication Scheme. *Proceedings - 14th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2017*, 545–549.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research*, *14*(3), 224-235.

Ponce, A. (2015). A Dynamic Behavioral Biometric Approach to Authenticate Users Employing Their Fingers to Interact with Touchscreen Devices, (46), 221.

Prakash, A., & Dhanalakshmi, R. (2016). Stride towards proposing multi-modal biometric authentication for online exam. *International Journal of Network Security*, *18*(4), 678–687.

Priya, B. S., & Rajesh, R. (2011). A note on fingerprint recognition systems. *2011 3rd International Conference on Electronics Computer Technology*, 95–98.

Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (2013). Secure biometrics: Concepts, authentication architectures, and challenges. *IEEE Signal Processing Magazine*, *30*(5), 51-64.

Rashed, A. S., & Henrique, A. E., Arwa, A. (2013, January). Biometrics acceptance in Arab culture: An exploratory study. In *2013 International Conference on Computer Applications Technology (ICCAT)* (pp. 1-7). IEEE.

Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. (2006). Cancelable biometrics: A case study in fingerprints. *Proceedings - International Conference on Pattern Recognition*, *4*, 370–373.

Rathod, V. J., Iyer, N. C., & Meena, S. M. (2015, October). A survey on fingerprint biometric recognition system. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 323-326). IEEE.

Raut, S. D. (2017). Development of Biometric Palm Vein Trait Based Person Recognition System Palm Vein Biometrics System, 18–21.

Rigas, I., & Komogortsev, O. V. (2017). Current research in eye movement biometrics: An analysis based on BioEye 2015 competition. *Image and Vision Computing*, *58*, 129–141.

Riley, C., Buckner, K., Johnson, G., & Benyon, D. (2009). Culture & biometrics: Regional differences in the perception of biometric authentication technologies. *AI and Society*, *24*(3), 295–306.

Riley, C., McCracken, H., & Buckner, K. (2007). Fingers, veins and the grey pound. *Proceedings of the 14th European Conference on Cognitive Ergonomics Invent! Explore! - ECCE '07*, (August), 149.

Rodriguez, R. J. (2015). An Electroencephalogram (EEG) Based Biometrics Investigation for Authentication: A Human-Computer Interaction (HCI) Approach. *Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing*, (67). Retrieved from http://nsuworks.nova.edu/gscis_etd%0Ahttp://nsuworks.nova.edu/gscis_etd/67.

Rogers, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.

Ronen, S., & Shenkar, O. (1985). Countries Clustering Dimensions : Attitudinal Synthesis and. *The Academy of Management Review*, *10*(3), 435–454.

Rose, J., Liu, Y., & Awad, A. (2017). Biometric Authentication Using Mouse and Eye Movement Data. *2017 IEEE Security and Privacy Workshops (SPW)*, 47–55.

Sabena, F., Dehghantanha, A., & Andrew, P. S. (2010). A review of vulnerabilities in identity management using biometrics. *2nd International Conference on Future Networks, ICFN 2010*, 42–49.

Sadasivuni, K. K., Houkan, M. T., Taha, M. S., & Cabibihan, J. J. (2017). Anti-spoofing device for biometric fingerprint scanners. *2017 IEEE International Conference on Mechatronics and Automation, ICMA 2017*, 683–687.

Sánchez-Franco, M. J., Martínez-López, F. J., & Martín-Velicia, F. A. (2009). Exploring the impact of individualism and uncertainty avoidance in Web-

based electronic learning: An empirical analysis in European higher education. *Computers and Education*, *52*(3), 588–598.

SANS Institute (n.d.). Glossary of Security Terms. Retrieved from https://www.sans.org/security-resources/glossary-of-terms/

Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information and Management*, *44*(1), 90–103.

Schneier, B. (2015). Identification and Authentication. *Secrets and Lies: Digital Security in a Networked World*, 135-150.

Sensales, G., & Greenfield, P. M. (1995). Attitudes toward computers, science, and technology: A cross-cultural comparison between students in Rome and Los Angeles. *Journal of cross-cultural Psychology*, *26*(3), 229-242.

Sharif Abbasi, M., Hussain Chandio, F., Fatah Soomro, A., & Shah, F. (2011). Social influence, voluntariness, experience and the internet acceptance. *Journal of Enterprise Information Management*, *24*(1), 30–52.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., ... & Cranor, L. F. (2010, July). Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.

Shubhangi, R. K., & Balbhim, N. B. (2017). Lip's movements biometric authentication in electronic devices. In *2017 International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 998-1001). IEEE.

Signorini, P., Wiesemes, R., & Murphy, R. (2009). Developing alternative frameworks for exploring intercultural learning: A critique of Hofstede's cultural difference model. *Teaching in Higher Education*, *14*(3), 253–264.

Simon, S. J. (2001). The Impact of Culture and Gender on Web Sites: An Empirical Study. *The DATA BASE for Advances in Information Systems*, *32*(1), 18–37.

Singh, N., Fassott, G., Chao, M. C. H., & Hoffmann, J. A. (2006). Understanding international web site usage. *International Marketing Review*, *23*(1), 83–97.

Sirota, D., & Greenwood, J. M. (1971). Understanding your overseas work force. *The International Executive*, *13*(2), 13-14.

Skaff, G. (2007). An alternative to passwords? *Biometric Technology Today*, *15*(5), 10–11.

SmartPLS GmbH. (2019). Model Fit. Retrieved from https://www.smartpls.com/documentation/algorithms-and-techniques/model-fit

Smith, D. F., Wiliem, A., & Lovell, B. C. (2015). Face recognition on consumer devices: Reflections on replay attacks. *IEEE Transactions on Information Forensics and Security*, *10*(4), 736–745.

Soniya, V., Sri, R. S., Titty, K. S., Ramakrishnan, R., & Sivakumar, S. (2017). Attendance automation using face recognition biometric authentication. *2017 International Conference on Power and Embedded Drive Control (ICPEDC)*, 122–127.

Spector, P. E., Cooper, C. L., & Sparks, K. (2001). An international study of the psychometric properties of the Hofstede values survey module 1994: A

comparison of individual and country/province level results. *Applied Psychology*, *50*(2), 269–281.

Sprager, S., Trobec, R., & Juric, M. B. (2017). Feasibility of biometric authentication using wearable ECG body sensor based on higher-order statistics. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 264–269.

Srite, M. (2006). Culture as an Explanation of Technology Acceptance Differences: An Empirical Investigation of Chinese and US Users. *Australasian Journal of Information Systems*, *14*(1), 5–26.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values i n technology acceptance^. *MIS Quarterly*, *30*(3), 679–704.

Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management*, *33*(1), 1–11.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., & Srite, M. (2002). Toward a Theory-Based Measurement of Culture. *Journal of Global Information Management*, *10*(1), 13–23.

Ahmed, B. S. E., & Elshoush, H. T. I. (2017, September). Biometrics solutions for blind person authentication. In *2017 Intelligent Systems Conference (IntelliSys)* (pp. 1053-1058). IEEE.

Tan, X., Chen, S., Zhou, Z. H., & Zhang, F. (2006). Face recognition from a single image per person: A survey. *Pattern Recognition*, *39*(9), 1725–1745.

Tarhini, A., Hone, K., & Liu, X. (2015). A cross-cultural examination of the impact of social, organisational and individual factors on educational technology acceptance between British and Lebanese university students. *British Journal of Educational Technology*, *46*(4), 739–755.

Tassabehji, R., & Kamala, M. A. (2009). Improving e-banking security with biometrics: Modelling user attitudes and acceptance. *3rd International Conference on New Technologies, Mobility and Security, NTMS 2009*.

Teo, T., Lee, C. B., Chai, C. S., & Wong, S. L. (2009). Assessing the intention to use technology among pre-service teachers in Singapore and Malaysia: A multigroup invariance analysis of the Technology Acceptance Model (TAM). *Computers and Education*, *53*(3), 1000–1009.

The World Bank Group (2019). World Bank Country and Lending Groups. Retrieved from https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups

Thomas, K. P., & Vinod, A. P. (2017). Toward EEG-Based Biometric Systems: The Great Potential of Brain-Wave-Based Biometrics. *IEEE Systems, Man, and Cybernetics Magazine*, *3*(4), 6–15.

Thomas, K. P., Vinod, A. P., & Robinson, N. (2017). Online Biometric Authentication Using Subject-Specific Band Power features of EEG. *Iccsp*, 136–141.

Tigre, P. B. (2003). Brazil in the age of electronic commerce. *Information Society*, *19*(1), 33–43.

Tilastokeskus. (2019). Suomi lukuina. Retrieved from https://www.stat.fi/tup/suoluk/index.html

Tilastokeskus (2019). Ulkomailla syntyneet. Retrieved from https://www.stat.fi/tup/maahanmuutto/maahanmuuttajat-vaestossa/ulkomailla-syntyneet.html

Tong, X. (2010). A cross-national investigation of an extended technology acceptance model in the online shopping context. *International Journal of Retail & Distribution Management*, *38*(10), 742–759.

Trewin, S., Swart, C., Koved, L., & Martino, J. (2012). Biometric authentication on a mobile device: a study of user effort, error and task disruption. *Proceedings of the 28th Annual Computer Security Applications Conference, (ACSAC '12)*, 159–168.

Trokielewicz, M., Czajka, A., & Maciejewicz, P. (2015). Assessment of iris recognition reliability for eyes affected by ocular pathologies. *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS 2015*.

Tylor, E. B. (1871). Primitive culture: researches into the development of mythology, philosophy, religion, art, and custom(Vol. 2). J. Murray.

Van Everdingen, Y. M., & Waarts, E. (2003). The effect of national culture on the adoption of innovations. *Marketing Letters*, *14*(3), 217-232.

Venkatesh, Morris, Davis, & Davis. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use : Integrating Control , Intrinsic Motivation , and Emotion into the Technology Acceptance Model. *Information System Research*, *11*(4), 342–365.

Venkatesh, V., & Davis, F. D. (1996). A Model of the Antecedents of Perceived Ease of Use: Development and Test. *Decision Science*, *27*(3), 451–481.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management science, 46(2), 186-204.

Venkatesh, V., Morris, M. G., Quarterly, S. M. I. S., Mar, N., & Morris, M. G. (2000). Why Don ' t Men Ever Stop to Ask for Directions ? Gender , Social Influence , and Their Role in Technology Acceptance and Usage Behavior. *MIS Quarterly*, *24*(1), 115–139.

Venkatesh, V., & Zhang, X. (2010). Unified theory of acceptance and use of technology: U.S. vs. China. *Journal of Global Information Technology Management*, *13*(1), 5–27.

Viberg, O., & Grönlund, Å. (2013). Cross-cultural analysis of users' attitudes toward the use of mobile devices in second and foreign language learning in higher education: A case from Sweden and China. *Computers and Education*, *69*, 169–180.

Visa Inc. (2016). European consumers ready to use biometricsfor securing payment. Retrieved from https://www.visaeurope.com/newsroom/news/european-consumers-ready-for-biometrics

Westin, A. F., & Ruebhausen, O. M. (1967). *Privacy and freedom* (Vol. 1., pp. 7-7). New York: Atheneum.

Wu, J. H., & Wang, S. C. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information and Management*, *42*(5), 719–729.

Wu, M. (2001). Hofstede ' s Cultural Dimensions 30 Years Later : A Study of Taiwan and the United States *, (1984), 33–42.

Yoo, S. J., & Huang, W. D. (2011). Comparison of Web 2 . 0 Technology Acceptance Level based on Cultural Differences. *Educational Technology & Society*, *14*(4), 241–252. Retrieved from http://www.ifets.info/download_pdf.php?j_id=53&a_id=1187

Yuan, C., Sun, X., & Lv, R. (2016). Fingerprint liveness detection based on multi-scale LPQ and PCA. *China Communications*, *13*(7), 60–65.

Zhou, W., Hu, J., Petersen, I., Wang, S., & Bennamoun, M. (2014). A benchmark 3D fingerprint database. *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2014*, 935–940.

Zhu, X., Lei, Z., Yan, J., Yi, D., & Li, S. Z. (2015). High-fidelity pose and expression normalization for face recognition in the wild. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 787-796).

Zimmermann, V., & Gerber, N. (2017, July). "If It Wasn't Secure, They Would Not Use It in the Movies"–Security Perceptions and User Acceptance of Authentication Technologies. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 265-283). Springer, Cham.

APPENDIX 1 ENGLISH, FINNISH AND PORTUQUESE VERSIONS OF THE FINAL QUESTIONNAIRE

Item abbreviation	Finnish questionnaire in English	Finnish questionnaire translated	Brazilian questionnaire in English	Brazilian questionnaire translated
	Thank you for taking part in this study. The purpose of this study is to understand societal views, attitudes towards biometric authentication technologies and security and privacy perceptions between Finnish and Brazilian nationals. Biometric authentication technologies utilize for an example fingerprint or eye iris to authenticate into a service or device, such as mobile phone or an ATM. Completing the survey takes approximately 15-20 minutes. Completing the survey is voluntary and you have the right to withdraw from the study at any time, leaving your results out of the final report. All information collected during the study will be kept confidential. No identifying information will be collected, and	Kiitos tutkimukseen osallistumisesta. Tämän pro gradu -tutkimuksen tarkoituksena on ymmärtää yhteiskunnallisia näkemyksiä, asenteita biometrisiä todentamisteknologioita kohtaan, sekä turvallisuuden ja yksityisyyden käsityksiä Suomen ja Brasilian kansalaisten välillä. Biometrisiä todentamisteknologioita ovat mm. sormenjäljen tai silmän iiriksen hyödyntäminen identiteetin todentamiseksi palvelussa tai laitteessa, esim. matkapuhelimessa tai pankkiautomaatilla. Kyselyn täyttämiseen kuluu aikaa noin 15-20 minuuttia. Kyselyn täyttäminen on vapaaehtoista. Voit halutessasi jäädä pois tutkimuksesta missä vaiheessa tahansa ja tällöin vastauksesi jäävät pois lopullisesta	Thank you for taking part in this study. The purpose of this study is to understand societal views, attitudes towards biometric authentication technologies and security and privacy perceptions between Finnish and Brazilian nationals. Biometric authentication technologies utilize for an example fingerprint or eye iris to authenticate into a service or device, such as mobile phone or an ATM. Completing the survey takes approximately 15-20 minutes. Completing the survey is voluntary and you have the right to withdraw from the study at any time, leaving your results out of the final report. All information collected during the study will be kept confidential. No identifying information will be collected, and	Obrigado por participar nesse estudo! O objetivo dessa pesquisa é entender pontos de vista sociais, atitudes sobre tecnologias de autenticação biométrica e percepções de segurança e privacidade entre os cidadãos da Finlândia e do Brasil. Tecnologias de autenticação biométrica utilizam, por exemplo, a impressão digital ou íris do olho para autenticar o acesso em um serviço ou em um aparelho, como celular ou caixa eletrônico. Completar o questionário leva aproximadamente 15 a 20 minutos. A sua participação é completamente voluntária, e em qualquer momento você tem o direito de se retirar do estudo e assim seus resultados não serão incluídos no relatório final. Todas as informações coletadas nesse estudo são

	therefore, responding will be completely anonymous. The survey results will only be used for scholarly purposes.	tutkimusraportista. Kaikki kerätty tieto on luottamuksellista. Mitään yksilöivää tietoa ei kerätä ja täten kyselyyn vastaaminen on täysin anonyymiä. Kyselyn tuloksia tullaan käyttämään ainoastaan akateemisen tutkimuksen tarkoituksiin.	therefore, responding will be completely anonymous. The survey results will only be used for scholarly purposes.	confidenciais. Nenhuma informação coletada é associada à identificação, e assim, as informações são completamente anônimas. Os resultados desse questionário vão ser usados somente para fins acadêmicos.
	You will first be asked some information about yourself (for statistical purposes):	Vastaisitko muutamaan kysymykseen tilastotietojen kartoittamista varten:	You will first be asked some information about yourself (for statistical purposes):	Primeiramente perguntamos algumas informações sobre você (para fins estatísticos):
NAT	What is your nationality? 1. Finnish 2. Brazilian	Mikä on kansalaisuutesi? 1. Suomalainen 2. Brasilialainen	What is your nationality? 1. Finnish 2. Brazilian	Qual é a sua nacionalidade? 1. Brasileiro (a) 2. Finlandês (a)
D	What was your nationality at birth (if different)?	Mikä oli kansalaisuutesi syntyessäsi (jos eri)?	What was your nationality at birth (if different)?	Qual foi a sua nacionalidade quando nasceu (se diferente da sua nacionalidade atual)?
			How would you define your color or race?	Como você define a sua cor ou raça?
D	What is your native language? 1. Finnish 2. Swedish 3. Sami 4. Russian 5. Other	Mikä on äidinkielesi? 1. Suomi 2. Ruotsi 3. Saame 4. Venäjä 5. Muu		
D	What is your gender? 1. Male 2. Female 3. Other	Mikä on sukupuolesi? 1. Mies 2. Nainen 3. Muu	What is your gender? 1. Male 2. Female 3. Other	Qual é o seu gênero? 1. Masculino 2. Feminino 3. Outro
D	What is your age?	Mikä on ikäsi?	What is your age?	Qual é a sua idade?

	1. Under 20 2. 20-24 3. 25-29 4. 30-39 5. 40-49 6. 50-59 7. 60 or older	1. Alle 20 2. 20-24 3. 25-29 4. 30-39 5. 40-49 6. 50-59 7. 60 tai vanhempi	1. Under 20 2. 20-24 3. 25-29 4. 30-39 5. 40-49 6. 50-59 7. 60 or older	1. Menos de 20 anos 2. Entre 20 e 24 anos 3. Entre 25 e 29 anos 4. Entre 30 e 39 anos 5. Entre 40 e 49 anos 6. Entre 50 e 59 anos 7. Mais de 60 anos
D	What is your marital status? 1. Married or domestic partnership 2. Judicially separated 3. Divorced 4. Widowed 5. Single and never married 6. Other	Mikä on siviilisäätysi? 1. Avio- tai avoliitossa 2. Asumuserossa 3. Eronnut 4. Leski 5 Naimaton 6. Muu	What is your marital status? 1. Married or domestic partnership 2. Judicially separated 3. Divorced 4. Widowed 5. Single and never married 6. Other	Qual é o seu estado civil? 1. Casado (a) 2. Separado (a) judicialmente 3. Divorciado (a) 4. Viúvo (a) 5. Solteiro (a) 6. Outro
D	What is your highest level of education? 1. Less than high school degree 2. High school degree or equivalent 3. Some higher education, no degree 4. Undergraduate or bachelor's degree 5. Master's degree 6. Doctorate degree 7. Other	Mikä on korkein koulutusasteesi? 1. Alempi kuin ylioppilastutkinto 2. Ylioppilastutkinto tai vastaava 3. Jonkin verran korkeakoulutusta, ei tutkintoa 4. Alempi korkeakoulututkinto 5. Ylempi korkeakoulututkinto 6. Tohtorin tutkinto 7. Muu	What is your highest level of education? 1. Less than high school degree 2. High school degree or equivalent 3. Some higher education, no degree 4. Undergraduate or bachelor's degree 5. Master's degree 6. Doctorate degree 7. Other	Qual é o nível mais alto de educação que você já completou? 1. Menor que ensino médio 2. Ensino médio ou equivalente 3. Ensino superior incompleto 4. Graduação 5. Mestrado 6. Doutorado 7. Outro
D	If you studied or study in a higher education institution, what is your major?	Jos opiskelit tai opiskelet korkeakoulussa, mikä on pääaineesi?	If you studied or study in a higher education institution, what is your major?	Se você estuda ou já estudou em instituição de ensino superior, qual é o seu curso?

D	If you have or have had a paid job, what kind of job is it / was it? 1. No paid job (includes full-time students) 2. Unskilled or semi-skilled manual worker 3. Generally trained office worker or secretary 4. Vocationally trained craftsperson, technician, IT-specialist, nurse, artist or equivalent 5. Academically trained professional or equivalent (but not a manager of people) 6. Manager of one or more subordinates (non-managers) 7. Manager of one or more managers	Jos olet tai olet ollut palkkatyössä, minkälainen työ se on / oli? 1. Ei palkkatyötä (sisältää päätoimiset opiskelijat) 2. Sekatyöläinen, ei-ammattilainen tai puoliammattilainen työntekijä 3. Toimistotyöntekijä tai sihteeri 4. Ammatillisesti koulutettu käsityöläinen, teknikko, IT-asiantuntija, hoitaja, taiteilija tai vastaava 5. Akateemisesti koulutettu ammattilainen tai vastaava (mutta ei esimies) 6. Yhden tai useamman alaisen (ei esimiehen) esimies 7. Yhden tai useamman esimiehen esimies	If you have or have had a paid job, what kind of job is it / was it? 1. No paid job (includes full-time students) 2. Unskilled or semi-skilled manual worker 3. Generally trained office worker or secretary 4. Vocationally trained craftsperson, technician, IT-specialist, nurse, artist or equivalent 5. Academically trained professional or equivalent (but not a manager of people) 6. Manager of one or more subordinates (non-managers) 7. Manager of one or more managers	Se você já teve ou tem um trabalho remunerado, qual tipo de trabalho foi ou é? 1. Nunca tive trabalho remunerado (inclui estudante) 2. Operário não especializado ou semiespecializado 3. Trabalho administrativo ou secretariado 4. Artista plástico, técnico, tecnólogo, especialista de TI, enfermeira ou equivalente 5. Cargo em que formação acadêmica é necessária (graduação) ou equivalente (excluindo gestores com subordinados) 6. Gestor de um ou mais subordinados (subordinados que não são gestores) 7. Gestor de um ou mais gestores
D	I am currently… 1. Employed for wages 2. Self-employed 3. Out of work and looking for work 4. Out of work and not looking for work 5. Homemaker 6. Student 7. Military 8. Retired 9. Unable to work 10. Other	Olen tällä hetkellä… 1. Palkkatyössä 2. Yrittäjä 3. Työtön työnhakija 4. Työtön, en hae työtä 5. Kotiäiti tai -isä 6. Opiskelija 7. Sotilashenkilö 8. Eläkkeellä 9. Työkyvytön 10. Muu	I am currently… 1. Employed for wages 2. Self-employed 3. Out of work and looking for work 4. Out of work and not looking for work 5. Homemaker 6. Student 7. Military 8. Retired 9. Unable to work 10. Other	No momento sou... 1. Empregado assalariado 2. Empreendedor 3. Desempregado e procurando por emprego 4. Desempregado e não procurando por emprego 5. Dono (a) da casa / do lar 6. Estudante 7. Militar 8. Aposentado (a)

				9. Em situação de invalidez 10. Outro
D	How much money total combined did all your household members earn in 2018? 1. 0 – 9 999 € 2. 10 000 – 19 999 € 3. 20 000 – 29 999 € 4. 30 000 – 39 999 € 5. 40 000 – 49 999 € 6. 50 000 – 59 999 € 7. 60 000 – 69 999 € 8. 70 000 – 79 999 € 9. 80 000 – 89 999 € 10. 90 000 – 99 999 € 11. 100 000 € or more	Kuinka paljon kotitaloutesi tulot olivat yhteensä vuonna 2018? 1. 0 – 9 999 € 2. 10 000 – 19 999 € 3. 20 000 – 29 999 € 4. 30 000 – 39 999 € 5. 40 000 – 49 999 € 6. 50 000 – 59 999 € 7. 60 000 – 69 999 € 8. 70 000 – 79 999 € 9. 80 000 – 89 999 € 10. 90 000 – 99 999 € 11. 100 000 € tai enemmän	How much was the total monthly income of all your household members in 2018? 1. Less than R$ 260,00 2. From R$ 260,01 to R$ 678 3. From R$ 678,01 to R$ 2.034,00 4. From R$ 2.034,01 to R$ 4.068,00 5. From R$ 4.068,01 to R$ 6.102,00 6. From R$ 6.102,01 to R$ 8.136,00 7. From R$ 8.136,01 to R$ 10.170,00 8. From R$ 10.170,01 to R$ 13.560,00 9. More than R$ 13.560,01	Qual foi a renda familiar mensal da sua casa em 2018? 1. Até R$ 260,00 2. De R$ 260,01 a R$ 678,00 3. De R$ 678,01 a R$ 2.034,00 4. De R$ 2.034,01 a R$ 4.068,00 5. De R$ 4.068,01 a R$ 6.102,00 6. De R$ 6.102,01 a R$ 8.136,00 7. De R$ 8.136,01 a R$ 10.170,00 8. De R$ 10.170,01 a R$ 13.560,00 9. Mais de R$ 13.560,01
	We are interested in your opinions. Please think of an ideal job, disregarding your present job, if you have one. In choosing an ideal job, how important would it be to you to... 1 = of utmost importance 2 = very important 3 = of moderate importance	Haluamme kuulla mielipiteesi. Kuvittele ihannetyösi, ottamatta huomioon mahdollista nykyistä työpaikkaasi. Valitessa ihannetyötä, kuinka tärkeää sinulle olisi… 1 = Äärimmäisen tärkeää 2 = Erittäin tärkeää 3 = Kohtalaisen tärkeää	We are interested in your opinions. Please think of an ideal job, disregarding your present job, if you have one. In choosing an ideal job, how important would it be to you to... 1 = of utmost importance 2 = very important 3 = of moderate importance	Queremos ouvir a sua opinião. Pense no emprego ideal, desconsiderando o seu atual emprego. O quanto seria importante para você... 1 = Extremamente importante 2 = Muito importante 3 = De importância moderada 4 = Pouco importante

	4 = of little importance 5 = of very little or no importance	4 = Ei kovin tärkeää 5 = Hyvin vähän tai ei ollenkaan tärkeää	4 = of little importance 5 = of very little or no importance	5 = Muito pouco ou nada importante
IDV1	have sufficient time for your personal or home life	Saada tarpeeksi vapaa-aikaa	have sufficient time for your personal or home life	Ter tempo suficiente para a vida pessoal e doméstica
PDI1	have a boss (direct superior) you can respect	Esimies, jota voit kunnioittaa	have a boss (direct superior) you can respect	Ter um chefe (superior direto) que você respeita
MAS1	get recognition for good performance	Saada tunnustusta hyvästä työstä	get recognition for good performance	Ter reconhecimento pelo bom desempenho
IDV2	have security of employment	Varmuus työsuhteen jatkumisesta	have security of employment	Ter estabilidade no emprego
MAS2	have pleasant people to work with	Työskennellä miellyttävien ihmisten kanssa	have pleasant people to work with	Trabalhar com pessoas agradáveis
IDV3	do work that is interesting	Tehdä mielenkiintoista työtä	do work that is interesting	Trabalhar em algo que ache interessante
PDI2	be consulted by your boss in decisions involving your work	Esimies, joka kääntyy puoleesi työhösi liittyvissä päätöksissä	be consulted by your boss in decisions involving your work	Ser consultado (a) pelo seu chefe em decisões que envolvem o seu trabalho
MAS3	live in a desirable area	Asua haluamassasi paikassa	live in a desirable area	Viver em um lugar da sua escolha
IDV4	have a job respected by your family and friends	Työpaikka, jota perheesi ja ystäväsi arvostavat	have a job respected by your family and friends	Ter um emprego respeitado por sua família e amigos
MAS4	have chances for promotion	Mahdollisuudet työssä ylenemiseen	have chances for promotion	Ter oportunidades de ser promovido (a)
	In your private life, how important is each of the following to you (answer in the scale 1-5): 1 = of utmost importance 2 = very important 3 = of moderate importance 4 = of little importance	Yksityiselämässäsi, kuinka tärkeää kukin seuraavista on sinulle (vastaa asteikolla 1-5): 1 = Äärimmäisen tärkeää 2 = Erittäin tärkeää 3 = Kohtalaisen tärkeää 4 = Ei kovin tärkeää	In your private life, how important is each of the following to you (answer in the scale 1-5): 1 = of utmost importance 2 = very important 3 = of moderate importance 4 = of little importance	Pensando em sua vida pessoal, o quanto é importante para você (responde na escada 1-5): 1 = Extremamente importante 2 = Muito importante 3 = De importância moderada 4 = Pouco importante

	5 = of very little or no importance	5 = Hyvin vähän tai ei ollenkaan tärkeää	5 = of very little or no importance	5 = Muito pouco ou nada importante
IVR1	keeping time free for fun	Ajan varaaminen hauskanpitoa varten	keeping time free for fun	Ter tempo livre para se divertir
IVR2	moderation: having few desires	Kohtuullisuus ja mielihalujen vähäinen määrä	moderation: having few desires	Ter moderação: se controlar para evitar excessos
LTO1	doing a service to a friend	Ystävien auttaminen	doing a service to a friend	Ajudar amigos
LTO2	thrift (not spending more than needed)	Säästäväisyys	thrift (not spending more than needed)	Simplicidade: não gastar mais do que o necessário
UAI1	How often do you feel nervous or tense? 1. always 2. usually 3. sometimes 4. seldom 5. never	Kuinka usein koet olosi hermostuneeksi tai jännittyneeksi? 1. Aina 2. Yleensä 3. Joskus 4. Harvoin 5. En koskaan	How often do you feel nervous or tense? 1. always 2. usually 3. sometimes 4. seldom 5. never	Com que frequência você se sente nervoso ou tenso? 1. Sempre 2. Normalmente 3. Às vezes 4. Raramente 5. Nunca
IVR3	Are you a happy person? 1. always 2. usually 3. sometimes 4. seldom 5. never	Oletko onnellinen? 1. Aina 2. Yleensä 3. Joskus 4. Harvoin 5. En koskaan	Are you a happy person? 1. always 2. usually 3. sometimes 4. seldom 5. never	Você é feliz? 1. Sempre 2. Normalmente 3. Às vezes 4. Raramente 5. Nunca
IVR4	Do other people or circumstances ever prevent you from doing what you really want to? 1. yes, always 2. yes, usually 3. sometimes 4. no, seldom 5. no, never	Estävätkö muut ihmiset tai olosuhteet koskaan sinua tekemästä mitä oikeasti haluaisit? 1. Kyllä, aina 2. Kyllä, yleensä 3. Joskus 4. Ei, harvoin 5. Ei, ei koskaan	Do other people or circumstances ever prevent you from doing what you really want to? 1. yes, always 2. yes, usually 3. sometimes 4. no, seldom 5. no, never	As outras pessoas ou circunstâncias impedem que você faça o que você realmente deseja fazer? 1. Sim, sempre 2. Sim, normalmente 3. Às vezes 4. Não, raramente 5. Não, nunca
UAI2	All in all, how would you describe your state of health these days? 1. very good 2. good	Miten kuvailisit terveydentilaasi näinä päivinä kokonaisuudessaan? 1. Erittäin hyvä 2. Hyvä	All in all, how would you describe your state of health these days? 1. very good 2. good	Em geral, como você descreveria seu estado de saúde atualmente? 1. Excelente 2. Bom

	3. fair 4. poor 5. very poor	3. Kohtalainen 4. Huono 5. Todella huono	3. fair 4. poor 5. very poor	3. Razoável 4. Ruim 5. Péssimo
LTO3	How proud are you to be a citizen of Finland? 1.very proud 2.fairly proud 3.somewhat proud 4.not very proud 5.not proud at all	Kuinka ylpeä olet Suomen kansalaisuudesta? 1. Erittäin ylpeä 2. Melko ylpeä 3. Jokseenkin ylpeä 4. En kovin ylpeä 5. En lainkaan ylpeä	How proud are you to be a citizen of Brazil? 1.very proud 2.fairly proud 3.somewhat proud 4.not very proud 5.not proud at all	O quanto você se orgulha de ser brasileiro? 1. Muito orgulhoso 2. Razoavelmente orgulhoso 3. Relativamente orgulhoso 4. Não muito orgulhoso 5. Nada orgulhoso
PDI3	How often, in your experience, are subordinates afraid to contradict their boss (or students their teacher?) 1. never 2. seldom 3. sometimes 4. usually 5. always	Omien kokemuksiesi mukaan, kuinka usein alaiset pelkäävät esittää vastaväitteitä esimiehelleen? (tai opiskelijat opettajalleen?) 1. Ei koskaan 2. Harvoin 3. Joskus 4. Yleensä 5. Aina	How often, in your experience, are subordinates afraid to contradict their boss (or students their teacher?) 1. never 2. seldom 3. sometimes 4. usually 5. always	No seu ponto de vista, com que frequência os subordinados sentem medo de contradizer o chefe (ou estudantes tem medo de contradizer o professor?) 1. Nunca 2. Raramente 3. Às vezes 4. Normalmente 5. Sempre
	To what extent do you agree or disagree with each of the following statements? 1 = strongly agree 2 = agree 3 = undecided 4 = disagree 5 = strongly disagree	Missä määrin olet samaa tai eri mieltä seuraavien väittämien kanssa? 1 = Vahvasti samaa mieltä 2 = Samaa mieltä 3 = En osaa sanoa 4 = Eri mieltä 5 = Vahvasti eri mieltä	To what extent do you agree or disagree with each of the following statements? 1 = strongly agree 2 = agree 3 = undecided 4 = disagree 5 = strongly disagree	Em que medida você concorda ou discorda com as afirmações abaixo? 1 = Concordo fortemente 2 = Concordo 3 = Não sei 4 = Discordo 5 = Discordo fortemente
UAI3	One can be a good manager without having a precise answer to every question that a subordinate may raise about his or her work	Esimies voi olla hyvä työssään ilman, että hänellä on tarkkoja vastauksia jokaiseen kysymykseen, jonka hänen alaisensa esittää työhönsä liittyen	One can be a good manager without having a precise answer to every question that a subordinate may raise about his or her work	Uma pessoa pode ser um bom gestor sem ter uma resposta precisa para toda pergunta que um subordinado pode fazer a respeito do seu trabalho

LTO4	Persistent efforts are the surest way to results	Sinnikäs vaivannäkö on varmin keino saada tuloksia	Persistent efforts are the surest way to results	Persistência é o melhor caminho para alcançar resultados
PDI4	An organization structure in which certain subordinates have two bosses should be avoided at all costs	Organisaatiorakennetta, jossa joillakin alaisilla on kaksi esimiestä, tulisi välttää kaikin keinoin	An organization structure in which certain subordinates have two bosses should be avoided at all costs	Uma estrutura organizacional em que os subordinados têm dois chefes deve ser evitada a qualquer custo
UAI4	A company's or organization's rules should not be broken - not even when the employee thinks breaking the rule would be in the organization's best interest	Yrityksen tai organisaation sääntöjä ei tule rikkoa – ei vaikka työntekijä uskoisi säännön rikkomisen olevan organisaation edun mukaista	A company's or organization's rules should not be broken - not even when the employee thinks breaking the rule would be in the organization's best interest	As regras de uma organização nunca devem ser quebradas – mesmo quando o empregado acha que a quebra da regra beneficia a organização
	You will now be asked questions regarding your perceptions of security and privacy. Choose the best response to the following statements by selecting either 1 = Strongly agree 2 = Agree 3 = Neither Agree nor disagree 4 = Disagree 5 = Strongly disagree	Seuraavat kysymykset käsittelevät näkemyksiäsi turvallisuuteen ja yksityisyyteen liittyen. Arvioi seuraavia väittämiä ja valitse mielestäsi sopivin vaihtoehto asteikolla 1-5, jossa 1 = Vahvasti samaa mieltä 2 = Samaa mieltä 3 = Ei samaa eikä eri mieltä 4 = Eri mieltä 5 = Vahvasti eri mieltä	You will now be asked questions regarding your perceptions of security and privacy. Choose the best response to the following statements by selecting either 1 = Strongly agree 2 = Agree 3 = Neither Agree nor disagree 4 = Disagree 5 = Strongly disagree	Agora você será perguntado (a) sobre questões relacionadas a suas percepções sobre segurança e privacidade. Escolha a melhor resposta às seguintes afirmações 1 = Concordo fortemente 2 = Concordo 3 = Não concordo nem discordo 4 = Discordo 5 = Discordo fortemente
P4	I feel it is important to avoid having personal information released that I think could be financially damaging.	Koen, että on tärkeää välttää mahdollisesti taloudellisesti vahingollisten henkilökohtaisten tietojen luovuttamista.	I feel it is important to avoid having personal information released that I think could be financially damaging.	Eu sinto que é importante evitar ter informações pessoais liberadas que podem ser financeiramente prejudiciais.
S4	My security at places of public access, such as a mall or airport, or special public events,	Turvallisuuteni julkisilla paikoilla, kuten ostoskeskuksissa tai lentokentillä, tai	My security at places of public access, such as a mall or airport, or special public events,	Minha segurança em lugares de acesso público, como por exemplo shoppings,

	such as big sports competitions, is important to me.	erityisissä julkisissa tapahtumissa, kuten suurissa urheilukisoissa, on minulle tärkeää.	such as big sports competitions, is important to me.	aeroportos, ou eventos públicos especiais como grandes competições de esportes, é importante para mim.
S8	I feel that the security of my personal information, such as my PC files or personal records (financial, medical, etc.) is important to me.	Koen, että henkilökohtaisten tietojeni, kuten tietokoneeni tiedostojen tai henkilökohtaisten asiakirjojeni (taloustiedot, terveystiedot jne.) turvallisuus on minulle tärkeää.	I feel that the security of my personal information, such as my PC files or personal records (financial, medical, etc.) is important to me.	Eu sinto que a segurança das minhas informações pessoais, como por exemplo, meus arquivos do computador ou registros pessoais (financeiros, médicos etc.) é importante para mim.
P3	I feel that it is important not to release sensitive information to any entity.	Koen, että on tärkeää olla luovuttamatta arkaluontoisia tietoja millekään taholle.	I feel that it is important not to release sensitive information to any entity.	Eu sinto que é importante não liberar informações sigilosas para nenhuma entidade.
S7	I feel that the safekeeping of my informational assets contained in digital or paper format is important to me (such as financial records, medical records, etc.).	Koen, että paperisessa tai digitaalisessa formaatissa olevan tieto-omaisuuteni (kuten talousasiakirjojen ja terveystietojen) turvallinen säilytys on minulle tärkeää.	I feel that the safekeeping of my informational assets contained in digital or paper format is important to me (such as financial records, medical records, etc.).	Eu sinto que a custódia dos meus bens de informação em formato digital ou papel é importante para mim (como por exemplo registros financeiros, médicos etc.).
P8	I feel that the release of personal information to entities where I feel as though I am anonymously providing the information is unacceptable.	Koen, että henkilökohtaisten tietojen luovuttaminen eri tahoille ei ole hyväksyttävää tilanteessa, jossa tunnen antavani tiedot anonyymisti.	I feel that the release of personal information to entities where I feel as though I am anonymously providing the information is unacceptable.	Eu sinto que é inaceitável liberar informações pessoais para entidades quando eu sinto que estou providenciando a informação anonimamente.
S5	I feel that the security of my tangible assets (such as my home, vehicle, etc.) is important to me.	Koen, että aineellisen omaisuuteni (kuten kotini, ajoneuvoni jne.) turvallisuus on minulle tärkeää.	I feel that the security of my tangible assets (such as my home, vehicle, etc.) is important to me.	Eu sinto que a segurança dos meus bens tangíveis (como por exemplo minha casa, meu veículo etc.) é importante para mim.
P7	I feel that the release of personal	Koen, että henkilökohtaisten tietojeni	I feel that the release of personal	Eu sinto que é inaceitável liberar

	information to individuals with whom I have a high comfort level is unacceptable.	luovuttaminen lähimmäisilleni ei ole hyväksyttävää.	information to individuals with whom I have a high comfort level is unacceptable.	informações pessoais para indivíduos com quem eu tenho alto nível de conforto.
P1	I feel my privacy is very important to me.	Koen, että yksityisyyteni on minulle erittäin tärkeää.	I feel my privacy is very important to me.	Eu sinto que a minha privacidade é muito importante para mim.
S3	I feel that my personal security at my place of work or other work-related places is important to me.	Koen, että henkilökohtainen turvallisuuteni työpaikallani tai muissa työhön liittyvissä paikoissa on minulle tärkeää.	I feel that my personal security at my place of work or other work-related places is important to me.	Eu sinto que a minha segurança pessoal no meu lugar de trabalho ou em outros lugares relacionados ao trabalho é importante para mim.
P2	I feel that my control over my personal information is very important to me.	Koen, että määräysvaltani omia henkilökohtaisia tietojani koskien on minulle erittäin tärkeää.	I feel that my control over my personal information is very important to me.	Eu sinto que ter o controle sob minha informação pessoal é muito importante para mim.
S9	I feel that the safekeeping of information I have provided to a corporation or other entity is important to me.	Koen, että yritykselle tai muulle taholle luovuttamani tiedon turvallinen säilytys on minulle tärkeää.	I feel that the safekeeping of information I have provided to a corporation or other entity is important to me.	Eu sinto que a custódia das informações que eu providenciei para uma corporação ou outra entidade é importante para mim.
P9	I feel that the use of personal information that has been released by me but is used in a manner not intended by me is unacceptable.	Koen, että ei ole hyväksyttävää käyttää luovuttamiani henkilökohtaisia tietoja tavalla, jota en ole tarkoittanut.	I feel that the use of personal information that has been released by me but is used in a manner not intended by me is unacceptable.	Eu sinto que o uso de informação pessoal que eu liberei, mas que é usado de um jeito que eu não desejei, é inaceitável.
P6	I feel it is important to avoid having personal information about me released that may go against social morals and attitudes.	Koen, että on tärkeää välttää minua koskevien, mahdollisesti normien ja asenteiden vastaisten henkilökohtaisten tietojen luovuttamista.	I feel it is important to avoid having personal information about me released that may go against social morals and attitudes.	Eu sinto que é importante evitar ter informações pessoais sobre mim liberadas, que podem estar contra a postura e a moral social.
S2	I feel that my personal security at my home or in my vehicle is important to me.	Koen, että henkilökohtainen turvallisuuteni kodissani tai ajoneuvossani	I feel that my personal security at my home or in my vehicle is important to me.	Eu sinto que a minha segurança pessoal na minha casa ou no meu veículo (carro,

		on minulle tärkeää.		moto etc.) é importante para mim.
P5	I feel it is important to avoid having personal information released that I think could be socially damaging to me.	Koen, että on tärkeää välttää mahdollisesti minulle sosiaalisesti vahingollisten henkilökohtaisten tietojen luovuttamista.	I feel it is important to avoid having personal information released that I think could be socially damaging to me.	Eu sinto que é importante evitar ter informações pessoais liberadas, que podem ser socialmente prejudiciais para mim.
S6	I feel that keeping my personal possessions, such as jewelry, money, electronics, etc., safe is important to me.	Koen, että henkilökohtaisen omaisuuteni, kuten korujen, rahan, elektroniikan jne. turvassa pitäminen on minulle tärkeää.	I feel that keeping my personal possessions, such as jewelry, money, electronics, etc., safe is important to me.	Eu sinto que manter minhas posses pessoais seguras, como por exemplo joias, dinheiro, eletrônicos etc., é importante para mim.
S1	I feel that the safeguarding from potential external threats of my physical being is important to me.	Koen, että suojautuminen itseeni kohdistuvilta, mahdollisilta ulkoisilta fyysisiltä uhilta on minulle tärkeää.	I feel that the safeguarding from potential external threats of my physical being is important to me.	Eu sinto que é importante para mim me resguardar de ameaças físicas potenciais contra mim.
	You will now be asked questions regarding your perceptions of biometric authentication technologies.	Seuraavat kysymykset käsittelevät näkemyksiäsi biometrisen todentamisen teknologioihin liittyen.	You will now be asked questions regarding your perceptions of biometric authentication technologies.	Agora você será perguntado (a) sobre questões relacionadas às suas percepções sobre tecnologias biométricas.
KNO	Have you heard of biometrics? 1. Yes 2. No	Oletko kuullut biometriasta? 1. Kyllä 2. En	Have you heard of biometrics? 1. Yes 2. No	Você já ouviu falar sobre biometria? 1. Sim 2. Não
	If yes, about which biometric technologies you have heard?	Jos kyllä, mistä biometrisistä teknologioista olet kuullut?	If yes, about which biometric technologies you have heard?	Se sim, sobre quais tecnologias biométricas você já ouviu falar?
FAM	Have you used biometrics? 1. Yes 2. No	Oletko käyttänyt biometriaa? 1. Yes 2. No	Have you used biometrics? 1. Yes 2. No	Você já usou biometria? 1. Sim 2. Não

	If yes, which biometric technologies you have used?	Jos kyllä, mitä biometrisiä teknologioita olet käyttänyt?	If yes, which biometric technologies you have used?	Se sim, quais tecnologias biométricas você já usou?
	Please read the following vignettes and then respond to each statement below. Your responses should fall between 1 = strongly agree and 5 = strongly disagree.	Ole hyvä ja lue seuraavat lyhyet kuvaukset ja vastaa kunkin kuvauksen jälkeen sen alla oleviin väittämiin. Vastaa asteikolla 1-5, jossa 1= vahvasti samaa mieltä ja 5= vahvasti eri mieltä.	Please read the following vignettes and then respond to each statement below. Your responses should fall between 1 = strongly agree and 5 = strongly disagree.	Por favor leia as seguintes vinhetas e responda cada afirmação abaixo. Você deve responder entre 1 = concordo fortemente e 5 = discordo fortemente.
V1	Jimi returns home from work. To enter his residence, he places his hand on a biometric hand geometry scanner located by the door instead of using a key for entrance. He holds his hand on the pad for a few seconds.	Jimi palaa töistä kotiin. Päästäkseen sisälle taloonsa, avaimen käyttämisen sijaan hän laittaa kätensä ovenpielessä sijaitsevalle biometriselle käden geometriaa tunnistavalle lukulaitteelle. Hän pitää kättään alustalla muutaman sekunnin ajan.	Tiago returns home from work. To enter his residence, he places his hand on a biometric hand geometry scanner located by the door instead of using a key for entrance. He holds his hand on the pad for a few seconds.	Tiago volta para a casa do trabalho. Para entrar na casa, ao invés de usar uma chave, ele coloca a mão em um scanner biométrico de geometria manual ao lado da porta. Ele mantém a mão no scanner por alguns segundos.
PU1	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU1	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU+PEU1	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI1	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.

IU1	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
V2	Pirjo goes to the airport to visit Turkey. A facial scanner is used upon entering the airport, where the image is compared against a database of known criminal offenders, to prevent the entry of undesirable persons to the sterile area of the airport. She has to step on a marked spot and look at a camera for a few seconds in order to have her face scanned to compare it with this database.	Pirjo menee lentokentälle matkustaakseen Turkkiin. Lentokentällä on käytössä kasvojenlukulaite, jonka avulla kuvaa Pirjon kasvoista verrataan rikollisista koostuvaan tietokantaan. Näin estetään ei-toivottujen henkilöiden pääsy lentokentän turvatulle alueelle. Hänen täytyy astua merkatulle paikalle ja katsoa muutaman sekunnin ajan kameraan kasvojen skannausta ja tietokantaan vertaamista varten.	Beatriz goes to the airport to visit Turkey. A facial scanner is used upon entering the airport, where the image is compared against a database of known criminal offenders, to prevent the entry of undesirable persons to the sterile area of the airport. She has to step on a marked spot and look at a camera for a few seconds in order to have her face scanned to compare it with this database.	Beatriz vai ao aeroporto para visitar a Turquia. Um scanner facial é usado na entrada do aeroporto. A imagem é comparada com um banco de dados dos criminosos, para prevenir a entrada de pessoas indesejadas na área protegida do aeroporto. Ela precisa passar no lugar marcado e olhar para a câmera por alguns segundos para ter uma foto escaneada que é comparada com esse banco de dados.
PU2	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU2	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU2	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI2	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.
IU2	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
V3	Kari works at a biochemical	Kari työskentelee biokemia-alan	Caio works at a biochemical	Caio trabalha em uma empresa

	company where sensitive research on cloning practices is taking place. This area of the company contains computers and sensitive research information that is restricted to certain employees. He needs to be authorized to enter the area every time access is needed by using a retinal scanner at the door. He has to place his face in a frame, with his chin in a chin slot. He has to look in a scanning device for a few seconds without blinking.	yrityksessä, jossa tehdään arkaluontoista tutkimusta kloonaukseen liittyen. Tämä yrityksen alue sisältää tietokoneita ja arkaluontoista tutkimustietoa, johon pääsy on rajoitettu tietyille työntekijöille. Päästäkseen alueelle, Karin täytyy joka kerta saada valtuutus käyttämällä ovella sijaitsevaa verkkokalvon tunnistavaa lukulaitetta. Hänen täytyy asettaa kasvonsa kehykseen ja leuka sille varattuun paikkaan. Karin täytyy katsoa lukulaitteeseen muutaman sekunnin ajan silmiä räpäyttämättä.	company where sensitive research on cloning practices is taking place. This area of the company contains computers and sensitive research information that is restricted to certain employees. He needs to be authorized to enter the area every time access is needed by using a retinal scanner at the door. He has to place his face in a frame, with his chin in a chin slot. He has to look in a scanning device for a few seconds without blinking.	bioquímica onde pesquisa sigilosa sobre clonagem está acontecendo. Essa área da empresa contém computadores e informações confidenciais da pesquisa que é restrita para empregados específicos. Toda vez que Caio precisa acessar a área, é necessário que ele seja autorizado por meio de um scanner de retina na porta. Ele precisa colocar o rosto em uma moldura e o queixo em uma abertura, sendo necessário que olhe no aparelho de escaneamento por alguns segundos, sem piscar os olhos.
PU3	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU3	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU3	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI3	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.
IU3	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.

V4	Jaana goes to the bank to get cash out of the ATM machine. In lieu of a passcode and ATM card, the transaction is authorized and her identity authenticated by the use of a fingerprint scanner. She has to press her thumb on a biometric device and the device scans her thumbprint instantaneously to access the records pertaining to her.	Jaana menee pankkiin nostamaan rahaa pankkiautomaatista. Pankkikortin ja PIN-koodin sijaan nostotapahtuman valtuutus ja hänen identiteettinsä todennus tapahtuu sormenjäljen tunnistavan lukulaitteen avulla. Päästäkseen käsiksi pankkitietoihinsa, Jaanan täytyy painaa peukalonsa biometriaa hyödyntävään laitteeseen, jolloin laite lukee hänen sormenjälkensä välittömästi.	Joana goes to the bank to get cash out of the ATM machine. In lieu of a passcode and ATM card, the transaction is authorized and her identity authenticated by the use of a fingerprint scanner. She has to press her thumb on a biometric device and the device scans her thumbprint instantaneously to access the records pertaining to her.	Joana vai ao banco para tirar dinheiro do caixa eletrônico. Ao invés de uma senha e cartão de débito, a transação é autorizada e a identidade autenticada por um scanner de impressão digital. Ela precisa colocar o dedo polegar no aparelho biométrico e o aparelho escaneia a impressão do polegar instantaneamente para acessar os registros que pertencem a ela.
PU4	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU4	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU4	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI4	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.
IU4	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
V5	Petteri works for a data center that contains highly sensitive information and expensive equipment. The data center	Petteri työskentelee datakeskuksessa, jossa säilytetään erittäin arkaluontoista tietoa ja kallista laitteistoa. Datakeskuksessa	Pedro works for a data center that contains highly sensitive information and expensive equipment. The data center	Pedro trabalha em um centro de processamento de dados que contém informação extremamente sensível e equipamento caro.

	tracks the times that the individual enters and exits the data center. Petteri enters the data center by using a hand geometry scanner and to exit the data center he has to also use a hand geometry scanner. To use the device, Petteri has to place his hand on the hand geometry scanner for a few seconds upon entry and exit to the data center.	seurataan aikoja, jolloin henkilö astuu sisään ja poistuu datakeskuksesta. Petteri käyttää sekä datakeskukseen sisään tullessaan että sieltä poistuessaan käden geometriaa tunnistavaa lukulaitetta. Käyttääkseen laitetta, Petterin täytyy asettaa kätensä muutamaksi sekunniksi käden geometriaa tunnistavalle lukulaitteelle.	tracks the times that the individual enters and exits the data center. Pedro enters the data center by using a hand geometry scanner and to exit the data center he has to also use a hand geometry scanner. To use the device, Pedro has to place his hand on the hand geometry scanner for a few seconds upon entry and exit to the data center.	O centro de processamento de dados monitora os horários de quando o indivíduo entra ou sai do local. Pedro entra no centro de processamento de dados usando um scanner de geometria de mão, e para sair do local, ele também precisa usar o mesmo scanner. Para usar o aparelho, Pedro precisa colocar a mão no scanner de geometria da mão por alguns segundos na entrada e saída do centro de processamento de dados.
PU5	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU5	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU5	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI5	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.
IU5	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
V6	Kari is one of the system administrators	Kari on yksi yrityksen järjestelmäylläpitäjistä. Ylläpitäjän	Caio is one of the system administrators	Caio é um dos administradores de sistemas em uma empresa. Como

	for a company. As a system administrator, Kari has access to all files on the computer. The company tracks administrator access to the server. The company is implementing a fingerprint biometric to authenticate onto the server as administrator. Kari has to place his index finger on a biometric device, which instantly authenticates him into the server.	ominaisuudessa Karilla on pääsy kaikkiin tietokoneen tiedostoihin. Yritys seuraa ylläpitäjien kirjautumisia palvelimille. Yritys on ottamassa käyttöön biometrisen sormenjälkitunnisteen ylläpitäjien palvelimelle todentamista varten. Karin täytyy sijoittaa etusormensa biometriaa hyödyntävälle laitteelle, joka välittömästi todentaa hänen identiteettinsä palvelimelle.	for a company. As a system administrator, Caio has access to all files on the computer. The company tracks administrator access to the server. The company is implementing a fingerprint biometric to authenticate onto the server as administrator. Caio has to place his index finger on a biometric device, which instantly authenticates him into the server.	um administrador de sistemas, Caio tem acesso a todos os arquivos no computador. A empresa monitora o acesso dos administradores no servidor. A empresa está implementando biometria de impressão digital para autenticar o acesso dos administradores nos servidores. Caio precisa colocar o dedo indicador no aparelho biométrico, que instantaneamente o autentica no servidor.
PU6	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU6	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU6	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI6	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.
IU6	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
V7	A hospital keeps medical records on all its patients. In the past, this information was protected by a password that was	Sairaala pitää kirjaa kaikkien potilaidensa terveystiedoista. Aiemmin tiedot suojattiin salasanalla, jota jaettiin	A hospital keeps medical records on all its patients. In the past, this information was protected by a password that was	Um hospital mantém registros médicos de todos os seus pacientes. No passado, essa informação foi protegida por uma

	freely passed around when information was needed. For liability reasons, the hospital wants to restrict access to the medical records to only doctors and nurses. The hospital decides to implement a retinal scanner biometric device to ensure that only authorized individuals access the medical records. The doctor or nurse has to stand in front of the retinal scanner staring at a marked spot for a few seconds to authenticate into the system.	vapaasti kaikille tietoja tarvitseville. Vastuukysymysten vuoksi sairaala haluaa rajoittaa pääsyn potilastietoihin vain lääkäreille ja hoitajille. Sairaala päättää ottaa käyttöön biometriaa hyödyntävän, silmien verkkokalvoja tunnistavan lukulaitteen varmistaakseen, että vain valtuutetut henkilöt pääsevät käsiksi terveystietoihin. Todentaakseen itsensä järjestelmään, lääkärin tai hoitajan täytyy seistä silmien verkkokalvoja tunnistavan lukulaitteen edessä ja pitää katseensa merkatussa pisteessä muutaman sekunnin ajan.	freely passed around when information was needed. For liability reasons, the hospital wants to restrict access to the medical records to only doctors and nurses. The hospital decides to implement a retinal scanner biometric device to ensure that only authorized individuals access the medical records. The doctor or nurse has to stand in front of the retinal scanner staring at a marked spot for a few seconds to authenticate into the system.	senha, que foi livremente divulgada quando a informação foi necessária. Por motivos de responsabilidade, o hospital deseja limitar o acesso de registros médicos somente para os médicos e enfermeiros. O hospital decide implementar um aparelho biométrico que escaneia retinas para garantir que somente indivíduos autorizados acessem os registros médicos. O médico ou enfermeiro precisa passar na frente do scanner de retinas e olhar em um ponto fixo por alguns segundos para autenticá-lo no sistema.
PU7	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU7	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU7	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI7	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse aparelho seria fisicamente invasivo.

IU7	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
V8	Katariina wants to use a credit card at a store to pay for her purchases. Normally, she would have to present an official photo id and sign a credit slip. To increase security, a digital signature device is used to authenticate the person. Katariina has to sign a digital pad instead of signing a credit slip.	Katariina haluaa käyttää luottokorttia maksaakseen ostoksensa kaupassa. Tavallisesti hänen tulisi esittää virallinen, kuvallinen henkilöllisyystodistus ja allekirjoittaa tosite. Turvallisuuden parantamiseksi kaupassa käytetään digitaalista allekirjoitusta hyödyntävää laitetta henkilön todentamiseksi. Katariinan tulee kirjoittaa allekirjoitus digitaaliselle alustalle tositteen allekirjoittamisen sijaan.	Catarina wants to use a credit card at a store to pay for her purchases. Normally, she would have to present an official photo id and sign a credit slip. To increase security, a digital signature device is used to authenticate the person. Catarina has to sign a digital pad instead of signing a credit slip.	Catarina quer usar um cartão de crédito para pagar as compras dela na loja. Normalmente, ela precisaria de apresentar uma identidade oficial com foto e assinar um recibo. Para aumentar a segurança, um aparelho de assinatura digital é utilizado para autenticação. Catarina precisa assinar uma plataforma digital em vez de assinar um recibo.
PU8	I think this biometric device is useful.	Uskon, että tämä biometriaa hyödyntävä laite on hyödyllinen.	I think this biometric device is useful.	Eu acredito que esse aparelho biométrico é útil.
PEU8	I think this biometric device is easy to use.	Uskon, että tämä biometriaa hyödyntävä laite on helppokäyttöinen.	I think this biometric device is easy to use.	Eu acredito que esse aparelho biométrico é fácil de utilizar.
PU/PEU8	I think one of the reasons this device is useful is because of its ease of use.	Uskon, että yksi syy, joka tekee tästä laitteesta hyödyllisen, on sen helppokäyttöisyys.	I think one of the reasons this device is useful is because of its ease of use.	Eu acredito que um dos motivos pelos quais esse aparelho é útil é por conta da sua facilidade de utilização.
PI8	I think that this device would be physically invasive.	Uskon, että tämä laite olisi fyysisesti tunkeileva.	I think that this device would be physically invasive.	Eu acredito que esse parelho seria fisicamente invasivo.
IU8	I think I would use this device.	Uskon, että käyttäisin tätä laitetta.	I think I would use this device.	Eu acredito que eu utilizaria esse aparelho.
	In an open comment, you can mention the	Tähän voit halutessasi kertoa omin sanoin syitä,	In an open comment, you can mention the	Em um comentário espontâneo, você pode mencionar os

	reasons to why you would want to adopt biometric authentication technologies.	joiden vuoksi haluaisit ottaa käyttöön biometrisen todentamisen teknologioita.	reasons to why you would want to adopt biometric authentication technologies.	motivos pelos quais você gostaria de adotar tecnologias de autenticação biométrica.
	In an open comment, you can mention the reasons to why you would not want to adopt biometric authentication technologies.	Tähän voit halutessasi kertoa omin sanoin syitä, joiden vuoksi et haluaisi ottaa käyttöön biometrisen todentamisen teknologioita.	In an open comment, you can mention the reasons to why you would not want to adopt biometric authentication technologies.	Em um comentário espontâneo, você pode mencionar os motivos pelos quais você não gostaria de adotar tecnologias de autenticação biométrica.
NAT = Nationality, D = Demographic information, IDV = Individualism vs. Collectivism, PDI = Power Distance, MAS = Masculinity vs. Femininity, IVR = Indulgence vs. Restraint, LTO = Long vs. Short Term Orientation, UAI = Uncertainty Avoidance, P = Perceived Need For Privacy, S = Perceived Need For Security, KNOW = Knowledge of Biometrics, FAM = Familiarity With Biometrics, V = Vignette, PU = Perceived Usefulness, PEU = Perceived Ease of Use, PI = Perceived Physical Invasiveness, IU = Intention to Use				