Citizen perceptions on Biometrics: Surveillance or service?

by

Tim Bussmann

S1709798

timbussmann@protonmail.com

Submitted in partial fulfillment of the requirements for the degree of Master of Science, program Public Administration, University of Twente

2019-2020

Supervisors:

Ringo Ossewaarde, BMS

Peter Stegmaier, BMS

Words: 19000+

Abstract

Background: With the coming of new technologies like biometrics, both public and private institutes are more than ever capable of invigilating citizens wherever they go. As a result, both negative and positive societal examples of the utilization of biometrics can be found across the globe. These examples influence the perception of citizens on biometrics technology, which leaves some citizens fearful of a future society where biometrics is a large part of their daily lives. However, in order for governments and companies to properly make use of biometrics in the future, citizen perceptions on biometrics acceptance have to be taken into account. In earlier research, it was found that biometrics acceptance among citizens was related to the extent of informedness and the degree of privacy concerns of citizens. Therefore, this study aims to investigate to what extent biometrics acceptance among citizens is related to biometrics informedness and biometrics privacy concerns

Methods: A questionnaire was constructed on the basis of earlier distributed questionnaires in the field of biometrics acceptance and finally distributed to the participants in the sample. On a ten-point scale, participants answered questions and statements regarding biometrics informedness, biometrics privacy concerns and biometrics acceptance. These participants were recruited through an online recruitment panel of the University of Twente and through the personal network of the researcher. The most important criterion was to be a resident of the Netherlands. In total, this led to a sample size of N=74. The survey data was later exported to and analyzed with SPSS 25.

Results: Descriptives of the sample indicated that Dutch residents are relatively uninformed in terms of biometrics acceptance, have a decent amount of privacy concerns and are somewhat willing to accept the utilization of biometrics in society. Furthermore, a pearson's correlation analysis showed that there were significant correlations between biometrics acceptance and the two other factors: biometrics informedness & privacy concerns. Finally, a multiple regression analysis showed that biometrics informedness has a positive effect on biometrics acceptance, whereas biometrics privacy concerns has a negative effect on biometrics acceptance. Interestingly, the effect of privacy concerns was 3 times as strong as the effect of biometrics informedness.

Conclusion: Biometrics informedness and biometrics privacy concerns do indeed have a significant impact on the biometrics acceptance of Dutch residents. This dependency was marginally studied in the past and often just one of both factors was taken into account during statistical analyses. With the insights of this study, both the government and biometrics companies can work to utilize biometrics in a way which gains the trust of their citizens, such as informing the general public and being able to safeguard their privacy and safety when utilizing biometrics. Future biometrics research should emphasize different theoretical models and more experimental research, in order to fully investigate the behaviour of citizens in a biometrics context.

Table of contents

1. Introduction

In the past, it was perhaps unthinkable to imagine that a democratic state could ever possess the ability to keep track of its citizens at all times. Nowadays, with the rise of the digital society and industry 4.0, governments have become more and more adept at keeping an eye on their citizens (Levinson-Waldman, 2016). Example given, the American based National Security Agency (NSA) has been known for spying on citizens and even foreign leaders like German chancellor Angela Merkel (The Guardian, 2015). By tapping phone lines and using digital spying software, governments are able to track their citizens more than ever (Zimmer, 2018). However, not just governments use tracking methods for their own gain. It has been identified that big tech companies are tracking individuals as well (Andrejevic & Gates, 2014). Not only do these tech companies use the data generated by individuals to improve their products and services, they also unwillingly make the data available for governments to use it for surveillance purposes (Wired, 2015; Cohen, 2008; Joh, 2016). Government agencies are perfectly able to use the content, that is generated by users of social media platforms, for their own agenda. Therefore, it evident that possessing an online identity is highly susceptible to surveillance, whether that is considered desirable or not.

Nevertheless, the governmental capacity to invigilate individuals is able to reach far beyond the realm of virtual traces. One of these technologies that is rising in terms of both its popularity and use cases is biometrics. Biometrics refers to “automatic identification or identity verification of living, human individuals based on physiological and behavioural characteristics” (Wayman, 2002). With biometrics, it is possible to recognize or trace individuals in all kinds of places on the basis of their physical characteristics. For example, with the use of facial recognition technology or analyzing one’s fingerprint somebody can get access to a building or a technological device such as a laptop (Lyon, 2008). Other use cases include border control and airport security, attendance management, dna matching and voice recognition. However, the information and possibilities that these technologies offer have recently seen a dark side as well. Massive state surveillance programs have surged in China where individuals are being monitored through their mobile phones, with the use of facial recognition technology (Forbes, 2019). Next to that, facial recognition technology is also used in China to monitor whether citizens behave properly and do not break the law in any way. As a result of behaving improperly, in 2020 citizens can be punished by not having access to certain government benefits or services (Liang et al., 2018). Especially because biometrics are not fully developed and researched technology yet, these dangers are right around the corner.

However, citizens have lately become increasingly more aware of the dangers that

biometrics can pose to society. Although biometrics has plenty of use cases and is definitely not used just for surveillance purposes, people are especially worried about the surveillance abilities it possesses (Miltgen et al., 2013). After the controversial introduction of China's Credit Score system, where the behaviour of individuals is monitored and scored (Liang et al., 2018), people have begun to wonder whether biometrics are for the better (CNBC, 2019). Nevertheless, in past studies on biometrics acceptance it has been shown that people are able to see the benefits of biometrics and able to accept the usage of this technology once their privacy and trust needs are met (Miltgen et al., 2013). This possibly indicates that people are not necessarily against the technology itself, but more against the possible violation of their privacy. It is important to study this phenomenon further, as it could reveal the underlying factors behind biometrics acceptance in society. These factors have implications for the future applications of biometrics in society, as both public and private organizations have to realize to what extent people actually desire this technology.

Next to the factors behind biometrics, there are also sociological factors which play a role in the potential acceptance of biometrics technology in society. It was found that, whether a company or a governmental institute initiates a project, there are varying opinions in terms of things like the efficiency and trustworthiness (Hvidman, 2019). There is often a more negative perception of how the public sector handles things such as the implementation of a new technology (Martin & Donovan, 2015), whereas in the case of private companies the potentially negative consequences of the said technology are more easily overlooked (Van Zoonen, 2016). A possible explanation for this difference is the fact that citizens more easily relate a failed project by a seemingly non-profit organization to the public sector and thus the government (Hvidman, 2019). However, these perceptions are not present in every nook and cranny of society. In the study by Hvidman (2019) it was identified that there are particular subgroups of citizens who consistently devalue the efforts made by public institutes. Especially those with pre deposited beliefs regarding public sector inefficiency are more likely to be triggered by cues that seemingly confirm their beliefs. Topics such as red tape, effectiveness and cost orientation are often cues which reinforce these beliefs among this subgroup of citizens, whereas the fairness and equity in terms of individual treatment are perceived to be more favorable among public organizations (Hvidman, 2019)

As previously mentioned, the rise of biometrics technology raises many questions in the public debate and its acceptance is highly disputed among citizens. Issues such as privacy concerns, technology abuse and many more are often addressed by political parties and human rights activists in relation to the rapid distribution of biometrics (Chau et al., 2004). However, some issues in relation to the acceptance of biometrics are not directly noticeable on the surface. First, biometrics authentication is not always what it seems like.

Especially in the first versions of several biometrics applications, false positives were a huge issue. For example, a false positive in an USA crime case has led to arresting the wrong person and keeping him into custody for months, just because the fingerprints were seemingly identical (Lyon, 2008). Next to that, several facial recognition programs have found to be susceptible to differences in lightning and consequently shown to not recognize people because of that (Jain et al., 2006). This also leads to a more negative perception of biometrics as a whole.

Related to this negative perception, one of the most striking tendencies of biometrics is that it has the tendency to discriminate inappropriately and unevenly between one group and another (Muller, 2004; Kloppenburg & Van der Ploeg, 2020). This point has been proven to raise several questions in society, as the notion of classification has often led to discriminatory and racist objectification, whether that was done on purpose or not (Muller, 2004). Especially in terms of power relations, biometrics pose a risk to create unfavorable conditions for those of a non-caucasian background. Example given, back in the days of American colonization a method was used to identify fingerprints on the basis of race. With this method, government officials could see whether one was from a caucasian or a so called ‘’brown’’ background when it came to their subjects (Lyon, 2008). Recently this also happened with the Eurodac (fingerprint analysis) system back in 2006, where some migrants had been searched far more than what was permitted by the Eurodac regulations (Lyon, 2008). Therefore, the exact conditions of biometrics are sometimes skewed in a way where certain racial backgrounds can experience negative consequences.

The final issue with biometrics acceptance is of a more ethical nature. Experts have been wondering whether biometrics pose a cultural and ethical risk in terms of utilizing bodies as some sort of ‘’password’’ (Lyon, 2008). In today’s digital services, information can be stored easily on the cloud and in theory biological information would then be accessible from all over the web. Utilizing these bodies as a password means that bodies themselves are being used and experienced in completely novel ways, which gives rise to certain ethical questions whether this development is for the better. Especially in the privacy domain, many people have shown concerns as to what happens with this information. Classifying populations on the basis of biological components, using them to communicate a certain message and consequently acting upon this message (Ericsson & Haggerty. 1997) is exactly what surveillance is and in particular by biometrics technology. Thus, biometrics also has potential for negative societal implications.

As a result of these issues, government institutes and biometrics companies face a lot of resistance when the topic of implementing biometrics comes up. Most literature studies in the domain of biometrics revolve around acceptance, but with acceptance usually comes resistance. Especially in a sociological context, citizens regularly don’t openly voice their

concerns on an individual basis, but also in the shape of actual resistance movements (Wolfson, 2017). However, both resistance and acceptance are not mutually exclusive (Lapointe & Rivard, 2005). Contrary to popular belief, technology resistance is a more rational process than many people belief. In many cases, technology acceptance relies on the situational context of the technology. For example, when citizens perceive a specific technology as easy to deal with and/or not very intrusive, they are more willing to lean towards acceptance (Demetriadis et al., 2003). Oppositely, when citizens perceive that this is not the case, they are more often found to be even more resisting towards a specific technology. Furthermore, often people are frustrated that they do not have a say in the way technology gets forced upon them, even if this technology possesses the ability to greatly enhance their quality of life. (Ebbers & Van Dijk, 2007). Especially when they do not exactly know how the technology works and what kind of implications it has for their privacy rights. As such, the implementation of new technologies such as biometrics require a sophisticated and nuanced approach in order to guarantee that citizens won't resist them on the basis of fixable issues. Communicating openly about the implementation of new technologies, rewarding citizen suggestions for improvement of the implementation and providing opportunities to learn how to deal with these technologies have shown to combat resistance effectively and are potentially able to pave the way for acceptance (Samhan, 2018). Therefore, when addressing the privacy issues and lack of knowledge regarding biometrics, the government should take a look at previously successful implementation strategies.

However, there is currently not a lot of information available in the existing literature on how citizens relate the acceptance of biometrics to privacy concerns and biometrics informedness. Despite the fact that there is a lot of literature available on the topics of biometrics as a whole or on modern privacy concerns, to our knowledge no study as of now has combined those two into one. Therefore, in this study the emphasis will be put on uncovering the underlying factors behind biometrics acceptance and to what extent people relate their acceptance to privacy concerns. The gap that is present in literature is not necessarily on the individual topics that are being addressed in this study, as there is substantial information on biometrics privacy concerns, biometrics informedness and biometrics acceptance. However, what is currently lacking in literature is the importance of linking these factors together, as these factors do not operate mutually exclusive. For instance, one could be rather knowledgeable and informed regarding the benefits of utilizing biometrics in society, but still not fully accept the usage of this technology due to the fact that it could be extremely harmful for privacy of citizens. The opposite is also potentially true, as people who are completely oblivious about biometrics perhaps do not know that it can have severe consequences for their privacy and therefore don't think that biometrics can pose a threat to society. There are plenty of these individual scenarios possible, but it is currently

rather vague what the bigger relation is between privacy concerns, biometrics knowledge/informedness and biometrics acceptance.

Unraveling the relation between the factors which drive biometrics acceptance and cater to the privacy needs of citizens is of great importance for the future of this technology in society. Next to that, it is important for governments to find out to what extent this technology has to be regulated in order to guarantee the safety and privacy of their citizens, as it is evident that people have privacy concerns about such technologies (Miltgen et al., 2013). Moreover, both tech companies and governments can use the insights of this study to gain a better understanding of human-biometrics interaction. With these insights, the government could properly implement biometrics in a safe and acceptable way for its citizens. Considering these potential contributions, a novel study has to capture the essence of both biometrics acceptance in general and the privacy concerns that people have about such technologies. Therefore, this study addresses the following research question:

''To what extent is biometrics acceptance among Dutch residents dependent on privacy concerns and biometrics knowledge?''

In order to fully inquire into the possible relationship between biometrics acceptance and privacy concerns, the following sub-questions were formulated:

1. ''To what extent are Dutch residents informed about the utilization of biometrics technology in the Netherlands?''

2. ''To what extent do residents of the Netherlands perceive biometrics as a threat to their privacy?''

3. ''To what extent do Dutch residents believe that they accept the utilization of biometrics technology in the Netherlands?''

These sub-questions will serve to cover parts of the primary research question, while the eventual answers to these questions can be analyzed both separately and in relation to each other. The answers to these questions all contribute to the final answer to the central research question. However, in order to properly answer the research question and to validate its contribution to being informed regarding the topic of biometrics, it is important to know to what extent the participants in the sample are informed about biometrics. Accordingly, the first question will revolve around measuring the biometrics informedness of the participants in the sample. In this case, biometrics informedness refers to the extent of

knowledge people have regarding the topic of biometrics and the pros and cons of utilizing biometrics in the Netherlands. For example, if the participants know what the current laws are for utilizing biometrics by the Dutch government and/or companies. This subquestion will address the current knowledge gap by indicating how (a lack of) informedness regarding biometrics can influence one's willingness to accept the utilization of biometrics technology in the Netherlands. The average informedness of a Dutch resident can reveal interesting things in terms of biometrics acceptance. Especially because in the past it has already been shown that a lack of informedness regarding a technology leads to a more negative view, whereas a higher amount often presents a more positive view (Bauer et al., 2007). This could have potential implications for biometrics acceptance as well, as the effects are perhaps the same. Therefore, it is important to fully uncover the relationship between biometrics informedness and acceptance.

The second question is related to the privacy concerns among Dutch residents. As stated before, privacy concerns among citizens are rising due to the unforeseen consequences which technologies such as biometrics can have for society (Miltgen et al., 2013). Inevitably, there exists a need to understand to what extent privacy concerns are related to a specific technology, which in this case is biometrics. Hence, the second question will seek to find out whether resident of the Netherlands see biometrics technology as a possible threat to their privacy. This is especially important for unraveling the factors behind the acceptance of biometrics, as people are showing more and more interest in protecting their privacy and taking the necessary measures to realize this (Bansal et al., 2016). Potentially, this has implications for the acceptance of biometrics technology, as earlier research has pointed out that privacy concerns can slow the process of technology acceptance in general (Miltgen et al., 2013). With the emphasis on privacy concerns, governmental organizations and biometrics companies can make sure to address the needs of Dutch residents in order to safely and responsibly implement biometrics in society. Therefore, this question addresses the role of privacy in technology acceptance.

Finally, the third question will seek to find out to what extent biometrics are accepted by residents of the Netherlands, in order to get a clear picture of the average attitude towards this technology. Acceptance in this case means that people are willing to accept the fact that biometrics are utilized in the Netherlands and see the societal value this technology can have. Acceptance itself is a rather broad term and can not easily be defined by just one or two factors (Miltgen et al., 2013). Factors such as privacy, the added value of a technology and for example even the judicial structure of a country can have a major influence on the acceptance by citizens. An earlier study by Van Dijk et al. (2008) has already shown that the acceptance and usage of a new technology, at least among Dutch residents, usually is a dynamic process which relies on the learning abilities of the individual.

For this matter, privacy concerns and the informedness/knowledge of the technology question seem to be rather important. With a lower amount of informedness, it might be that one will take longer to understand the inner workings of biometrics and how to properly deal with them. Next to that, a high degree of privacy concerns could also potentially slow down this process and therefore disrupt the process of biometrics acceptance in general. Nevertheless, the emphasis of this sub-question solely revolves around the general acceptance of biometrics. Although the data from this component will be analyzes while taking the other two factors into account, the primarily goal of this sub-question is to find out to what extent Dutch residents are willing to accept the utilization of biometrics in society as of now. Thus, this sub-question serves to determine the general end-acceptance of biometrics technology by Dutch residents.

All in all, this paper revolves around the dependence of biometrics acceptance on two important factors: privacy concerns and informedness regarding biometrics. In order to find out to what extent biometrics acceptance is dependent on these two factors, questionnaire-based research was conducted. The ultimate goal of this study is not just to find out to what extent these factors are able to explain a contemporary gap in literature, but also to illustrate how actual human behaviour is able to influence the extent of biometrics acceptance. The adoption of new technologies begins at the very core of human behaviour, not just at a policymaker or technology company forcing it upon citizens. Without the support of a large portion of the citizens, new technologies are doomed to fail (Van Zoonen, 2016). The factors behind the adoption of biometrics are important in a societal context, as addressing these factors could help to introduce technologies such as biometrics in a safe and responsible manner. This way, in the end a solution can be found which satisfies the needs and concerns of citizens, but also allows biometrics technology to function in a socially responsible way.

Eventually, the data that comes from this questionnaire was analyzed in SPSS and revealed several interesting findings regarding biometrics acceptance and the two related factors, which could very much help with the eventual acceptance of biometrics among citizens. As for the paper itself, it is structured in the following way. First, the theoretical section is compiled of several different paragraphs which indicate what is already known regarding biometrics technology, its utilization in society and the way people come to accept new(er) technologies in general. Next to that, these paragraphs also cover the necessary background information on the different biometrics applications in society and will showcase a few theoretical models on (biometrics) technology acceptance. Second, the methods section illustrates which research design was chosen, how the data collection was structured and finally how this data was analyzed. Third, the results section showcases the findings of this research and the way these findings can be interpreted in general. Fourth and finally, the

discussion and conclusion sector will serve as a reflection on the study in general. This section shows what can be concluded from the findings, what these findings mean for future research projects in this domain and how the findings of this paper can be utilized in a practical way.

2. Theoretical section

In this section, the most important theoretical components regarding the topic of this study are showcased and further elaborated. This section illustrates how society has to deal with (unwanted) consequences of the rise of surveillance technologies. Citizens are fearful that these technologies might harm their privacy rights and impair their freedom in society. Especially because of the increasing amount of biometrics applications that are part of our daily lives. These applications vary in their use-cases and to what extent they are able to positively or negatively influence the future of society as a whole. Furthermore, people have varying opinions on the basis of these differences and acceptance of biometrics relies on the context in which these applications are used. Ultimately, this leads to several thoughts on what to expect from research on this subject.

2.1 The rise of surveillance society and biometrics technology

In the current state of the world, more and more technologies are introduced to our daily life. On a daily basis, the number of technologies that play an integral role in our lives increases. Whereas individuals once made use of a horse and carriage to traverse distances, nowadays people can simply use a machine with four wheels to traverse the same distances in a fraction of the time that it took a mere 100 years ago. Nevertheless, the transport industry is just one out of many that have been transformed in the past century. As it stands, some technologies that are being introduced to us are not necessarily for the better. Especially when it comes to technologies that seem to challenge our fundamental human rights, people are not so keen to see them being integrated in our daily lives (Borkovich & Breese-Vitelli, 2014). Governments and companies often promise an integral increase of the quality of life of citizens due to these technologies, but forget to mention that this increase comes with other impactful consequences as well. One such example of a range of technologies that potentially have severe consequences for human rights, is surveillance based technology.

Surveillance based technology consists of multiple different applications, but some of the most widely used ones are surveillance cameras, facial recognition and even internet based surveillance (Reddick et al., 2015). The goal of this group of technologies is to monitor (digital) public spaces and to identify individuals in the open, but its actual effectiveness is heavily debated, but not in terms of its technological capacity (Cayford et al., 2019). The core issues of these technologies lie within the implications that the utilization has for individual rights in society (Cayford et al., 2019). Oftentimes, there is no mutual consent between the government and its citizens when it comes to surveillance. Although most people are aware of the fact that being in public spaces can lead to them being observed by

others, there is still a lack of awareness of why people are being surveilled in the first place. Governments will often claim to use surveillance for a ‘’good cause’’ such as protecting the public against terrorism and crime, but there is no guarantee that this is really the case (Trüdinger & Steckermeier, 2017). Next to that, there is often no profound judicial basis for the use of certain technologies. Consequently, people fear that governments might use these technologies for the worse.

For example in the case of China, mass surveillance programs have been launched to specifically track the behaviour of citizens (Qiang, 2019). When citizens display behaviour that is regarded as unwanted, e.g. they cross a red light in traffic or exceed the speed limit, they will receive punishment in the shape of a lower ‘’social score’’. This social score represents one’s status as a civilian, as citizens with a higher score are deemed as better behaving citizens and enjoy privileges such as a better mortgage or insurances, whereas citizens with a lower social score might for example be prohibited to make use of public transport services (Qiang, 2019). Evidently, this is a dystopian image which likely influences the opinions of people within western society as well (Wijk, 2015). Specifically, similar examples influence the perception of technology in a negative manner (Martin & Donovan, 2015).

As mentioned before, biometrics technology potentially plays a role in the rise of the surveillance society, if not used responsibly. Smart speakers which record and analyze conversations of users are prevalent in the homes of many individuals, governmental institutes that make use of biometric information such as fingerprints to identify individuals and surveillance cameras that identify individuals on the basis of facial information are an integral part of our daily lives nowadays. However, just like with many new technologies, technological development usually takes place at a faster pace than that of the policy makers and politicians who are responsible for a safe and accountable introduction of new technologies in society (Van Zoonen, 2016). Especially because there are many different applications of biometrics technology, it is hard to find an one-size-fits-all solution for the introduction of this technology. Allowing governments to utilize fingerprints as a way of identification does not necessarily justify mass surveillance by cameras with facial recognition components, nor does having a smart speaker in your home justify surveillance by American governmental institutes (Reddick et al., 2015). Thus, biometrics technology needs to be tackled on a componental basis, where individual types of biometrics each get an individual treatment when it comes to laying down the judicial and societal basis for further developing and integrating these technologies.

Nevertheless, biometrics itself is not an inherently harmful group of technologies. In its core, biometrics simply exists to provide solution to real life cases such as identification on the basis of an individual’s biometric data. Although this could potentially be used with

maleficent intent, it does not mean that it always will and should be. In many cases, biometrics is already applied in a useful and rather safe manner by both private and public organizations. Example given, a biometrics start-up called 20face provides users a privacy-proof facial recognition platform with many use cases. Citizens can enter a football stadium on the basis of their facial data, unlock the front door of their home and many other things are possible while using this platform. However, what is the most impressive thing about this platform is that its users are able to delete their data at any given moment and are even able to specify for which use case their data is available. In practice this means that people are fine with opening their front door by showing their face, but still prefer to walk into a football stadium by scanning their ticket. This way, citizens are able to give consent to specific ways of using biometrics in society.

Such usage of biometrics technology shows that the existence of surveillance society and biometrics as a whole can in fact be mutually exclusive. As earlier mentioned, citizens often believe these two to go hand in hand due to the fact that the implementation often does not happen in a proper privacy proof way. However, there are several conditions which can either facilitate or stop biometrics from becoming a surveillance technology. First, the principle of mutual consent is important for many citizens when it comes to technologies such as biometrics (Samhan, 2018). Often, citizens have to find out on their own that their (biometric) data was used without their consent. Consequently, citizens get frustrated and have a more negative perception of such technologies (Van Zoonen, 2016). Without mutual consent, citizens feel like they are being watched and thus consider biometrics as a surveillance technology (Norval & Prasopoulou, 2019). Second, the lack of transparency and insights in how the data of citizens' is used plays a role in the extent to which biometrics is used for surveillance. If citizens generally know how, where and why they are being watched in a certain place, there often is already more understanding for the usage of a technology like biometrics (Demetriadis et al., 2003). Without this transparency, citizens regularly feel as if they are being watched without a solid reason, even if the government claims that its used for example for anti-terrorism purposes.

Finally, citizens are concerned about the fact that the current judicial system does not protect them against potential abuse by biometrics (Liberatore, 2007). In an ideal democratic constitutional state, its citizens have the option to appeal to the judicial system in case of potential abuse by the state. This is one of the implications of living in a democracy, which is why citizens fear that their democratic rights are at stake when the law does not protect them against potential biometrics abuse by the government and/or private companies (Liberatore, 2007). In a political administration with no regard to individual freedom and human rights, biometrics might be more easily used as a surveillance technology in society. Without the introduction of laws which protect the individual democratic rights and liberties of citizens,

surveillance technology can possibly be utilized for oppression of individuals.

2.2 Mainstream biometrics applications

Evidently, biometrics is a rather diverse group of technologies with potential for both the good and the bad, it is important to consider the strengths and weaknesses of each and every form of biometrics (Jain et al., 2006). For example, signature or keystroke recognition might be very cost efficient biometric applications, but they lack the absolute security and accuracy that for example facial recognition has to offer. In other words, there is no omnipotent application of biometrics, although a number of them have a wide variety of possible applications in society (Jain et al., 2006). Consequently, the suitability of a specific form of biometrics depends on the requirements of a certain application and the properties that a single form of biometrics can offer. Currently the following forms of biometrics are being used in society:

Facial recognition: Facial recognition refers to the recognition of humans on the basis of their facial characteristics. This form of biometrics is usually utilized in order to identify specific individuals in a larger crowd and/or to verify one's identity in order to gain access to something. At the moment, facial recognition technology is primarily done by either locating the distinct features of one's face (e.g. the nose, mouth, eyes etc.) or by analysing the overall characteristics of one's face, which is seen as a weighted combination of a number of canonical faces (Li & Jain, 2011). Nowadays, facial recognition technology has been shown to operate under different illumination conditions and recognize small pixels in one's face, which is an upgrade over the past versions where a lack of light could pose a problem (Jain et al., 2006).

Fingerprint analysis: In biometrics, fingerprint analysis is a relatively common method for identification and matching purposes. For many decades, this method has been in use by for example the police and also more and more digital services start making use of fingerprint analysis for authentication purposes, as the accuracy of this method is very high (Maltoni et al., 2009). The typical way fingerprint analysis is done, is on the basis of the pattern of ridges and valleys of the fingertip. This is different from each and every individual, which makes it the perfect and easy to use for authentication purposes. Nowadays, a fingerprint scanner costs less than 20$, which makes it easily affordable for many organizations and companies as well (Jain et al., 2006). The only issue with fingerprint analysis is that it requires extensive computational resources to work properly. Next to that, fingerprint analysis is susceptible to biological changes to the fingers such as aging, diseases, cuts and bruises and other genetic and environmental factors (Jain et al., 2006).

Hand geometry: Hand recognition systems base their identification process on several measurements taken from the physical characteristics of one's hand, such as its shape, the size of the palm and the length and the width of the fingers. On a commercial basis, hand geometry is commonly applied as it is a relatively simple method and also rather cost efficient. Commonly known issues with hand geometry are the fact that it does not hold up so well with biological factors such as aging and limitations in hand movements such as arthritis. Next to that, these devices usually do not work on regular laptops and computers due to the large size of computation power that they require.

Iris recognition: As part of the eye, the iris is the iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side (Jain et al., 2006). The nature of the iris is very complex and distinctive, which makes it useful for personal recognition and authentication purposes (Daugman, 2003). Currently, iris recognition is rapidly developing and its accuracy and applicability in many use cases makes it a promising technology for the long term. Newer systems have proven to be more cost efficient and user friendly as well. The only issue that currently exists with iris recognition is that the false reject rate of these systems can be a bit on the high side (Jain et al., 2006).

Keystroke pattern: This form of biometrics is on the new side and still a very controversial pick when it comes to its applicability. It is hypothesized that every person has a unique way of typing on a keyboard, which is the basis of this form of biometrics (Jain et al., 2006). However, it does not necessarily mean that people can not have a similar way of typing, as this method would mostly be used for things like identity verification. Nevertheless, this method requires a strong continuity of a person's way of typing before it works efficiently, which makes it partly unreliable.

Signature recognition: The least reliable method of biometrics currently into existence. Although signatures are widely accepted as a manner of personal identification and distinction, it is being replaced on a large scale by more reliable methods of biometrics. The biggest issues with signature recognition include susceptibility to professional counterfeit devices, the lack of continuity among individuals as every signature differs at least slightly from another and they are influenced by the physical and emotional conditions of the signatories (Nalwa, 1997).

Voice recognition: Voice recognition has risen to the mainstream after big companies such as Google and Apple have been incorporating this technology into their devices. Smart home speakers rely on voice input and even Apple's iPhone has plenty of voice-based functions in its arsenal. The reason this technology has been growing in popularity is primarily because of the biological components of ''voice''. Voice is a combination of physical and biological characteristics, as the features of an individual's voice are based on thing like the shape and the size of the appendages that are used in the

synthesis of the sound (Jain et al., 2006). Disadvantages of this technology include the susceptibility to biological conditions such as aging, consequences of smoking, emotional state but also relatively common medical issues such as a flu or common cold. Therefore, it may not be a very appropriate technology for things like identity verification.

2.3 Citizen opinions about biometrics: privacy issues and informedness

Now that biometrics applications come in different forms and are more prevalent in society than ever, it is necessary to understand the citizens' views on governmental and commercial surveillance that takes place through the utilization of these applications. As both governments and companies have the ability to massively analyze data, citizens are often confused and feel left behind, as their opinions are rarely taken into account for these matters (Reddick et al., 2015). Instead of finding out to what extent citizens are willing to accept a certain technology in advance, politicians and companies often first decide to facilitate the development and integration of these technologies. Consequently, when citizens voice their concerns, these same politicians and companies frequently fail to see where these concerns come from (Webster, 2012). If governments and perhaps companies want the full support of their citizens with regard to biometrics technology, it is of utmost importance to take the public opinion into account (Martin & Donovan, 2015). Without citizen support, these technologies will never be fully accepted.

When it comes to biometrics, there is variation in the concerns that arise from the public views of citizens. Prabhakar et al. (2003) found that citizens especially put an emphasis on the reliability of the data that emerges from biometrics. Citizens seemed to have less faith in data that came from iris scans, whereas data coming from facial recognition was deemed to be more reliable. Nevertheless, it is often hard for ''regular'' citizens to uncover the actual differences between these technologies and what these differences imply for potential changes in their daily lives. Especially because the average citizen might not be well-versed in reading scientific literature on these new technologies , does not keep up with the developments of new technologies or works with these technologies in their daily lives, it is hard for them to fully grasp the consequences (Martin & Donovan, 2015). This deficit in knowledge can lead to unwanted consequences for citizens. Scientists and policy makers are often aware of the knowledge-gap, but don't address it accordingly. As a result, people remain uninformed and unaware of the pros and cons of new technologies (Bauer, 2009). This is extremely detrimental for the public opinion of a technology such as biometrics, as the people in charge for the introduction of this technology are not on the same page with regular citizens. Potentially, those in charge could ignore the views of citizens as a whole (Martin & Donovan, 2015).

Given that people might not get a fair chance to form a neutral opinion about

biometrics, it is understandable that the debate regarding the acceptance of biometrics will sway in a certain way. However, if governments and companies manage to increase general awareness and knowledge regarding biometrics among citizens, this could prove to be very positive for the public opinion about biometrics (Martin & Donovan, 2015). It has been shown that an increase in knowledge and awareness regarding a technology has resulted in a more positive attitude among citizens (Bauer et al., 2007). The more informed the general public is, the more inclined they are to support scientists and tech developers in their work. It is especially important to get a positive attitude at first, because once trust in a certain technology is lost and a negative opinion is formed, it is rather difficult to reshape it to a positive attitude (Martin & Donovan, 2015).

However, the informedness of the general public is just one part of the acceptance of new technologies, as informedness is not able to solve all of the issues that a new technology can bring. For example, new technologies sometimes have unintended consequences for individuals such as undesirable reliance on these technologies (Dalcher, 2007), a loss of social skills (Zheng & Lee, 2016) and a lack of privacy and digital security (Hallinan et al., 2012). Especially the latter issue has been increasingly more important, as politicians and other governmental institutes such as the EU have already emphasized the importance of data and privacy protection (Linden et al., 2020) However, privacy is a hot topic not just in literature and governmental institutes, but also on an individual level. More and more citizens have begun to value the protection and anonymity of their data and demand the judicial system and the government to protect them from unwanted consequences (Hallinan et al., 2012).

Then again, privacy itself is a difficult concept. Especially in the current societal context, privacy has evolved into something far bigger than it once used to be. Just a few decades ago, individual privacy was more something along the lines of ‘’a state in which one is not observed by other individuals’’ (Ware, 1993). In a sense, this still holds up, as most people don’t enjoy continuous observation by other individuals and as a consequence withdrawing in one’s own home with the curtains closed can induce a very safe and private feeling (Petronio, 2002). However, in the digital society as we know it, traces of an individual’s thoughts and action can often still be found online (Cullen, 2009). Visiting certain websites or searching for specific queries on google leads to this information being stored on the world wide web (Bennett, 2001). Once an individual has searched a few times for the newest model of the Volkswagen Golf, it is very likely that this individual will constantly be reminded of the fact that one has shown digital interest in this specific car, often in the shape of advertisements or biased results when utilizing search engines. One can take measures such as using a VPN to browse the internet and even if that is considered to be a drastic measure, most browsers nowadays offer an option to browse anonymously. Yet, this is not

always enough to fully safeguard one's privacy.

Some technologies are more intrusive in terms of the way they collect an individual's data. For example in the case of biometrics, if an individual walks around the street and a camera utilizes facial recognition to see which specific individuals are currently on the streets, this person can essentially not do anything about the fact that they are being surveilled. Especially because some recent facial recognition companies are even able to figure out an individual's identity while they are wearing some sort of mask (Telegraph, 2020). Another example is the case of smart speakers. These speakers utilize voice input to function, which means that they are always listening to conversations that take place in their vicinity. What's striking however, is that the developers of these applications often listen to these conversations as well (Lau et al., 2019). Often, the developers of these speakers will claim that this is solely for improvement purposes, but several experts have shown to question whether that is completely true. Furthermore, the fact that a company can get so easily away with such privacy infringement, does not seem very appealing to many individuals (Scott et al., 2005). Especially considering that if a company can already infringe upon an individual's privacy so easily, a government could potentially abuse such technologies even more.

Subsequently, most people are not very fond of the thought of new technologies endangering our privacy even more. It was found in multiple papers that citizens are rather skeptical about the introduction of new technologies which, potentially speaking, could have negative consequences for individual privacy (Cullen, 2009; Miltgen et al., 2013; Bansal et al., 2016; Reddick et al., 2015; Van Zoonen, 2016). Although most citizens have some sort of concerns for their privacy, the nature of these concerns seems to differ among several groups of citizens. For example, Cullen (2009) has found that there are differences between more individualistic and collectivist cultures when it comes to their privacy. Previous research shows that individuals who operate in an individualist culture seem to possess higher levels of trust towards others, unless they have reasons to show distrust, whereas those from a more collectivist culture show more distrust in general towards out-group members. From a privacy point of view, this could mean that in individualist cultures people are more likely to distrust for example companies or the government with their data, as they realize that their individual sense of worth could be harmed. On the other hand, individuals within a collectivist culture potentially do not distrust companies or governments that much with new technologies, given that they are members of the in-group. Especially because in collectivist cultures there is a strong sense of sharing, nurturing and supporting those who are part of the in-group (Cullen, 2009).

Another interesting finding in literature is the way in which there is a substantial paradox in citizens' privacy concerns. Although many people display concerns for their

privacy, most people still use the same password for many digital services and statistics show that 1234 remains the most used pin code for debit and credit cards (Van Zoonen, 2016). Next to that, individuals share sensitive and personal information on open platforms such as Facebook and Twitter. In literature, this phenomenon is called the ‘’privacy paradox’’ (Young & Quan-Haase, 2013). People are convinced that they are in control of what they post and the implications this has for their privacy. However, it is often unknown to them that their digital traces can be stored by companies and their data can be utilized for other means than for example analyzing individuals who like cat videos on a social media network (Van Zoonen, 2016).

Nevertheless, in general there are three consistent factors which trigger most people’s privacy concerns; the type of data, the purpose of collecting and utilizing this data and the people or organizations which collect and utilize the data. In terms of data types, it was shown that individuals are more sensitive about medical and financial data than for example one’s age and gender (Van Zoonen, 2016). However, demographic variables are used more and more by governments to classify specific groups, which leads some citizens to believe that even this data is not safe from being abused (Ju et al., 2018). As for the purpose of the data collection, people are rather picky in terms of what they deem acceptable. Generally speaking, citizens dislike the fact that sometimes data is used for things other than the initial purpose of the data collection (Van Zoonen, 2016). Finally, citizens have shown to put different levels of trust in individuals and organizations who collect their data. On the high end of the spectrum are usually institutes such as hospitals and banks, but on the lower end social media and telecom companies can be found to have a low level of public trust (Van Zoonen, 2016). Although generally speaking perceived as a more trustworthy entity, numerous government institutes have shown to handle data collection quite badly and therefore trust in those has decayed in the past years (De La Robertie, 2019).

2.4 Acceptance of biometrics technology

The acceptance of biometrics technology is still a rather controversial topic in society. On the basis of the aforementioned issues, a large portion of society is skeptical about the introduction of such technologies (Miltgen et al., 2013). The utilization of biometrics is already widely available in society beyond its initial goals such as border control and identity verification (Norval & Prasopoulou, 2019). For example, owners of modern day phones happily make use of biometrics to utilize their phones for all sorts of reasons. Such phones utilize fingerprint analysis, voice recognition and face recognition technologies for things like debit card payment, identification verification and access to the world wide web (Norval & Prasopoulou, 2019). However, once these technologies are not utilized for individual use but

on a larger scale such as governmental surveillance, people come to realize that they might not accept certain use-cases of biometrics (Van Zoonen, 2016). Acceptance of technologies might not always be as straightforward and simple as thought by those responsible for the introduction of these technologies in society. Oftentimes, the context is also highly relevant for individuals whether to accept this technology or not (Norval & Prasopoulou, 2019). Next to the context, there are also more consistent and omnipresent factors when it comes to deciding whether one accepts a technology or not. One such model which illustrates this process, is the Technology Acceptance Model (Lala, 2014).

The Technology Acceptance Model (TAM) provides a rudimentary framework which simplifies the process of how potential end-users of a certain technology come to see value in it and ultimately come to accepting the technology as a part of their daily lives (Davis, 1989). Although the TAM is sometimes considered as a rather simple sketch of reality, its parsimonious nature has been proven to be valuable in studying the intent to accept new information technologies in a wide variety of contexts (Miltgen et al., 2013). Especially because the TAM considers many psychological factors that are relevant for the way in which people come to accept technology, it has been able to become an influential model in the field of IS. (Lala, 2014). In the past decades, the TAM has been revised several times, primarily to fit the context of different fields of research (Venkatesh & Bala, 2008; Lala, 2014). However, for several reasons, the most known and used version of the TAM will be applied in this study, which is the original version by Davis (1989).

First of all, the TAM model by Davis presents a rather simple and applicable view of technology acceptance, which is utilized in many studies in the fields of information systems and even psychology or public administration.. Compared to the model by Venkatesh and Bala (2008), the model by Davis is much less complex. However, a complex model is in this case not very desirable. Surely, some aspects of the model by Venkatesh and Bala could prove to be relevant for biometrics acceptance in general. Yet, these would not necessarily contribute to the main goal of the study, as the goal is to find out to what extent biometrics privacy concerns and biometrics informedness have an impact on biometrics acceptance. With this goal in mind, it is more desirable to have a clear and perhaps a parsimonious model in mind for the biometrics acceptance component, as this acceptance is already being linked to two factors; biometrics informedness and biometrics privacy concerns. Secondly, the surveys which were used as a basis to compile this study's questionnaire mostly used the original TAM model as their basis. Using a newer model such as the one devised by Venkatesh and Bala would perhaps not present a fair and valid view on biometrics acceptance, as this model is far more complex and could have different implications for the results of our questionnaire's biometrics component. Finally, the model by Venkatesh and Bala might seem more complex and thus some researchers would argue that it could

present a more realistic view of technology acceptance, but the biggest emphasis of this model is put on workplace acceptance and technology integration. In this study, the emphasis is put on citizen perceptions on biometrics acceptance. This emphasis aligns more with the original model by Davis, as it is a more general and robust model which can also be applied in a sociological context. Therefore, the model by Davis was deemed as the most fitting version of the TAM model for the context of this research.

The TAM model by Davis revolves around the notion that people's decision to make use of a certain technology is influenced by two main principles: perceived usefulness and perceived ease-of-use. Perceived usefulness can be described as *"the degree to which a person believes that using a particular system would enhance his or her job performance"*, whereas perceived ease-of-use refers to "the degree to which a person believes that using a particular system would be free from effort" (Davis 1989, p.320). The sum of these two factors has been found to ultimately influence the attitude of potential end-users towards the technology itself. This can be seen as the basis for any behavioral intention to make use of a specific technology. Nevertheless, the extent of perceived usefulness also has a direct influence on the behavioral intention, as can be seen in figure 1.

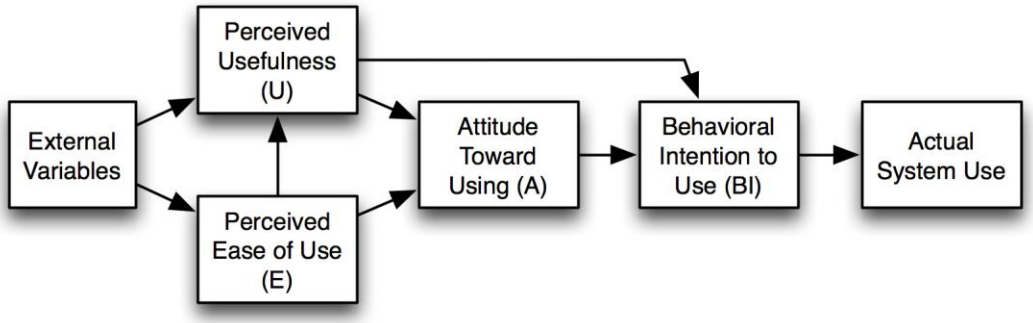


Figure 1. The Technology Acceptance Model by Davis et al. (1989)

According to Davis (1989), there are several determinants which describe the extent to which an individual perceives the usefulness of a certain technology. First, the perceived ease-of-use of a product is highly influential on the perceived usefulness of a certain technology. If a technology is not easy to use or easy to learn, people are inclined to believe that this technology will not be useful to them (Davis, 1989). Second, the subjective norm that exists around a certain technology is important to individuals. If the people that are considered important to an individual do not accept a certain technology, that individual is more inclined to refuse the acceptance of this technology (Davis, 1989). Cognitive processes are not the only thing that influences perceived usefulness, as social factors are deemed

equally important. Third and related to this is the image that using a certain technology produces. More specifically, the image is related to the degree to which an individual perceives the usage of a specific technology to raise one's social status (Davis, 1989). For example, Blackberry attempted to appeal to this determinant by trying to create a ''businessman'' aura surrounding their phones (Business Insider, 2019). Fourth, the job relevance that a certain technology can have for an individual is relevant for the perceived usefulness as well. If an individual believes that a certain technology might not be applicable to one's job at all, this person will be less likely to use it (Davis, 1989). Nowadays, almost everyone uses a computer or laptop device at work for a large amount of tasks, but in the past computers were so big that they had the size of a small elephant. Therefore, they were not used as much because people believed that such a big device was not relevant for their personal usage. Fifth, the output quality is of crucial importance to the usefulness of a system. If a technology does not perform well enough to produce the desired outcomes, it will simply not be used anymore after a while (Davis, 1989). Finally, the results of a specific technology's usage should be demonstrable. A system can produce very good results and do exactly that what is expected of it, but it should also be easy to find out where these results come from and how to present them to a larger public (Davis, 1989).

Additionally, there is a visible trend in literature and practice that technologies that are hard to use or learn do not survive as long as those which are significantly easier to learn and make use of (Venkatesh & Bala, 2008). It is not entirely random that many big companies have begun to recruit UX/UI designers into their ranks, as research has shown that this is a crucial factor for the retention of customers and users in general (Ashraf et al., 2016). Next to that, a system should also not be tedious to use. Systems that require a lot of actions before you finally get what you want are often also neglected after a while of using them. Simple and intuitive technologies thrive, whereas complex systems with a heavy learning curve do not (Venkatesh & Bala, 2008). Interestingly, systems that have some degree of a ''fun factor'' embedded into their usage also seem to perform better in terms of technology acceptance (Venkatesh & Bala, 2008). The perceived enjoyment of individuals potentially makes it easier for them to learn how a system works and to continuously make use of it.

Undoubtedly, a widely renown and commonly used model like the TAM attracts both positive and negative criticism from researchers across the globe. The TAM has especially been successful in its field due to the fact that it is rather simple, which makes it very applicable in several different contexts (Venkatesh & Bala, 2008). Concepts like perceived usefulness and the perceived ease-of-use are widely applied in the context of new technologies and sometimes religiously utilized by UX/UI designers in the field. However, often researchers and technology professionals forget to consider the actual contribution of

this model in their work (Ajibade, 2018). In the first place, the TAM sometimes fails to concretely predict human behaviour in the context of new technologies (Hai & Alam Kazmi, 2015). The simplicity of the model might be considered useful in many cases, but for studying the actual behaviour of humans it can be quite lacking. Evidence from literature indicates that the TAM is not able to provide sufficient information regarding social factors which influence technology acceptance (Torres & Gerhart, 2019). Furthermore, the external variables in the TAM are not properly addressed according to several scholars (Ajibade, 2018; Napitupulu, 2017; Persico et al., 2014). Factors such as age and education level can play a big role in the individual acceptance of a new technology, but these are not properly taken into account in the model (Persico et al., 2014).

Albeit most of this criticism is justified in its own way, the TAM does provide a relatively omnipotent and applicable model for explaining a significant portion of the factors which are relevant for technology acceptance (Venkatesh & Bala, 2008). In literature, there are already plenty of studies which investigate the role of external variables such as age and educational level in the acceptance of technologies. The strengths of the TAM primarily lie in the fact that it properly outlines the influence of human perception on technology acceptance. Factors such as the perceived usefulness and the perceived ease-of-use of a technology are important for individuals when it comes to accepting new technologies such as biometrics (Miltgen, 2013). Especially for such publicly debated and privacy-sensitive technologies like biometrics, people often question what is in it for them to make use of something so controversial. When there is no socially justified use-case or if the learning curve of using biometrics is too steep for most individuals, it could be that they won't even consider using or accepting biometrics. In this case, external factors such as age and educational level are merely a side issue. This was already found in the research by Miltgen et al. (2013), as factors such as perceived usefulness and the ease-of-use had a significant impact on the eventual acceptance of biometrics technology. Thus, the criticism on the TAM might be justified, but it does not completely devalue the usage of the model in a scientific context. Moreover, especially for a group of technologies like biometrics, the factors which are pointed out by the TAM can prove to be very useful for understanding the process of acceptance among citizens.

In a study by Krempel and Beyerer (2014) it was shown that the TAM can also be applied in the context of surveillance technologies. Especially the perceived usefulness factor seemed to have a significant positive impact on the personal acceptance of a surveillance system. Once people were convinced of the usefulness of a surveillance system, people were more willing to accept the placement of this system in general (Krempel & Beyerer, 2014). However, the overall emotional attitude towards these system was by far the most influential factor in terms of the overall acceptance. It was found that this factor was

also influenced by related factors such as the perceived risks of a surveillance system the the transparency of the data it produced. Interestingly, the emotional attitude of participants was negatively influenced by the perceived risks. People who perceived to be personally at risk by surveillance technologies had a far more negative perception of these systems in general (Krempel & Beyerer, 2014). Although biometrics technology is not the same as surveillance systems and has definitely got more use-cases than simply surveilling individuals, the results of this TAM-based study are in line with the previous findings in the field of biometrics. Previous studies have found that seeing the usefulness in biometrics is able to positively influence one's attitude towards biometrics at the hand of rational justification (Miltgen et al., 2013;Chau et al., 2004), whereas privacy concerns often invoke a more emotional response which leads to a more negative view on biometrics (Miltgen et al., 2013; (Norval & Prasopoulou, 2019). Moreover, biometrics resistance can be lifted when people perceive the technology to have an added value. This indicates that the TAM model is able to sketch important components of human behaviour under (potential) surveillance by certain technologies.Therefore, the TAM model is very much applicable for technologies in a potential surveillance context and can thus be utilized for biometrics-based research as well.

2.5 Hypotheses

As this study will be of confirmatory nature, several things were hypothesized on the basis of the findings of earlier biometrics research in the theoretical section. In the first place, it was hypothesized that having privacy concerns leads to a lower level of biometrics acceptance in general (Chau et al., 2004). In a western country like the Netherlands, individualist culture thrives, which implies that citizens might show a larger distrust towards those who can potentially harm them (Cullen, 2009). Next to that, a significant amount of people perceives that biometrics is something beyond their own control, which leads them to believe that once abused, it has severe consequences for their freedom and privacy (Van Zoonen, 2016).

Finally, earlier research shows that people who are more knowledgeable about new technologies, for example biometrics, are more willing to accept biometrics as a future component of society (Miltgen et al., 2013). Knowledge and some extent of technological literacy seems to be an important part of accepting certain technologies in one's life, as most people who don't have access to this knowledge are not as able to form a profound opinion on such matters (Martin & Donovan, 2015). Related to that, a lack of knowledge has even been found to negatively influence the acceptance of a technology in general (Bauer et al., 2007). Especially because biometrics technology in its current shape is relatively new to most citizens, it could be that they are more fearful towards biometrics.

3. Methods

The purpose of this section is to showcase the research methods that were used to get the best possible answer to the research question at hand. Furthermore, this section consists of the methods for the research design, data collection process, the recruitment of participants and ultimately how the data was analyzed. The choices that were made for these specific components will be substantiated in the following paragraphs. Finally, this chapter serves to increase the transparency and the reproducibility of this study by carefully elaborating the whole research process.

3.1 Research design

For this study, a quantitative approach was utilized, with the extent of biometrics informedness of Dutch Residents and their extent of biometrics privacy related concerns as independent variables and the extent of biometrics acceptance as the dependent variable. As based on the theoretical framework, it was shown in earlier studies that biometrics acceptance is influenced by privacy concerns and biometrics informedness (Miltgen et al., 2013), but the actual statistical dependency is often ignored and not properly investigated. As a result, a quantitative approach with a profound empirical basis is necessary to investigate this relationship. Next to that, the central research question in this thesis is of confirmatory (hypothesis-driven) nature, which can best be answered by quantitative data analysis, as a quantitative approach helps in this case because it allows one to statistically analyze the opinions and/or perceptions of a relatively large amount of participants in the sample. This method is the opposite of a qualitative approach, as qualitative is better tailored towards smaller N-size samples and does not provide any numerical evidence other than frequency analysis for its findings (Verhoeven, 2018).

Taking these considerations into account, a 2(Biometrics knowledgeability/informedness & privacy concerns) x 1(Biometrics acceptance) cross-sectional quantitative design was used in this research, solely using data from a within-subjects basis. In order to fully observe to what extent the level of biometrics acceptance among residents of the Netherlands is related to potential privacy concerns and their informedness regarding biometrics as a whole, a questionnaire was utilized in order to gather the necessary data. questionnaire-based research allow allows a relatively large sum of respondents to state their opinions and preferences regarding a certain topic (Verhoeven, 2018). On the basis of these opinions, statistical relationships can also be determined between constructs. Especially because in this research the emphasis is put on uncovering the statistical relationship between biometrics informedness, privacy concerns and

biometrics acceptance, it is important to pick a research instrument which allows for profound analysis of multiple constructs at once. Next to that, a qualitative analysis with a large N size sample is rather time-consuming and does not present profound statistical evidence surrounding its findings, quantitative analysis was also determined to be the better option in this research. Furthermore, given the time constraints and the fact that this research is carried out as a master thesis project, survey analysis was partially also conducted because of its efficiency in terms of gathering data on a larger N size sample.

Related to that, the residents of the Netherlands in the sample will serve as the units of observation. Residents of the Netherlands were chosen on the basis of two important considerations.The first one is that Dutch residents deal with contemporary western society and its technological developments on a daily basis. The Netherlands can also be described as a rather liberal country (te Velde, 2008), which makes it more plausible that citizens are more wary of technologies that threaten their individual liberty and rights (Van Zoonen, 2016), thus making it a rather interesting target group to analyze in a biometrics context. Secondly, due to the fact that the researcher is carrying out this research in the shape of a Dutch master thesis project, it was relatively convenient to study citizens of the Netherlands. Simply speaking, it would be far more complex and time-consuming to gather insights from a large and diverse group of (European) countries.

3.2 Data collection

In order to collect data, participants were able to express their privacy concerns and extent of biometrics knowledgeability and acceptance by answering the questions from a survey. This survey (Appendix A) was constructed with the online survey creation platform called Qualtrics. The demographic questions of the survey were taken from a standard format for survey research, which includes questions such as *What is your age?* and *What is your current primary occupation?*. In the rest of the survey, theories from psychology, information systems and public administration were combined to understand the relationship between biometrics acceptance, privacy concerns and biometrics informedness. More specifically, existing questionnaires were used per component to guarantee as much reliability and validity as possible (Verhoeven, 2018). In order to guarantee a respectable level of reliability and validity of the study, previously used surveys in the domain of technology acceptance were used as the basis for the survey questions. These are all previously tested and validated surveys that were utilized in peer reviewed articles. Furthermore, contextual elements from other peer reviewed articles in the biometrics domain were also used in order to preserve the relevance of the devised questions. Many of the items in these questionnaires fit the premise of the research, as they were taken from biometrics-based studies.

Initially, the questionnaires that were used as a basis of inspiration for constructing the survey had too many similar items to incorporate into a single survey. Based on the literature and the similarities within the previous works, in total 42 items were chosen to be part of the final survey which was distributed. To answer these items, respondents indicated to what extent they agreed on a scale from zero to ten (0 = completely disagree, 10 = completely agree). Ultimately, these items were not tested and/or modified on the basis of the feedback of a pre-test. Although it could have potentially led to an increase in relevant items and/or the modification of a few items, the researcher decided not to work with a pre-test before distribution of the actual questionnaire. This consideration was made as this research was carried out in the shape of a master thesis project, which had to deal with some unexpected circumstances that led to a delay in the data collection process. Therefore, the instrument which was distributed to the participants in the sample is the very first version of the in this study devised survey.

3.3 Survey construction

The biometrics informedness component was deeply influenced by previous work of Miltgen et al. (2013), as they have constructed a biometrics acceptance survey on the basis of earlier peer-reviewed work. This component was measured using eight items, with both novel items and items from the work of Miltgen et al. (2013). This survey was utilized especially cause it features previous work on the topic of biometrics informedness and acceptance. As identified in the literature, the average (western) citizen is often not very informed regarding new technologies such as biometrics (Bauer et al., 2007; Martin & Donovan, 2015). Given the fact that this also influences people's perception on biometrics, specific items from the survey of Miltgen et al. (2013) were used to determine whether people are informed about how biometrics is utilized in society, its potential benefits, how the judicial system is able to protect them against abuse and more topics related to biometrics informedness. In the end, these items offered a profound view on the extent of the biometrics informedness in the sample, as they directly stem from earlier used questionnaires and relevant issues in the domain of biometrics informedness research. Ultimately, this component's items were each rated on a scale from zero to ten (0 = completely disagree, 10 = completely agree). Examples are *I am familiar with biometrics and how it is currently used in society* and *I know a lot about different biometrics applications*. The mean score of these items can be used to measure the average biometrics knowledgeability/informedness of the respondents.

Next to that, the privacy component was shaped alongside the Privacy Attitude Questionnaire by Chignell et al. (2003) and the Need For Privacy Instrument by and Trepte and Masur (2017). This component was measured using 21 items, with both novel items and

items from the aforementioned works. These two questionnaires are well-known in the field of privacy research and their items were slightly adapted to fit the context of biometrics research. Especially since many privacy-based surveys are not necessarily targeted towards biometrics or technology in general, this was necessary to make the questionnaire fit with the premise of discovering the relationship between privacy concerns and biometrics acceptance. As such, the privacy component has general items regarding privacy but also some that are more tailored to the subject of biometrics. Next to that, the component also offers participants to distinguish their concerns regarding different types of biometrics applications, as there are differents to what extent they can be implemented in society (Jain et al., 2006). The questionnaire's items were each rated on a scale from zero to ten (0 = completely disagree, 10 = completely agree). Concrete examples of items are *I am comfortable with providing my data to biometrics companies* and *I believe that the government can be trusted when they utilize biometrics in society*.

Ultimately, the biometrics acceptance component was constructed by taking inspiration from the works of Miltgen et al. (2013), Park (2009) and El-Abed et al. (2010). This component was measured using 13 items, with both novel items and items from the aforementioned works. The aforementioned works contain items related to the TAM model and (biometrics) technology acceptance in general, which were slightly changed to fit the context of biometrics research. The main goal of this component was to measure the acceptance of biometrics in society, which in turn could be related to the outcomes of the privacy and the informedness components. Consequently, some of the survey items were adapted to be more relevant for the main research question. Most of these items were previously used in prominent technology acceptance studies, but in this study the word technology is often changed to ''biometrics'' or ''biometrics technology''. As acceptance is a rather broad term, many factors behind technology acceptance were considered when devising the survey. Examples of such factors are the perceived usefulness, perceived ease-of-use, trust, transparency but also more minor factors like a technology's fun-factor.
The items of this construct were each rated on a scale from zero to ten (0 = completely disagree, 10 = completely agree) as well. Some examples of these items are *I believe that it will be easy to learn how to deal with biometrics technology* and *I put my trust in biometrics*.

3.4 Participants & Distribution

This survey was distributed during the period of the 18th of may until the 10th of june. This distribution period resulted in a rather diverse group of participants within the sample. Originally, 80 participants were part of the sample. However, due to incomplete answers in the data, 6 of them were removed. As a result, the group of participants consisted of 74 people with a mean age of 28 (*SD* = 11.5, range 18-63). 45 were male and 29 were female.

Furthermore, 41 participants have the Dutch nationality, 23 participants have the German nationality and the other 10 specified to have a different nationality.

Possibly, the high standard definition in terms of the sample's age can be explained by the sampling method, as recruitment of the participants primarily happened through the personal network of the researcher and on the online research participation platform of the University of Twente, which is also known as SONA. As a result, a large portion of the sample is either a student or a regular citizen of an age of over 30. Therefore, the sampling method can best be described as convenience sampling. This sampling method was utilized as the research takes place in a master thesis context with a specific time-constraint in which the data collection process has to take place. As a result, there was no sufficient budget or time to properly gather hundreds or potentially even thousands of respondents in the sample. However,given the limited resources of the researcher, the final sample can be considered somewhat representative for the target group, as there are still differences visible in terms of educational level and age.

In any case, the participation requirements of this study allowed Dutch residents from many different age, ethnic and occupational backgrounds to participate in the study. Specifically because the inclusion criteria of this study were; being able to understand written English properly, being able to read, not having any physical deficiencies which could hinder participation and finally being a resident of the Netherlands. These criteria are rather inclusive, as most Dutch residents would potentially be eligible to participate in the study. However, a downside of this sampling method is that potentially non-Dutch residents could have taken part in the study, as there was no physical or digital verification of their citizenship status. Nevertheless, geographical data of the participants showed that most participants filled in the survey from the Netherlands, which makes it more probable to assume that they are permanent residents of the Netherlands.

Finally, the sample data was kept until the 31st of august, in order to allow the researcher to finalize the paper and use this data for analysis purposes. The data was fully anonymized and stored on both the laptop of the researcher and the online qualtrics platform. After the 31st of august, data was removed from both platforms in order to safeguard the privacy of the participants within the sample. Ultimately, the data was solely used for analysis purposes and not spread to any third parties. Before participation, participants gave their consent to the researcher to use their data for research purposes only.

3.5 Data Analysis

The literature review in the introduction and the theoretical section allowed for a thorough understanding of the important components of biometrics acceptance among citizens. It was identified that, next to the already known and meticulously researched components of biometrics acceptance, the extent of one's privacy concerns and biometrics informedness potentially have an influence on biometrics acceptance as wel (Miltgen et al., 2013). More specifically, the hypotheses of this study state that it is expected that a higher level of biometrics informedness leads to more acceptance, whereas a higher level of biometrics privacy concerns leads to less acceptance. In order to find out whether these hypotheses can be confirmed or not, the data from the survey which was mentioned in the previous paragraph was used.

As a manner of properly analyzing this data, the survey was exported from Qualtrics to the data analysis software named SPSS. This software contains many different statistical functions which can show the statistical relationships between several types of data. Due to the quantitative nature of the survey and its data, several analyses were performed on the basis of quantitative data analysis methodology. In order to investigate the reliability of the survey that the participants filled in, a cronbach's alpha analysis was conducted for each survey component. After this analysis was conducted, the content of the survey data was analyzed quantitatively. These quantitative analyses were conducted to investigate the statistical significance of the hypotheses and to properly answer the sub-questions of this study, which in turn seek to provide an answer to the central research question at hand. As this research is of confirmatory nature, the analyses that were conducted among the three factors investigate to what extent the factors are related and correlated to and with each other. For this study, the primary analyses which were conducted are the pearson's correlation analysis and a multiple regression analysis. The pearson's correlation analysis measures a linear correlation between two variables, whereas the multiple regression analysis extends upon this correlation by sketching a statistical model of the extent to which biometrics informedness and privacy concerns have an influence on one's biometrics acceptance.

First, the sub-question *''To what extent are Dutch residents informed about the utilization of biometrics technology in the Netherlands?''* was analyzed in terms of the answers that participants have given on the scale from 1 to 10. Consequently, a pearson's correlation analysis was conducted to assess the relationship between biometrics informedness and the other two constructs (biometrics acceptance & privacy concerns). Next to that, a multiple linear regression was conducted investigate to what extent biometrics informedness is able to influence one's biometrics acceptance in general. Moreover, the

average score of the participants was also taken into account to get a clear picture on the over all biometrics informedness. Finally, a cronbach's analysis was conducted to measure the reliability of the 8 biometrics knowledge items (α = .929). This indicates that there is a very high level of reliability within the items of this construct.

Second, the sub-question *''To what extent do residents of the Netherlands see biometrics as a privacy threat''* was also analyzed in terms of the answers that participants have given on the scale from 1 to 10. On the basis of these answers, a pearson's correlation analysis was conducted to assess the relationship between biometrics privacy concerns and biometrics acceptance. Next to that, a multiple linear regression was conducted to investigate to what extent privacy concerns are able to influence one's biometrics acceptance in general. Moreover the average score of the participants was also taken into account to get a clear picture on the overall extent of privacy concerns. Finally, a cronbach's analysis was conducted to measure the reliability of the 17 privacy concerns items (α = .909). This indicates that there is a very high level of reliability within the items of this construct.

Third, the sub-question *''To what extent do Dutch residents believe that they accept the utilization of biometrics technology in the Netherlands?''* was also analyzed in terms of the answers that participants have given on the scale from 1 to 10. However, as most of the analyses have already been done in comparison to the biometrics acceptance of the participants, the primary emphasis of this sub-question was to measure to what extent the average participant in this study has a certain level of biometrics acceptance. This level serves as the baseline for the other sub-questions in the study. Finally, a cronbach's analysis was conducted to measure the reliability of the 13 biometrics acceptance items items (α = .926). This indicates that there is a very high level of reliability within the items of this construct.

3.6 Conclusion

This section described the methods that were used in order to study the research question at hand. Furthermore, the methods were showcased in such a way that they can be replicated for future studies on this topic. In this study, a survey-based approach was used to analyze a relatively large group of citizens in terms of their opinions towards biometrics technology. An advantage of this method is that a larger sample can illustrate more significant and conclusive answers to the research question in general. The survey that was used in this study consists of components of earlier distributed questionnaires on the topic of biometrics, such as by Miltgen et al. (2013). Next to that, it was elongated by developing new items on the basis of the findings in the theoretical section. As a consequence, a new survey was developed which measures to what extent citizens of the Netherlands have a certain amount

of biometrics knowledge, privacy concerns and to what extent they are willing to accept biometrics in society. Ultimately, these items were analyzed in the shape of cronbach's analysis and several regression analyses. This in order to find out to what extent one's biometrics informedness and privacy concerns influenced the willingness to accept biometrics as a part of society.

4. Results

This section revolves around the outcomes of the previously outlined data analysis plans. On the basis of the conducted survey, this section will illustrate to what Dutch residents are willing to accept the utilization of biometrics in society. Related to that, it will also be shown to what extent this acceptance is dependent on their informedness regarding biometrics and the privacy concerns they might have. These two factors were hypothesized to have an influence on the biometrics acceptance of Dutch residents. Therefore, the statistical impact of these two factors will be fully showcased.

The section itself is structured on the basis of the sub-questions and hypothesis that were described in the introduction and theory sections. First, the general descriptives of the study results will be discussed. Examples are the means of each factor, the standard deviations and the implications of these numbers. Second the analyses regarding the biometrics informedness factor will be outlined. This primarily entails the pearson's correlation with the biometrics acceptance factor. Thirds, the analyses regarding the biometrics privacy concerns factor will be outlined. This primarily entails the pearson's correlation with the biometrics acceptance factor. Finally, the biometrics acceptance will be analyzed in general. The conducted analysis includes the regression model with regard to biometrics informedness and privacy concerns.

4.1 General survey findings

To start with, the general descriptives of the three survey components will be taken into account. These numbers will provide an indication of the general state of the three relevant factors in this study, namely biometrics informedness, privacy concerns and biometrics acceptance. Several interesting findings regarding these factors were discovered. However, the implications of these descriptives are not meant to service as statistical evidence in order to accept or reject the hypotheses. They merely serve to indicate to what extent a certain factor was present among the Dutch residents in the sample, as the profound statistical analyses will be elaborated upon in future paragraphs of the results section.

First, the biometrics informedness of Dutch residents seemed to be an interesting phenomenon in this study. On the basis of the 8 items ($\alpha = .929$) that were part of this survey construct, a mean biometrics knowledgeability score of ($M = 3.65$, $SD = 1.95$) was identified. This means that on average, participants within the sample indicate that they possess a relatively low level of informedness regarding the functionality of biometrics and the way it can be utilized by for example the Dutch government. Moreover, an interesting find regarding the demographic variables is that men on average seem to possess a higher level of informedness ($M = 4.10$, $SD = 2.10$) than women ($M = 2.97$, $SD = 1.48$). These relatively

low scores could potentially have implications for the rest of the results. Seemingly, Dutch residents seemed to be very unaware of the implications of biometrics technology in a societal context. Assuming that the average Dutch resident in the sample has a low degree of biometrics informedness, it could possibly explain why the results were also skewed in that direction. Nevertheless, these results were in line with the expectations, as earlier research already outlined that the average citizen likely does not possess a very high degree of knowledge regarding new technologies (Bauer et al., 2007; Martin & Donovan, 2015). Primarily due to the fact that only a relatively low amount of citizens are higher educated and thus have had more access to scientific information and information processing (Martin & Donovan, 2015). This phenomenon will be further elaborated upon in the biometrics acceptance section, as it has implications for the regression model.

Second, privacy concerns were also very much prevalent among Dutch residents. On the basis of the 21 items (α = .909) that were part of this survey construct, a mean biometrics privacy concerns score of (*M* = 6.09 , *SD* = 1.36) was identified. This means that on average, participants within the sample indicate that they have a decent amount of privacy concerns regarding the utilization of biometrics in society by for example the Dutch government and biometrics companies. On average, both men (*M* = 5.90, *SD* = 1.49) and women (*M* = 6.37, *SD* = 1.08) have similar scores on this construct. The fact that Dutch residents are wary of biometrics technology, does not come as a surprise. Earlier studies in the field have shown that citizens have concerns regarding biometrics and other new technologies (Miltgen et al., 2013; Martin & Donovan, 2015). Western media sometimes portray biometrics as an intrusive technology, which countries such China utilize to keep an eye on their citizens and potentially control their lives (Miltgen et al., 2013). Moreover, in an culturally individualistic country such as the Netherlands, citizens also are more likely to show distrust to those who could potentially harm them (Van Zoonen, 2016).
Thus, it can be said that these results are in line with the expectations which stem from the theoretical framework.

At last, the general degree of biometrics acceptance among Dutch residents was analyzed. On the basis of the 13 items (α = .909) that were part of this survey construct, a mean biometrics privacy concerns score of (*M* = 5.55 , *SD* = 1.61) was identified. This means that on average, participants within the sample indicate that they are slightly willing to accept the utilization of biometrics technology in society. A difference was identified between men and women, as men are more willing to accept biometrics (*M* = 6.00, *SD* = 1.40) than women (*M* = 4.86, *SD* = 1.70). Interestingly, these results do show that Dutch residents are somewhat willing to accept the utilization of biometrics technology in the Netherlands. A low degree of biometrics informedness and significant privacy concerns apparently did not completely crush the acceptance factor, although the results do indicate that there should be

some effect on the acceptance. Perhaps, Dutch residents do see the added value of biometrics technology.

Table 1

Means, standard deviations & Cronbach's Alpha per survey component

Scale	No. Items	Cronbachs' Alpha	*M*	*S.D.*
Biometrics informedness	8	.929	3.65	1.95
Privacy concerns	21	.909	6.09	1.36
Biometrics acceptance	13	.926	5.55	1.61

Note. Survey items were rated on a scale from 0 to 10.

4.2 Biometrics Knowledgeability/Informedness

As the descriptives already showed, Dutch residents are fairly uninformed regarding biometrics, which shows in the outcomes of the individual analysis of the survey items. Namely, the question with the highest level of biometrics informedness was *I understand the potential risks that biometrics can pose for society* (*M* = 5.23), whereas the question with the lowest level of biometrics informedness was *I am aware of the current biometrics regulations in the Netherlands* (*M* = 1.96). This indicates that people are somewhat aware of the potential risks of biometrics technology for the average citizen, but then again also do not know to what extent the judicial system currently protects them against these risks. More item scores are shown in Appendix B. Next to these descriptives, several analyses were conducted to test the hypothesis related to the sub-question *''To what extent are Dutch residents informed about the utilization of biometrics technology in the Netherlands?''.* It was hypothesized that people with a higher level of biometrics informedness would be more willing to accept biometrics utilization in society, as a higher level of knowledge regarding a technology was found to influence the acceptance in general (Bauer et al., 2007). A pearson's correlation analysis was conducted to analyze the correlation between biometrics informedness and the acceptance of biometrics technology among the participants. Biometrics informedness and biometrics acceptance were found to be slightly correlated $r(74) = .285$, $p = .014$. This indicates that when one has a higher level of biometrics informedness, one is slightly more likely to accept the utilization of biometrics in society. Evidently, this is in line with the hypothesis, which means that it can be accepted.

4.3 Biometrics privacy concerns

Privacy concerns regarding biometrics seemed to be prevalent among Dutch residents. Although the average score was not extremely high (6.09), it was still an indication of the concerns at hand. Nevertheless, some items still scored relatively high. In terms of the survey items, the question with the highest level of privacy concerns was *Not everyone is allowed to know everything about me online* (*M* = 8.65), whereas the question with the lowest level of privacy concerns was *I trust fingerprint analysis with my privacy* (*M* = 4.46). This indicates that people are very much protective regarding their online activities, but also aware of the fact that certain biometrics applications could have implications for their privacy. More item scores are shown in Appendix B. Next to these descriptives, several analyses were conducted to test the hypothesis related to the sub-question *''To what extent do residents of the Netherlands perceive biometrics as a threat to their privacy?".* It was hypothesized that people with more privacy concerns would be less willing to make use of or accept biometrics in general, as privacy concerns have been shown to negatively influence technology adoption among citizens (Van Zoonen, 2016). Furthermore, past research has already shown that this is also the case for biometrics technology (Chau et al., 2004). Finally, a pearson's correlation analysis was conducted to analyze the correlation between biometrics privacy concerns and biometrics acceptance. Biometrics privacy concerns was found to be strongly negatively correlated with biometrics acceptance $r(74) = -.696$, $p = .000$. This indicates that when one has privacy concerns, it is likely that this will lead to a decrease in biometrics acceptance. As a result, the hypothesis that has been formulated can be accepted.

4.4 Biometrics acceptance

Considering the average biometrics acceptance among Dutch residents, the component's items with the highest and lowest mean scores were in line with the expectations.The question which showed the highest level of acceptance was *I believe that biometrics can be considered useful to society* (*M* = 6.73), whereas the question with the lowest acceptance was *If possible, I am among the first to try out new biometrics applications* (*M* = 4.14). Possibly, this could indicate that while people do view biometrics as potentially useful to society, they do not necessarily desire to be among the early adopters. Taking into account the science literacy and understanding of the average citizen, these findings are not surprising. More item scores are shown in Appendix B.

Finally, in order to fully analyse the extent to which biometrics acceptance depends on biometrics informedness and privacy concerns, a multiple regression analysis was conducted. These two variables statistically significantly predicted biometrics acceptance

[$F(2,71) = 51.260$, $p = .00$, $R^2 = .591$]. This implies that, at least among the participants in the current sample, the extent to which one has a certain level of biometrics informedness and concerns about threats to their privacy has an influence on the extent to which one accepts the utilization of biometrics in society. Furthermore, it was particularly examined to what extent the regression model fits the premise of the two hypotheses in the study (H1: Biometrics informedness leads to more acceptance, H2: Biometrics privacy concerns lead to less acceptance). The results indicate that biometrics informedness indeed positively predicts biometrics acceptance [$B = .269$, $SE = .06$, $p = .00$] and that biometrics privacy concerns negatively predict biometrics acceptance [$B = -.849$, $SE = .09$, $p = .00$]. Ultimately, the general form of the equation to predict biometrics acceptance from biometrics informedness and biometrics privacy concerns is: biometrics acceptance = 9.379 + (0.269 x biometrics informedness) - (0.849 x privacy concerns). Both variables added statistically significantly to the prediction, $p < .05$. Although biometrics acceptance in general was relatively speaking on the high side, considering the mean privacy concerns and biometrics informedness, this regression model shows that the two earlier accepted hypotheses do indeed influence biometrics acceptance in the predicted ways.

4.5 Discussion

In terms of the study, it was found that the formulated hypotheses could be accepted on the basis of the results. Furthermore, analyzing the survey's reliability and consistency also showed that the separate components are all significantly internally consistent. However, in hindsight, the survey components are not entirely flawless. In several questions, it was often not clear what was specifically meant. For example the question ''*I believe that the government can be trusted when they utilize biometrics in society''* does not directly imply that the Dutch government is meant, instead of the European or any other level of government. Potentially, this could have led to a distortion of the results, as people might have answered differently if such questions were crystal clear.

Although the results have shown that there several interesting findings regarding biometrics acceptance, it is worth nothing that there might have been some flaws or inconsistencies in the process. Based on the geographical distribution of the participants, it becomes clear that a large majority of the Dutch residents sample is either a native from the area of Twente or a German student. Inherently, this could pose a problem to the general representativeness of the results of this study. These two groups are certainly valuable for research purposes, but the purpose of this study was to get a clear image on biometrics acceptance among all sorts of Dutch residents. As of now, this image is a bit skewed in the direction of Twente natives and German students. A possible explanation is the personal network and geographical roots of the researcher, as these are primarily based in the area of

Twente and consists of a large amount of Dutch and German students.

Another issue that popped up in the analysis of the results, is that the average Dutch resident in the sample has a strikingly low amount of biometrics informedness. Despite the fact that this could simply mean that Dutch residents are simply very uninformed about biometrics, it could also have implications for the rest of the survey. Potentially, it could be that barely understanding what biometrics is and how it is currently utilized in society also means that individuals were not properly able to fill in the survey. Surely, significant effects were found and the two hypotheses have been accepted, but that does not yet imply that the results are an actual representation of the convictions of Dutch residents. Perhaps, if citizens are more engaged with the topic of biometrics and are slightly more informed about the implications that this group of technologies has, they could be more capable of deciding whether they are more willing to accept biometrics. This was somewhat visible already in the research by Martin and Donovan (2015), as those with a higher extent of biometrics informedness were more accepting, up until a point where being an actual expert leads to a more negative perception of the possible dangers of biometrics.

4.6 Conclusion

This research showed that the biometrics acceptance among Dutch residents does indeed rely on the extent of their biometrics informedness and privacy concerns. For both factors, there was statistical evidence that they have an influence on one's level of biometrics acceptance. In terms of biometrics informedness, a higher level of biometrics informedness leads to more acceptance of biometrics acceptance, whereas a higher level of biometrics privacy concerns leads to less biometrics acceptance. In practice, this means that when a Dutch resident is more informed about the pros and cons of biometrics technology, they are more likely to accept the utilization of biometrics in society. Furthermore, if a Dutch resident has concerns about threats to their privacy, this heavily decreases the likeliness that they are willing to accept the utilization of biometrics in society. In comparison, one's privacy concerns have a significantly bigger impact on biometrics acceptance than biometrics informedness.The difference in impact on biometrics acceptance between those two factors is more than 300%. On the basis of these findings, it can be said that the hypotheses for this study can indeed be accepted. In general, Dutch residents have a low degree of biometrics informedness, a decent amount of privacy concerns and are somewhat willing to accept the utilization of biometrics in society.

5. Conclusion

This study aimed to investigate to what extent biometrics informedness and privacy concerns were able to influence biometrics acceptance among Dutch residents. Consequently, the following central research question was formulated: *''To what extent is biometrics acceptance among Dutch residents dependent on privacy concerns and biometrics knowledge?'.* On the basis of this question, it was identified that both factors seemed to have an impact on biometrics acceptance among Dutch residents. This was done by conducting a survey study which put the emphasis on the three factors which were relevant for this research question: biometrics informedness, biometrics privacy concerns and biometrics acceptance. In order to fully elaborate upon the implications of this study, this section addresses the central research question, illustrates the strengths and the limits of the study, discusses the practical and societal contributions it has and outlines the recommendations for future research in the domain of biometrics research.

5.1 Key insights

The survey analysis showed that the main question *''To what extent is biometrics acceptance among Dutch residents dependent on privacy concerns and biometrics knowledge?''* can be answered on the basis of the results of the survey. It was found that biometrics acceptance among Dutch residents does indeed depend on the extent of their privacy concerns and informedness regarding biometrics. However, the influence of privacy concerns was found to be much bigger than that of the biometrics informedness. The dependency of biometrics acceptance on privacy concerns was, statistically speaking, 3 times as big as the dependency on biometrics informedness. Thus, in terms of the central research question, biometrics acceptance among Dutch residents is very well dependent on privacy concerns and biometrics informedness, but the effect of privacy concerns is significantly bigger than the effect of one's informedness regarding biometrics.

Next to the central research question, there were also some interesting findings regarding the three sub-questions. The analysis of the data regarding first sub-question *''To what extent are Dutch residents informed about the utilization of biometrics technology in the Netherlands?''* was found to have striking implications. For example, the average Dutch residents seems to be fairly uninformed about the utilization of biometrics in society, the capacities of this technology and also to what extent the judicial system is able to protect them against eventual dangers of this technology. Although residents are somewhat aware of the risks that this technology can pose, they are not aware of what they can do against these dangers and how the government potentially protects them. Ultimately, male residents were shown to have a slightly higher extent of informedness than female residents.

The second sub-question *'To what extent do residents of the Netherlands perceive biometrics as a threat to their privacy?''* was perhaps the most influential one in terms of providing an answer to the central research question. Dutch residents showed that, although on some aspects they are not very aware of their privacy, they do have moderate concerns about them. For example, when it comes to their personal data, Dutch residents prefer not to have it shared with third parties or other curious individuals. Next to that, there was certainly a degree of skepticism regarding biometrics technology. Aspects such as trusting companies with biometrics data or trusting specific biometrics applications such as fingerprint analysis scored relatively low. These findings are relatively similar for both male and female residents, although female residents had slightly more concerns for their privacy.

Finally, the third sub-question *'To what extent do Dutch residents believe that they accept the utilization of biometrics technology in the Netherlands?''* revealed that people were somewhat willing to accept the utilization of biometrics technology within the Netherlands. Most Dutch residents believe that biometrics can definitely be useful to society and that it will make identifying oneself easier than before. However, people are not necessarily keen to be among the first to make use of biometrics and also do not believe that making use of biometrics will be rather fun. Ultimately, male residents were shown to be more willing to accept biometrics than female residents. This is not a surprising finding considering the regression equation, as female residents were shown to be less informed regarding biometrics and had a higher degree of privacy concerns.

5.2 Links to past research

The fact that this study investigated the dependency of biometrics acceptance on biometrics informedness and privacy concerns, is not a complete surprise. In the past, studies on biometrics acceptance already showed links to privacy concerns (Miltgen et al., 2013; Bansal et al., 2016; Reddick et al., 2015) and informedness/knowledgeability (Miltgen et al., 2013; Martin & Donovan, 2015). With the rise of surveillance society and the digital world, these two factors are a hot topic among researchers, politicians and increasingly among citizens as well. Consequently, the connection between this study and past research on biometrics informedness & privacy concerns will be elaborated upon in this section.

5.2.1 Past research on biometrics informedness

In the first place, this study identified that being informed or knowledgeable regarding biometrics leads to a higher degree of acceptance. In past studies, similar findings were also identified with both biometrics and other new technologies (Miltgen et al., 2013; Martin & Donovan, 2015). Being more informed or knowledgeable often led to more acceptance or

willingness to make use of technology such as biometrics (Miltgen et al., 2013). However, the opposite has also been found to be true. A study by Martin and Donovan (2015) showed that although the British government tried to present biometrics technology as accessible and easy to learn, this was merely a pretence in the eye of many citizens. Most citizens do not exactly know how biometrics technology works, what its pros and cons are and what implications the utilization of biometrics in society has for an average citizen (Martin & Donovan, 2015). One explanation for this is the lack of science literacy of the average citizen (Bauer et al., 2007). Not every individual has had access to (higher education) where there is an extensive emphasis on scientific literature and understanding science in general (Bauer, 2009). Consequently, the majority of its citizens are not as literate or understanding when it comes to the introduction of new technologies.

However, those with a high understanding of biometrics and a high extent of science literacy were often also less willing to accept than those who did not (Martin & Donovan, 2015). Perhaps, those who are more involved with a new technology and have a bigger understanding of this technology, also have more to worry about than people who are not so informed regarding a specific technology. Thus, there could be some sort of paradox involved in the knowledge component. Evidently, a lower level of knowledge leads to low acceptance (Miltgen et al., 2013; Martin & Donovan, 2015), although a very high level of knowledge has the same effect (Martin & Donovan, 2015). Nevertheless, a moderate level of knowledge, as presented in this study, was able to increase the amount of acceptance (Miltgen et al., 2013). This shows that it could potentially go both ways regarding biometrics informedness/knowledgeability. Future research should be conducted to unravel the extent of this paradox.

5.2.2 Past research on privacy concerns

In terms of the privacy concerns, the links to past research are more one-sided. The findings of this study show that having privacy concerns have a significant impact on one's willingness to accept and make use of biometrics. Past studies show similar results, as privacy concerns often negatively impact the acceptance of new technologies (Cullen, 2009; Miltgen et al., 2013; Bansal et al., 2016; Reddick et al., 2015; Van Zoonen, 2016). In the domain of biometrics, people are fearful for all sorts of privacy violations that can happen due to the utilization of biometrics in society (Martin & Donovan, 2015). Nevertheless, privacy concerns were found to have a substantial cultural basis as well (Cullen, 2009). It was found that in individualistic cultures people often trust out-group members more, unless they have a profound reason to show distrust. The results of this study are in line with this conviction, as people indeed showed distrust towards the government and biometrics companies, because of the fact that their privacy was potentially at stake. Especially

because most residents in the sample had a western background, it could be that these individualist principles were a key factor driving the privacy distrust.

Finally, the results of this study did not clearly identify the existence of the privacy paradox when it comes to biometrics technology. The participants indicated rather high feelings of wanting to be anonymous in digital environments and also showed major distrust towards GPS-based companies. However, they did not explicitly state that they do trust biometrics more than they have concerns. Next to that, they also often questioned as to why a certain company or website desired specific information of them. This shows that although there might be a privacy paradox visible among many citizens (Van Zoonen, 2016), this is not necessarily the case when it comes to biometrics technology. Perhaps this is because people view biometrics as more intrusive and dangerous than for example liking cat videos on a social media platform, although this data can potentially also be used for maleficent purposes.

5.3 Theoretical and practical implications

This study is of value to researchers in the field of biometrics technology and perhaps to researchers in the field of technology acceptance in general. Several things were found which contribute to the further understanding of biometrics acceptance and to what extent privacy concerns and biometrics informedness have an influence on this. First, the findings revealed that while one can potentially have a great extent of knowledge regarding biometrics, the influence of privacy concerns remains much bigger than expected. One would expect that an increase in biometrics knowledge would nullify some of these concerns, but perhaps a big increase in knowledge also leads to more privacy concerns, as in that case one is more informed about the potential risks and dangers of biometrics technology. Privacy concerns were often only noted to be a relatively distant factor when it comes to biometrics research, but this study shows that its influence is perhaps bigger than previously noted in biometrics research.

In any case, the results also show that the average biometrics informedness among Dutch residents is strikingly low. Most residents do not understand the potential risks of biometrics and to what extent the judicial system potentially protects them against these risks. This is of importance to scientists in the field of biometrics, as it shows that they have to take into account in their research that the average citizen is relatively clueless when it comes to being informed about biometrics. Previously, this was not necessarily noted in earlier research. Although several scientists note that the technology/science literacy of the average citizen is not very high (Bauer et al., 2007; Martin & Donovan, 2015), it was not yet actively applied in the context of biometrics research. As a consequence, this research shows that it is necessary to be aware of this pretense in future biometrics studies.

Nevertheless, the results of this study have major implications for practical applications of biometrics as well. As this study showed that the average Dutch resident is relatively uninformed regarding biometrics, the emphasis of the Dutch government should be put on properly informing the citizens. However, when this was tried by the UK government by showing that biometrics is easy to understand and learn, this failed miserably. Therefore, when the Dutch government will attempt to spread awareness regarding the utilization of biometrics technology, an honest view on biometrics technology should be presented in order to avoid misunderstandings among citizens. By properly informing the general public about the way biometrics will be utilized, the benefits it will bring and how potential dangers of this technology are addressed, citizens will likely be more willing to accept biometrics utilization in society.

Another important practical consideration is how the government and biometrics companies are supposed to deal with the privacy concerns of many Dutch citizens. As shown in this study, citizens are very reluctant to accept biometrics technology when they have a high degree of privacy concerns. However, these concerns can be addressed by ensuring the average citizen that this technology has its benefits and can be used for a good cause as well. Likely, many citizens are put off by the dystopian views of biometrics due to the fact that human rights organizations such as bits of freedom warn us about the way it is utilized in China. Nevertheless, this does not necessarily mean that similar utilization will take place in Dutch society. If anything, the Netherlands is a far more liberal democratic country than China.

In order to preserve the Dutch liberal humanist values, the government should be aware of the fact that the average Dutch citizen is not too keen on biometrics at the moment. One way to responsibly introduce biometrics technology is to establish laws and policy instruments which protect the individual privacy of citizens. For example, biometric data of individual citizens could be stored for a short period only. Furthermore, biometric companies should also introduce some sort of privacy safeguarding in their biometrics applications. This could be done by only collecting data from individuals who have given their permission to share their data. Moreover, a law could be put in place where biometric companies are forced to anonymize the data of those who make use of their technology. A biometrics company called 20face set the example by converting the data they gather from individuals in a bunch of relatable pixels, which allows them to be recognized on their system. Furthermore, users of this facial recognition software can always decide whether they want to be recognized when making use of certain platforms and ultimately even delete their biometric data from the software altogether. Such ways of handling user privacy should be a prime example of how governments and biometrics companies should utilize biometrics in the future.

5.4 Strengths and limits

This study has a number of strengths which make the conducted research more credible. To start, this study focussed on two key factors in biometrics acceptance which were not thoroughly researched before. Although there were some studies which investigated privacy concerns and biometrics informedness to some extent, they were often not of a quantitative nature. Next to that, none of these studies clearly analyzed any statistical relationship between these two factors and biometrics acceptance as a whole. This is an important asset in this study, as it illustrates to what statistical extent these two factors are responsible for biometrics acceptance among dutch residents.

Furthermore, the survey which served to collect the data of the dutch residents in the sample, proved to be very reliable. Every construct had a cronbach's alpha of over 0.9, which indicates that there is a high degree of coherence among the items of each construct. Likely, the constructs are so coherent because existing survey items were used and combined into the survey at hand. Next to that, only items with a profound theoretical basis or relevance were used in order to keep the validity as high as possible. Moreover, this study was in no way related to a company or an organization which develops or utilizes biometrics themselves. Participants were informed beforehand that the researcher carries the research out independently and anonymizes their data afterwards. This was an important measure to reduce socially desirable answers and thus limit the amount of social desirability bias.

Next to these strengths, there were also a few limits visible in this study. The first limitation is that although the survey seemed to be rather reliable and coherent, some of the items were still relatively lacking. This study explicitly measured the biometrics acceptance of Dutch residents, but some of the questions were not tailored towards this sample. For example, *I believe that the government can be trusted when they utilize biometrics in society* does not specifically mention the Dutch government or Dutch governmental institutes. As a result, people might have not understood that the Dutch government was the actor in this question. Next to that, some questions were not so ''crystal clear'', as they carried some suggestive elements. Finally, there was no pre-test conducted before the survey was distributed to the sample. Although the items had a relatively high cronbach's alpha, some questions could have still been more clear on the basis of the feedback from the pre-test sample. This is something to consider in future research, especially in studies with a potentially much larger sample and a longer data collection period.

The second limitation revolves around the sample in this research. Two minor issues were identified which could have influenced the results to some extent. The first issue is that the sample within the study might not be fully representative for all of the Dutch residents, as most of the participants with a Dutch and German nationality within the sample stem from

the area of Twente. Furthermore, most Dutch participants were either students or relatively old civilians from this area, whereas all of the German participants were students. This means that in some cases, the sample was relatively homogenous. Furthermore, the second issue is that the participants in the sample had a relatively low understanding of biometrics in general. Perhaps this is true for the average citizen in general, but it was still relatively striking how low the numbers were in the biometrics informedness component. As a consequence, this could have led to the fact that the influence of biometrics informedness component was lower than it is in reality. In any case, this should be further investigated in future research in the area.

The final limitation is the fact that the biometrics acceptance component could have been influenced by the TAM model. This was the sole theoretical model which was utilized to determine the biometrics acceptance component. Evidently, there is also some criticism present regarding this model, as it is a relatively easy but basic model in terms of technology acceptance. Therefore, the results were possibly steered in a certain direction due to the fact that the survey items also stem from surveys which have utilized the TAM model as their theoretical source of inspiration. Adding different theoretical models could have steered the result in a more neutral direction, regarding the technology acceptance.

5.5 Future research

Several things should be taken into consideration when further tackling the topic of biometrics acceptance and the related factors. First, taking the limits of the current research into account, survey studies should make sure that the items are clear enough that participants know for example which government is meant with questions such as *I believe that the government can be trusted when they utilize biometrics in society*. This limits the room for interpretation and thus increases the validity and reliability of these items. Next to that, future studies should also attempt to extend the sample beyond the geographical home area of the researcher(s). Due to the fact that the researcher in this study was a student in the area from Twente, with birth roots in Twente as well, a large majority of this sample consisted of people from the area of Twente. Ideally speaking, each area of a country is properly represented when the residents of this country are the target group. Perhaps contact could be sought with municipalities and provinces if they are able to assist in spreading the questionnaire, in order to realize a larger and a geographically more diverse sample. Also, different theoretical models than just the TAM should be utilized to create a stronger theoretical research basis surrounding the topic of biometrics acceptance.

Finally, future research should emphasize different research methods other than survey studies. Especially because self-reporting is not always the same as actual behaviour (Verhoeven, 2018). A recommendation would be to make use of for example experimental

studies, which gives a better indication of actual behaviour. Related to that, because not many Dutch residents have a decent amount of knowledge regarding biometrics, it would perhaps be more interesting to investigate their behaviour in an experimental setting. This way, more concrete and relevant insights regarding human behaviour towards biometrics acceptance could be gathered. Furthermore, it would be interesting to compare the views of a country with a more individualistic culture and a country with a collectivistic culture, in order to find out to what extent there are differences in terms of privacy concerns.

6. References

Ajibade, P. (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. *International Journal of Science and Technology, 3*(2), 173-181

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, *12*(2), 185-196.

Ashraf, A. R., Thongpapanl, N. T., & Spyropoulou, S. (2016). The connection and disconnection between e-commerce businesses and their customers: Exploring the role of engagement, perceived usefulness, and perceived ease-of-use. *Electronic Commerce Research and Applications*, *20*, 69-86.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1-21.

Bauer, M. W., Allum, N., & Miller, S. (2007). What can we learn from 25 years of PUS survey research? Liberating and expanding the agenda. *Public understanding of science*, *16*(1), 79-95.

Bauer, M. W. (2009). The evolution of public understanding of science—discourse and comparative evidence. *Science, technology and society*, *14*(2), 221-240.

Bennett, C. J. (2001). Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. *Ethics and Information Technology, 3*(3), 195-208.

Borkovich, D. J., & Breese-Vitelli, J. (2014). THE INFLUENCE OF MOBILE TECHNOLOGY CULTURE: BLIND TRUST, NAÏVETÉ, OR SKEPTICISM. *Issues in Information Systems*, *15*(2).

Business Insider. (2019). *How BlackBerry went from controlling the smartphone market to a phone of the past.* Retrieved from: https://www.businessinsider.nl/blackberry-smartphone-rise-fall-mobile-failure-innovate-2019-11?international=true&r=US

Cayford, M., Pieters, W., & Hijzen, C. (2018). Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology. *Intelligence and national security*, *33*(7), 999-1021

Chau, A., Stephens, G., & Jamieson, R. (2004). Biometrics acceptance-perceptions of use of biometrics. *ACIS 2004 Proceedings*, 28.

Chignell, M. H., Quan-Haase, A., & Gwizdka, J. (2003). The Privacy Attitudes Questionnaire (PAQ): Initial Development and Validation. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 4*7(11), 1326–1330. https://doi.org/10.1177/154193120304701102

CNBC. (2019). *China's surveillance tech is spreading globally, raising concerns about Beijing's influence.* Retrieved from: https://tinyurl.com/chinaconcerns

Cohen, N. S. (2008). The valorization of surveillance: Towards a political economy of Facebook. *Democratic Communiqué, 22*(1), 5.

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review, 33*(3), 405–421. https://doi.org/10.1108/14684520910969871

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Dalcher, D. (2007). Why the pilot cannot be blamed: a cautionary note about excessive reliance on technology. *International Journal of Risk Assessment and Management*, *7*(3), 350-366.

Daugman, J. (2003). The importance of being random: statistical principles of iris recognition. *Pattern recognition*, *36*(2), 279-291.

De La Robertie, C. (2019). Unplugged-Thinking the organisational and managerial challenges of intelligent towns and cities: a critical approach to the Smart Cities phenomenon. *M@ n@ gement*, *22*(2), 357-372.

Demetriadis, S., Barbas, A., Molohides, A., Palaigeorgiou, G., Psillos, D., Vlahavas, I., ... &

Pombortsis, A. (2003). “Cultures in negotiation”: teachers’ acceptance/resistance attitudes considering the infusion of technology into schools. *Computers & Education*, *41*(1), 19-37.
Ebbers, W. E., & Van Dijk, J. A. (2007). Resistance and support to electronic government, building a model of innovation. *Government Information Quarterly*, *24*(3), 554-575.
El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology,* 70-178.
Forbes. (2019). *China Slams 800M+ Internet Users With Facial Recognition Monitoring To Get Online.* Retrieved from: https://tinyurl.com/chinarecognition
Hai, L. C., & Alam Kazmi, S. H. (2015). Dynamic support of government in online shopping. *Asian Social Science; 11*(22), 1-9
Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer law & security review*, *28*(3), 263-272.
Hvidman, U. (2019). Citizens’ evaluations of the public sector: Evidence from two large-scale experiments. *Journal of Public Administration Research and Theory*, *29*(2), 255-267.
Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security*, *1*(2), 125-143.
Joh, E. E. (2016). The new surveillance discretion: Automated suspicion, big data, and policing. *Harv. L. & Pol'y Rev.*, *10*, 15.
Ju, J., Liu, L., & Feng, Y. (2018). Citizen-centered big data analysis-driven governance intelligence framework for smart cities. *Telecommunications Policy*, *42*(10), 881-896.
Kloppenburg, S., & Van der Ploeg, I. (2020). Securing identities: biometric technologies and the enactment of human bodily differences. *Science as Culture*, *29*(1), 57-76.
Krempel, E., & Beyerer, J. (2014). TAM-VS: A Technology Acceptance Model for Video Surveillance. *Privacy Technologies and Policy*. 86–100. https://doi.org/10.1007/978-3-319-06749-0_6
Lala, G. (2014). The emergence and development of the technology acceptance model (TAM). *Marketing From Information to Decision, (7)*, 149-160
Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. *MIS quarterly*, 461-491.
Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-31.
Levinson-Waldman, R. (2016). Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public. *Emory LJ*, *66*, 527.
Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, *10*(4), 415-453.
Liberatore, A. (2007). Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union. *European Journal on Criminal Policy and Research, 13*(1-2), 109-137.
Li, Z. & Jain, A. (2011). *Handbook of face recognition.* London New York: Springer.
Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 47-64.
Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, *22*(9), 499-508.
Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.
Martin, A. K., & Donovan, K. P. (2015). New surveillance technologies and their publics: A case of biometrics. *Public Understanding of Science*, *24*(7), 842-857.
Miltgen, C. L., 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*, 103-114.
Muller, B. J. (2004). (Dis) qualified bodies: securitization, citizenship and ‘identity management’. *Citizenship studies*, *8*(3), 279-294.
Nalwa, V. S. (1997). Automatic on-line signature verification. *Proceedings of the IEEE, 85*(2),

215-239.
Napitupulu, D. (2017). A conceptual model of e-government adoption in Indonesia. *International Journal on Advanced Science, Engineering and Information Technology*, *7*(4), 1471-1478.
Norval, A., & Prasopoulou, E. (2019). Seeing Like a Citizen: Exploring Public Views of Biometrics. *Political Studies*, *67*(2), 367-387.
Park, S. Y. (2009). An analysis of the technology acceptance model in understanding university students' behavioral intention to use e-learning. *Journal of Educational Technology & Society*, *12*(3), 150-162.
Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE security & privacy*, *1*(2), 33-42.
Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.
Persico, D., Manca, S., & Pozzi, F. (2014). Adapting the Technology Acceptance Model to evaluate the innovative potential of e-learning systems. *Computers in Human Behavior*, *30*, 614-622.
Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy*, *30*(1), 53-67.
Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, *32*(2), 129-141.
Samhan, B. (2018). Revisiting Technology Resistance: Current Insights and Future Directions. *Australasian Journal of Information Systems, 22.* https://doi.org/10.3127/ajis.v22i0.1655
Scott, M., Acton, T., & Hughes, M. (2005). An assessment of biometric identities as a standard for e-government services. *International Journal of Services and Standards, 1*(3), 271. https://doi.org/10.1504/ijss.2005.005800
Telegraph. (2020). *The facial recognition tech that can identify you even with a face mask*. Retrieved from: https://tinyurl.com/telegraphbiometrics
The Guardian. (2015). *NSA tapped German Chancellery for decades.* Retrieved from: https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel
Torres, R., & Gerhart, N. (2019). Mobile proximity usage behaviors based on user characteristics. *Journal of Computer Information Systems*, *59*(2), 161-170.
Trepte, S., & Masur, P. K. (2017). Need for privacy. *Encyclopedia of personality and individual differences. London: Springer.*
Trüdinger, E. M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly*, *34*(3), 421-433.
Van Dijk, J. A., Peters, O., & Ebbers, W. (2008). Explaining the acceptance and use of government Internet services: A multivariate analysis of 2006 survey data in the Netherlands. *Government Information Quarterly*, *25*(3), 379-399.
Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.
Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision sciences, 39*(2), 273-315
Verhoeven, N. (2018). *Wat is onderzoek? : praktijkboek voor methoden en technieken*. Amsterdam: Boom
Ware, W. H. (1993). The new faces of privacy. *The Information Society*, *9*(3), 195-211.
Wayman, J. L (2002) Digital signal processing in biometric identification: a review, *2002 International Conference on Image Processing (Proceedings)*, *1*, 37-40.
Webster, C. W. R. (2012). Surveillance as X-ray. *Information Polity*, *17*(3, 4), 251-265
Wijk. (2015). *Machtspolitiek.* Amsterdam: AUP..
Wired. (2015). *Rating Tech Giants on Privacy: Google Slips, WhatsApp Fails.* Retrieved from: https://www.wired.com/2015/06/rating-tech-giants-privacy-google-slips-whatsapp-fails/
Wolfson, T. (2017). Technology and social movements. *Soundings: A journal of politics and culture*,

65(65), 129-131.
Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479-500.
Zheng, X., & Lee, M. K. (2016). Excessive use of mobile social networking sites: Negative consequences on individuals. *Computers in Human Behavior*, *65*, 65-76.
Zimmer, S. G. (2018). Cell Phone or Government Tracking Device: Protecting Cell Site Location Information with Probable Cause. *Duq. L. Rev.*, *56*, 107.

7. Appendices

Appendix A: Questionnaire

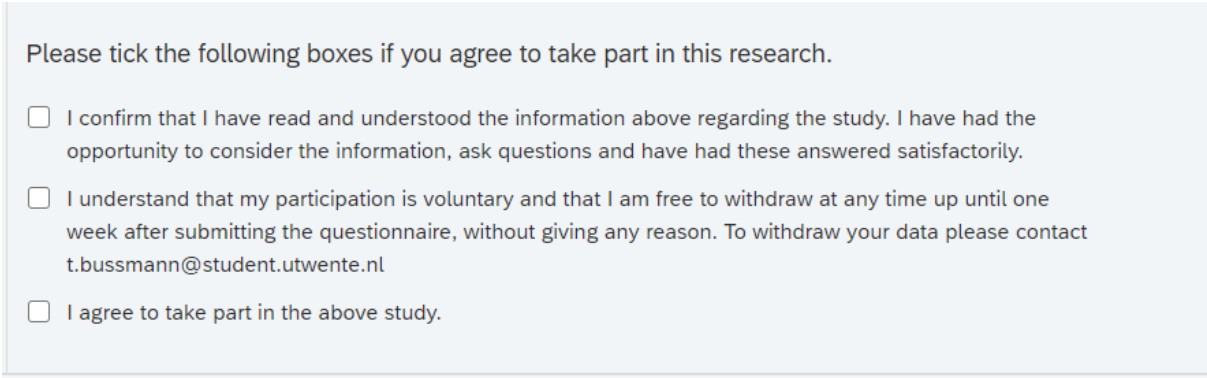
Citizen perceptions on Biometrics: Surveillance or service?

Researcher: Tim Bussmann

Thank you for agreeing to take part in this research. In agreeing to participate you have the following rights and protections as laid down in the British Psychological Society's ethical guidelines.

Your participation is entirely voluntary Under no circumstances will your real names or identifying information be included in the reporting of this research. You may withdraw your data from this research at any point until one week after the submitting the survey. Nobody, except the researcher and the research supervisors will have access to this anonymised material in its entirety.

In agreeing to the terms of this consent form, participants should be aware that any anonymised
material is solely for use in the current research project.



A few instructions before you proceed:

There are no right or wrong answers. Your personal opinion is what matters in this research. Try to be honest while answering the questions. All data will be treated confidentially and will only be seen by the researcher.

Demographic questions

What is your sex?

What is your age?

What is currently your primary occupation?

What is your highest current or completed educational level?

What is your nationality?

Knowledge component (scale 0-10)

I am familiar with biometrics and how it is currently used in society

I consider myself to be knowledgeable enough to describe the inner workings of biometrics

I know a lot about different biometrics applications

I am aware of the benefits that biometrics has to offer for society

I understand the potential risks that biometrics can pose for society

I am aware of the current biometrics regulations in the Netherlands

I keep up with new developments regarding biometrics

I believe that I am knowledgeable enough to work with biometrics in a future job

(Biometrics) Privacy component (scale 0-10)

In general, I value my privacy

In general, I am concerned about my privacy on the internet (e.g people reading your email, finding out what websites you visit, etc.)

Organizations and other individuals are not allowed to distribute personal information about me without my knowledge

I am not comfortable with giving out personal information on the internet

I frequently question why I'm providing personal information

I would prefer to stay as anonymous as possible when using the internet or other technologies

I do mind if my personal data is publicly available to others (e.g. other individuals or third parties)

Not everyone is allowed to know everything about me online

I do not trust applications and technology to take good care of my GPS data

In general, I believe that biometrics technology does not infringe upon my individual privacy rights

---

I am comfortable with providing my data to biometrics companies

I am comfortable with providing my data to governmental biometrics applications

I believe that Biometrics companies can be trusted with my privacy

I believe that the government can be trusted when they utilize biometrics in society

I believe that the current laws and judicial system protect against abuse by biometrics technology

I believe that there are privacy differences in terms of which biometrics application is used

I trust the following biometrics applications with my privacy to this extent:

- Facial recognition
- Voice recognition
- Fingerprint analysis
- Iris recognition
- Signature recognition

Biometrics acceptance (scale 0-10)

I believe that biometrics can be considered useful to society

I believe that biometrics will make it easier to identify oneself

I believe that biometrics technology will be easy to use for individuals

I believe that it will be easy to learn how to deal with biometrics technology

If possible, I am among the first to try out new biometrics applications

I believe that making use of biometrics will be fun

I am willing to make use of biometrics in general

I am willing to make use of biometrics in my own home

I am willing to accept that the government will often make use of biometrics in the future

I have positive feelings regarding biometrics

Making use of biometrics in society seems like a wise idea

I put my trust in biometrics

I believe that the information provided by biometrics technology is reliable

Appendix B: Individual item scores per component.

Table 2

Means & standard deviations of the biometrics informedness items

Survey item	*M*	*S.D.*
I am familiar with biometrics and how it is currently used in society	4,74	2,36
I consider myself to be knowledgeable enough to describe the inner workings of biometrics	3,29	2,22
I know a lot about different biometrics applications	3,37	2,33
I am aware of the benefits that biometrics has to offer for society	5,12	2,31
I understand the potential risks that biometrics can pose for society	5,24	2,88
I am aware of the current biometrics regulations in the Netherlands	1,96	1,93
I keep up with new developments regarding biometrics	2,51	2,24
I believe that I am knowledgeable enough to work with biometrics in a future job	2,93	2,69

Table 3

Means & standard deviations of the biometrics privacy concerns items

Survey item	*M*	*S.D.*
In general, I value my privacy	7,83	1,53
In general, I am concerned about my privacy on the internet (e.g people reading your email, finding out what websites you visit, etc.)	6,56	2,10
Organizations and other individuals are not allowed to distribute personal information about me without my knowledge	7,52	2,37
I am not comfortable with giving out personal information on the internet	6,40	2,32
I frequently question why I'm providing personal information	5,82	2,44
I would prefer to stay as anonymous as possible when using the internet or other technologies	6,64	2,42
I do mind if my personal data is publicly available to others (e.g. other individuals or third parties)	7,32	2,34
Not everyone is allowed to know everything about me online	8,64	1,71
I do not trust applications and technology to take good care of my GPS data	5,87	2,28
In general, I believe that biometrics technology does not infringe upon my individual privacy rights	5,89	1,92

I am comfortable with providing my data to biometrics companies	6,09	2,14
I am comfortable with providing my data to governmental biometrics applications	5,65	2,08
I believe that Biometrics companies can be trusted with my privacy	6,08	2,05
I believe that the government can be trusted when they utilize biometrics in society	5,63	2,04
I believe that the current laws and judicial system protect against abuse by biometrics technology	5,83	2,12
I believe that there are privacy differences in terms of which biometrics application is used	4,46	2,02
(I trust the following biometrics applications with my privacy to this extent:) Facial recognition	5,37	2,56

Voice recognition	5,41	2,50
Fingerprint analysis	4,45	2,74
Iris recognition	4,75	2,91
Signature recognition	5,48	2,65

Table 4

Means & standard deviations of the biometrics acceptance items

Survey items	*M*	*S.D.*
I believe that biometrics can be considered useful to society	6,72	1,84
I believe that biometrics will make it easier to identify oneself	6,62	2,23
I believe that biometrics technology will be easy to use for individuals	6,71	1,91
I believe that it will be easy to learn how to deal with biometrics technology	6,33	2,09
If possible, I am among the first to try out new biometrics applications	4,13	2,57
I believe that making use of biometrics will be fun	5,04	2,55
I am willing to make use of biometrics in general	5,63	2,16
I am willing to make use of biometrics in my own home	5,44	2,32
I am willing to accept that	5,45	2,10

the government will often make use of biometrics in the future		
I have positive feelings regarding biometrics	5,06	2,19
Making use of biometrics in society seems like a wise idea	5,16	2,15
I put my trust in biometrics	4,41	2,29
I believe that the information provided by biometrics technology is reliable	5,41	2,20