Vrije Universiteit Amsterdam

Universiteit van Amsterdam

Master Thesis

An Assessment of Public Knowledge and Attitudes Concerning Facial Recognition Technologies

Author: student name Chao Zhang
VUA Student nr: 2619800
UvA Student nr: 11991976

1st supervisor: supervisor name: Natalia Silvis-Cividjian
2nd reader: supervisor name: Wan J. Fokkink

A thesis submitted in fulfillment of the requirements for the joint UvA-VU Master of Science degree in Computer Science

July 8, 2021

Abstract

Facial recognition is a controversial technology because it not only provides convenience to our daily life but also concerns the public's privacy. In this thesis, we aim to assess the general public's attitudes and perceptions of facial recognition applied on surveillance cameras. We need to determine the factors that influence those attitudes. We designed a survey containing 27 questions and collected data from different background testers. With the statistical tests, we concluded that: age range, gender, education level, nationality, working field and the understanding level of facial recognition have a significant effect on attitudes toward facial recognition technology applied on different scenarios. We also found that the public is willing to using facial recognition because it causes convenience in daily life. However, the privacy invasion is the biggest concern for general public. Regardless of all kind of concerns, 83.7% survey respondents believe that facial recognition technology will be more widely used in the next ten years. With the result of these new findings, technology producers, government agencies and law enforcement will be better informed as how to effectively roll out facial recognition technology with minimal push back from the public.

Keywords: Facial recognition technology, surveillance cameras, survey, public attitudes, public opinions, concerns, security, privacy

Abbreviation

Abbreviations List	
Acronym	Definition
ANOVA	Analysis of Variance
API	Application Programming Interface
BSIA	British Security Industry Authority
CCTV	Closed Circuit Television
CHINA	People's Republic of China
DV	Dependent Variable
EBGM	Elastic Bunch Graph Matching
EC	Exclusion Criteria
FRA	Facial Recognition Algorithm
FRT	Facial Recognition Technology
GAN	Generative Adversarial Network
GDPR	General Data Protection Regulations
HCI	Human-Computer Interaction
IC	Inclusion Criteria
IHS	Information Handling Services
IV	Independent Variable
LBPH	Local Binary Pattern Histograms
LDA	Linear Discriminant Analysis
NACRO	National Association for the Care and Resettlement of Offenders
PCA	Principal Component Analysis
PPB	Pilot Parliaments Benchmark
SDK	Software Development Kit
SVM	Support Vector Machine
UK	United Kingdom
USA	United States of America

Acknowledgements

First of all, I would like to thank my two supervisors dr.Natalia Silvis-Cividjian and prof.dr.Wan J. Fokkink for their infinite patience and academic support during my research. I also would like to thank dr. Lars Lischke for surpervising me at the beginning. I have learned a lot from them. I am grateful to all my friends and other people who helped me to fill in my surveys, for collecting enough data to analyze my research. I appreciate my friend Bob Span who helped me modify my translation of survey in Dutch. I also want to thank my dear friend Dr.William L. Coale personally, as well my mentor, for giving me suggestions and encouragement to improve my study. Last but not least, I want to thank all my family, especially my husband Jan Dekkers who gives me unconditional all kinds of support during the university period, also giving me a new life in the Netherlands. There were a lot of things happened to anyone in 2020, there is no doubt that it was been a tough year, I wish everyone starts a better new life from 2021.

Contents

CONTENTS

List of Figures

List of Tables

1

Introduction

In this section, we present the background of facial recognition technology, including its conflicting attitudes in public. According to Jeffrey C. Price and Jeffrey S. Forrest *Practical Aviation Security: Predicting and Preventing Future Threats.* 3rd ed., Elsevier, 2017. "Facial Recognition uses a two-dimensional or three-dimensional image of the visible physical structure of an individual's face for recognition purposes[4]." Facial recognition provides benefits in society, including increasing safety and security, preventing crimes, helping finding missing people, making shopping more efficient, it can even help improve healthcare systems[5]. Despite all the advantages of facial recognition, the problem is that there is push-back against the facial recognition technology which it has prompted calls for bans and stricter regulation[6]. The development of facial recognition technology shows the significant issues with being utilized in public. The reasons for conducting this research were: 1)facial recognition has been applied in our life in a quiet and fast way, for instance, unlocking your phone with FaceID, managing your mobile banking with FaceID, facial recognition aided verification systems that have been partially implemented in 70 (out of a total 218) Civil Aviation airports in China by August 2018. Especially at Beijing Daxing International Airport, passengers were able to get their boarding passes with the help of China Eastern Airlines' facial recognition system without showing any ID cards[7]. 2) There is very few research about the public opinions and attitudes about applying facial recognition technology. There is only one paper is closing related to our research by the time we collect data. In September 2019, the Ada Lovelace Institute summarized a report from a survey *Beyond face value: public attitudes to facial recognition technology* in UK[8]. There is barely academic research concern what the public thinks about facial recognition technology. For reasons like these, that is why it is critically important to study individual's attitudes and factors behind those attitudes, so that facial recognition technology can

provide better assistance for the public and be accepted by the society.

1.1 Context

Throughout the history of computing, interactions between humans and computers have increased in a fast way. In order to achieve highly effective human-computer interaction (HCI), there is a growing need for the computer-human interaction to take place similarly to the way human-human interaction does[9]. The traditional way of humans interacting with each other is mainly through speech; however, body language interaction (i.e face expression) is an important method to emphasize interactions and display of emotions as speech [9]. Since the development of facial recognition technology, these kind of interactions are not only limited between human and human, the computer can "interact" with humans through surveillance cameras. A facial recognition program maps facial features from a video or picture and then compares the information with a database of known faces in order to find a match.

In espionage and counterintelligence, surveillance is the monitoring of behavior, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people[10]. Over the last two decades, the extraordinary growth of state surveillance technology of the global population (UK, USA and China, (see Chapter 2)) has been fuelled by political and technological developments. For instance, it has been estimated that the average UK urban resident is now monitored more than 300 times a day, making Britain the most visually surveilled nation on Earth[11].

Under the commercial and private needs, economic and political encouragement, come to the Internet age, surveillance cameras have never been so effective and convenient these days, especially Wi-Fi connectivity and cloud storage has given surveillance experts more video footage than they could ever review. In 2015, Information Handling Services (IHS)[1] Markit has measured the installed base of security cameras for the first time. The analysis was driven from ten years of unit shipment data collected for its video surveillance research. IHS estimated the service life of cameras in each sub-region by end-user industry to size the current installed base. According to IHS, there were 245 million professionally installed video surveillance cameras active and operational globally in 2014. Whilst the majority of these cameras were analog, over 20 percent are estimated to have been network cameras and around two percent HD CCTV cameras [12].

[1]IHS Markit is a global leader in information, analytics and solutions for the major industries and markets that drive economies worldwide.`https://ihsmarkit.com/index.html`

Graham argued that CCTV is set to follow a similar pattern of development over the next 20 years, to become a kind of 'fifth utility[1]'[13]. As the rush to ubiquity, surveillance cameras present normalization, and regularization; however surveillance technology, especially CCTV cameras have been controversial throughout their history, the fear of being watched is showing [13]. CCTV systems integrate state-of-the-art surveillance cameras, often with remarkable resolution and infrared night-time capability. Video recorders are used to record the images from all cameras for use in criminal prosecution and police investigation. New uses are constantly being found for CCTV beyond its initial purpose: from traffic monitoring, checking the performance of street cleaners, monitoring graffiti, preventing teenagers smoking to discouraging terrorism (or at least providing evidence for tracking down terrorists after attacks). Often, such systems include sophisticated computer-assisted scanning operations, motion-detection facilities, loudspeaker systems and zoom capabilities. Especially applying facial recognition algorithms on CCTV cameras takes some people's privacy fears to a higher level.

Facial recognition is widely applied. This technology is not theoretical in our daily life anymore. In November 2017, Apple Inc. initially released Face ID[2] to their new products. That system allows biometric authentication for unlocking a device, making payments, and accessing sensitive data, as well as recognizing detailed facial expression [14]. Moreover, facial recognition is changing the e-commerce paying method. In December 2018, Alipay first rolled out its facial recognition system: Smile-to-Pay[3] - paying with your face. With the development of this technology, no need to bring your phone and instead using only facial recognition[15]. This payment method has expanded it to over 300 cities in China by July 2019. Facial recognition can as easily be used by a shopping mall to monitor potential shoplifters, by casinos to track potential fraudsters, by law enforcement to monitor spectators, at a Super Bowl match or used for identifying terrorists at airports which is currently in operation at various US airports.

Facial recognition technology is getting more and more mature over time; for instance, photo retrieval, access control and attendance system. Its application has been classified into six categories: 1) commercial, residential building safety and management, i.e. Facial recognition security door; 2) digital passport and ID, i.e. immigration control, civil aviation; 3) public security, justice and criminal investigation, i.e. track down fugitives; 4)

[1] The five primary utilities are form, time, place, possession and information.

[2] `https://support.apple.com/en-us/HT208108`

[3] `https://www.bbntimes.com/financial/introducing-smile-to-pay`

automated self-services, i.e. ATM; 5) information security, i.e. log in computer, mobile payment; 6) entertainment, i.e. age guesser application.

However, the development of facial recognition technology has been postponed recently. Since 25th May 2018, the General Data Protection Regulation (GDPR)[1] is a new EU data privacy law that has been in force. It stipulates that a company in collecting user's biometric data such as the face must obtain the person's permission in advance. If there are any violations, mandated by law, the fine is based on 4% of the party's annual turnover and 2.65% of its anticipated turnover for the coming year [16]. In April 2019, the publication of work Megapixels Project[2] by Berlin-based security researcher Adam Harvey documents many large data sets, how they are used, and what's at stake for your privacy. In June 2020, IBM got the ball rolling earlier this month when IBM CEO Arvind Krishna sent a letter to Congress. It states that IBM will no longer offer general purpose facial recognition or analysis software or be offered by other vendors. The mass surveillance, racial profiling, violations of basic human rights and freedoms are not consistent with values and Principles of Trust and Transparency. It is time to discuss how domestic law enforcement agencies should adopt this technology.[17] Later, other tech giants quickly followed and the same week Amazon announced that it will stop providing its facial recognition technology to police forces for one year due to questions that the company was not committed to fighting racism. Just one day later, Microsoft decided not to sell the controversial technology to police departments until there is a federal law regulating it.[17]

Most of the algorithms are at the heart of software systems. Thus, it is difficult to get access to them for inspection and scrutiny. More specifically, however, even if you can go through the code line by line, it is impossible to inspect that code in operation, as it becomes implemented through multiple layers of translation for its execution. At the most basic level we have electric currents flowing through silicon chips, at the highest level we have programmed instructions, yet it is almost impossible to trace the connection between these as it is being executed. The facial recognition capability canbe embedded into existing CCTV networks, making its operation impossible to detect. Thus, it is virtually impossible to know if the code you inspected is the code being executed[18].

[1] `https://gdpr.eu/what-is-gdpr/`
[2] `https://megapixels.cc/datasets/`

1.2 Problem Definition

1.2.1 Problem Statement

Facial recognition used on CCTV cameras is a double-edged sword, it was designed for protection of citizens and prevention of crime. However, it reflects not only its positive significance but also its hazards [19]. Under the growth of CCTV cameras all over the world, facial recognition presents more and more commercial and private demands. Both public and private sector organizations are incorporating facial recognition into products and services to create substantial benefits for consumers [20]. Facial recognition technology provides huge potential development not only limited to financial and security domains. In face, the public attitudes are odd between each other in terms of level of acceptance. It is critical that we assess and uncover the factors that influence the public's attitudes toward facial recognition technology. Our purpose is to provide different scenarios of applying facial recognition technology to the survey respondents, so that they can express their attitudes. The results will provide perspectives for any agency or organizations to make informed decisions while applying facial recognition in public.

1.2.2 Research Questions

There are two main questions to address in this thesis:

RQ1: How do facial recognition systems work?

RQ2: What public attitudes exist toward using facial recognition technology on CCTV cameras?

RQ3: What factors influence the public attitudes toward using facial recognition technology?

1.3 Research Method

1.3.1 Literature Study

By aiming at answering our research questions, we first conduct a literature study. To identify the initial set of studies we performed an automatic search query on *Google Scholar* and *DBLP*[1]*-Computer Science Bibliography*. We selected such digital library for the following reasons[21]: 1) *Google Scholar* provides the highest number of potentially relevant studies compared to other four relevant libraries (Scopus, ACM, Digital Library, IEEE

[1]What is dpld? `https://dblp.org/faq/What+is+dblp.html`

Explore, and Web of Science); 2) the query results could be automatically extracted from the indexer. The query selects studies containing either a keyword referring to "camera", "surveillance camera", "CCTV", or "facial recognition" and related acronyms in their title. 3)the full-text of the studies must contain both on of the keywords referring to "surveillance camera" and "facial recognition". 4) the dblp database is the on-line reference for bibliographic information on major computer science publications.

We filtered all the remaining research papers according to a set of rigorously defined selection criteria. A research paper was included in the set of primary studies exclusively if it satisfied all of our inclusion criteria (IC) and none of the exclusion criteria (EC). In order to thoroughly examining the literature in a time-efficient and objective manner. The inclusion and exclusion criteria were utilized as below [21]:

IC1 - Studies focusing on facial recognition applied on surveillance cameras.

IC2 - Studies focusing on facial recognition application, algorithms and security systems are included.

IC3 - Studies focusing on the general public's attitudes towards on facial recognition or surveillance cameras. With these inclusion criteria, we ensure that only papers discussing the public's opinion of facial recognition are included.

EC1 - Secondary or tertiary studies (e.g., systematic literature reviews, etc.). This exclusion criterion is adopted in order to exclude studies which do not report the desired level of detail of facial recognition technology.

EC2 - Studies in the form of editorials and tutorial, short papers,and poster, as they are deemed to not provide the required level of detail and information.

EC3 - Studies that have not been published in English or Chinese language, as their analysis would be too time consuming and the translation is not accurate.

EC4 - Duplicate papers or extensions of already included papers, in order to avoid possible threats to conclusion validity.

EC5 - Papers that are not available, as we cannot find them in university library or internet.

There are 60 items selected (see Reference), 47 academic articles from chosen digital library and 13 resources from online. First we presented the related work on the growth of CCTV cameras around the globe and the effectiveness of CCTV in preventing crimes. By introducing the history of facial recognition technology and the methods of facial recognition, we provide a clear understanding of how it works on CCTV cameras. We aim to present the existing active and passive attitudes of CCTV cameras and facial recognition technology. We introduce the technology behind face recognition systems to address the

first research question. Then we focus on the public attitudes and perception are key information to answer the second and third research questions.

1.3.2 Data Collection and Data Analysis

Through the literature studies, we have identified general ideas that the public has concerns about regarding the security, accuracy and privacy invasion of facial recognition technology. We also identified what kind of impacts exist to the public. According to Goodman et al.[22], interviews, usability evaluations, surveys, and other forms of user research are a good way to figure out how to improve products or services, to develop something new or even it can change the market completely. To figure out existing attitudes of facial recognition in our daily life, we decided to create surveys and do interviews. After collecting data, we needed to compile information and organize all data on spreadsheet and do statistical tests with IBM SPSS[1] software. After we analyzed the valid data, we will use the related results to answer second and third research questions.

1.4 Objectives

This report has two main objectives:
(i) We aim to introduce how facial recognition systems work, including its architecture and most common algorithms.
(ii) We focus directly on discovering how people feel about the use of facial recognition technology. (iii) We aim to identify what factors (education/nationality/age range/profession, etc.) influencing public attitudes toward the use of facial recognition technology as well as assess the degree to which the public is knowledgeable about these technologies.

The target audience of this thesis is composed of:
(i) Researchers willing to understanding and critically reflecting to surveillance technology;
(ii) Scientific audiences willing to understand public attitudes and perceptions of facial recognition;
(iii) Practitioners who has computer science or engineering background willing to care about how facial recognition technology affects daily life.

[1] `https://www.ibm.com/nl-en/analytics/spss-statistics-software`

1.5 Thesis Outline

The chapter 1 is the introduction which contains the background, conflicting attitudes about the situation of develop facial recognition from different countries based on reality. Then we discuss research questions of the thesis which need to be solved. Also we explain the research method and objectives of our work. The chapter 2 contains the literature reviews of CCTV cameras and facial recognition technology. This chapter also focuses on facial recognition systems which will answer our first research questions. The chapter 3 discusses the plan of the research which includes the details of the survey and research design. In chapter 4, it covers data collection and analysis methods, we will post all the outputs from the collecting data to answer the second research question. The chapter 5 contains the discussion of our research, also we will draw follow-up questions discuss the future work. Chapter 6 contains the conclusions, limitations. In chapter 7, we provide the additional information which helps the reader clearly understand the thesis.

2

Literature Review

In this chapter, we aim to address the first research questions. We present the general architecture of how facial recognition system work. Later we introduce most common facial recognition methods and algorithms, all the software or products adopt one or multiple algorithms to develop or improve the accuracy.

2.1 The History of Surveillance Cameras

CCTV is generally used as a complementary security measure and is widely used in industries, military, airports, shops, offices, factories, industries and even today many housing units and apartment buildings have been using and applying this technology [23]. According to Stratistics MRC[1], the global video surveillance market stood at 19.51 billion dollars in 2015 and is expected to reach 63.2 billion dollars by 2022 [24]. The growth of CCTV cameras is dramatic especially in three countries: United Kingdom(UK), United States of America(USA) and China.

UK: UK has a long history of surveillance cameras as one of the earliest countries applying CCTV cameras to improve public security [25]. By 1961, the first permanent surveillance cameras were set up in order to improve security at London's bustling railway stations [26]. Ten years later, from 1970 to 1980, police use of CCTV remained limited and focused on marginal groups such as football hooligans and political demonstrators. Until 1985, the first large-scale public space surveillance system was erected in Bournemouth. By 2002, CCTV market analysts were reporting on year growth of 14% - 18% for the previous decade. In 2008, analysts MBD suggesting that the market will be worth around £1.1

[1]StratisticsMRC is a global market research company offering a wide spectrum of market research reports with deep industry analysis`https://www.strategymrc.com`

billion [23]. In 2013, the British Security Industry Authority (BSIA) estimated including 750,000 cameras in "sensitive locations" such as schools, hospitals and care homes. It is estimated that there are between 291,000 and 373,000 cameras in public sector schools, plus a further 30,000 to 50,000 in independent schools. Surgeries and health centres have an estimated 80,000 to 159,000, while there are believed to be between 53,000 and 159,000 cameras in restaurants[27]. There is estimated to be one CCTV camera for every 14 people in the UK[28]. By the end of 2018, the British Security Industry Authority (BSIA) estimated that £2.2 billion is spent on video surveillance systems each year, and the ubiquity of CCTV cameras estimates suggest a total of 5.9 million[1], with the majority being privately owned which seems set to continue [29].

USA: The first national survey of CCTV in 1997 stated: only 13 cities' police departments in the country used CCTV video surveillance systems [30]. Twenty-five U.S. cities were using CCTV to monitor public areas, the Security Industry Association forecast that sales could grow to over 1.6 billion dollars by the end of 2001 [30]. From 2009 to 2011 there are an estimated 30 million surveillance cameras now deployed in the U.S. shooting 4 billion hours of footage a week. The growth of CCTV cameras in U.S. was set to increase dramatically after 9/11 attacks[2], the sale of CCTV surveillance cameras could soar to nearly 5.7 billion dollars by the end of 2001 [30]. Between 2012 and 2016, according to IHS Markit, predicted that the installed base of security cameras in North America was expected to grow from just 33 million cameras in 2012 to nearly 62 million by the end of 2016.

CHINA: The history of CCTV cameras in China is obviously shorter than UK and USA, but it moved with inconceivable speed on increasing the number of surveillance cameras. According to IHS Markit, it was predicted that there would be 176 million CCTV cameras in China by 2017. In 2019, According to UK-based research firm Comparitech[3], 8 out of 10 of the most-monitored cities in the world are in China [31]. Based on the trend, IHS Markit predicted that China will reach 626 million[4] by the end of 2020. This means the country will have one surveillance camera for every two people on its streets [31].

[1]UK population is 66.65 million by 2019. https://datacommons.org/place/country/GBR?utm_medium=explore&mprop=count&popt=Person&hl=en

[2]https://www.vice.com/en_asia/article/9keya8/most-surveilled-cities-in-the-world-china

[3]https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

[4]China population is 1398 million by 2019. https://datacommons.org/place/country/CHN?utm_medium=explore&mprop=count&popt=Person&hl=en

2.2 The Effectiveness of Surveillance Cameras on Preventing Crime

One of the biggest reasons people support CCTV cameras is that they were originally created for the purpose of security surveillance (security surveillance system) to anticipate criminal activity: theft, robbery, and many other things in connection with a crime and the activities that are not desirable. Advances in technology now make these cameras not only for viewing directly through the monitor, but they also equipped with a camera recording system using hard drive storage media.

A NACRO[1](National Association for the Care and Resettlement of Offenders) report has summarised the assumptions behind the use of CCTV for crime prevention purposes: deterrence, efficient deployment, self discipline by potential victims or by potential offenders, presence of a capable guardian and detection [32]. The effectiveness of CCTV cameras is the most important concern. In 2002, the UK Home Office research study 252 conducted a systematic review on crime prevention effects of CCTV. The search strategies resulted in 22 CCTV evaluations which were carried out in three main settings: 1) city centre or public housing, 2) public transport, and 3) car parks. Of the 22 included evaluations, 11 of them (50%) found a desirable effect on crime and 5 found an undesirable effect on crime. There are 5 evaluations that found a null effect on crime (i.e., clear evidence of no effect), while the remaining one was classified as finding an uncertain effect on crime (i.e., unclear evidence of an effect) [32].

A meta-analysis was also applied and the results provide a clearer picture of the crime prevention effectiveness of CCTV. Four evaluations were excluded because they did not provide the needed data to be included in the meta-analysis. From the 18 remaining evaluations, it was concluded that CCTV had a significant desirable effect on crime, although the overall reduction in crime was a very small (4%). Half of the studies (nine out of 18) showed evidence of a desirable effect of CCTV on crime. All nine of these studies were carried out in the UK. Conversely, the other nine studies showed no evidence of any desirable effect of CCTV on crime [32].

The meta-analysis also examined the effect of CCTV on the most frequently measured crime types. It was found that: "CCTV had no effect on violent crimes (from five studies), but had a significant desirable effect on vehicle crimes (from eight studies). In car parks, there was evidence that CCTV led to a statistically significant reduction in crime of about 41% in experimental areas compared with control areas [33]."

[1] nacro.org.uk

Overall, conducting from Home Office research in 2002, the best current evidence suggests that: “CCTV reduces crime to a small degree. CCTV is most effective in reducing vehicle crime in car parks, but it had little or no effect on crime in public transport and city centre settings.” [33]

There are evaluations to prove that CCTV cameras have effectiveness on minor offenses, for instance, vehicle crime. However, results do not appear to prove it prevents crime or reduce crime rates efficiently. One application of facial recognition technology is public security which makes people wonder if it would achieve the effectiveness they expected before it was massively applied on surveillance cameras.

2.3 The Architecture of Facial Recognition

In specific application scenarios, facial recognition can be roughly divided into three types: 1:1, 1:N, and N:N. The one-to-one level of face recognition is the most basic “prove you are you”. One-to-one type is the user uploading personal photos in advance and storing them in the system. During each verification, the offline photos are compared with the photo stored in the system to determine whether you are you. For instance, you unlock your phone with FaceID. Unlike one-to-one comparison, 1:N type requires a photo to be compared with a large number of photos in the system, it is about to “prove you are who”, for instance, automated personal identification verification system in the airport. Multiple comparison results are showed according to the similarity, however, the first ranking result may not be accurate. There are many factors could affect the accuracy,like the location of use, environment, light, collection angle and even glass reflection, etc. As for N:N type face recognition, it is actually equivalent to multiple 1:N recognition at the same time, it used to “prove who is who”.[34] The most common face recognition is mainly divided into four modules: face detection, face alignment, face verification and face identification [35]. Figure 2.3 presents that the most common architecture of an automated facial recognition system. There could be a slight difference on names in different working process, for instance, face alignment step is also called face extraction. Some of the architecture combines two steps together or divides one step into multiple steps. Our architecture aims to provide a clear picture to understand how general facial recognition systems work.

Face detection: the camera detects or captures a photo from static images or videos of a human face, it could be alone or multiple people. The image may show the person face features either straight ahead or in profile, the better image resolution, the higher accuracy while matching the face. The face detection step could automatically detect one

or multiple faces from a image or video. The system rectangular crop focused on either all faces or on the biggest face, face cropping step aims to focus on targeted face.

Face Alignment: the facial recognition algorithm starts to analyze an image of the face during this step. Normally the image is 2D instead of 3D because it can more conveniently match a face with public photos or existing database. Before the algorithm analyzes the geometry of input face, the systems extract facial features. The metric is different depends on different algorithms applied, the facial landmarks are normally divided into 68 points[1] (see figure 2.1) or 106 points[2] (see figure2.2). After all the data is extracted, the input face landmarks are recorded.

Face verification: the image will be improved before the face verification step, it will help identify you more efficiently. The input faces are simply cropped out of from the former step on both texture and range images. After normalization, the size of the texture and range images is different from one model to another. During this step, input facial features will be transferred from analog information digital information, those information is essentially turned into a mathematical formula. The numerical code is called a face-print[36], each person has their own unique face-print just like fingerprint.

Face recognition: finding a match with input face from the database. The facial recognition algorithms starts to extract facial features from gallery database to match the digital information collected from the last step. Input face-print is then compared against a database of other known faces. If input face-print matches an image in a facial recognition database, then a determination is made.

However, the match result could be multiple, the performance in reality is worse than those experiments which the lighting and face expressions are under control, especially when it happens to identical twins[37]. After the process, the system will send a result to the user whether the input face is matching the registered identity. The result could be one or multiple depending on the situation and accuracy of the system. For instance, the static image has better accuracy than the image captured from a dynamic video, the image taken under ideal lighting condition is always better than fuzzy background. Therefore the system could provide multiple results which descending order with matching ratio. If there is no correct match, restart the process with a better image or video.

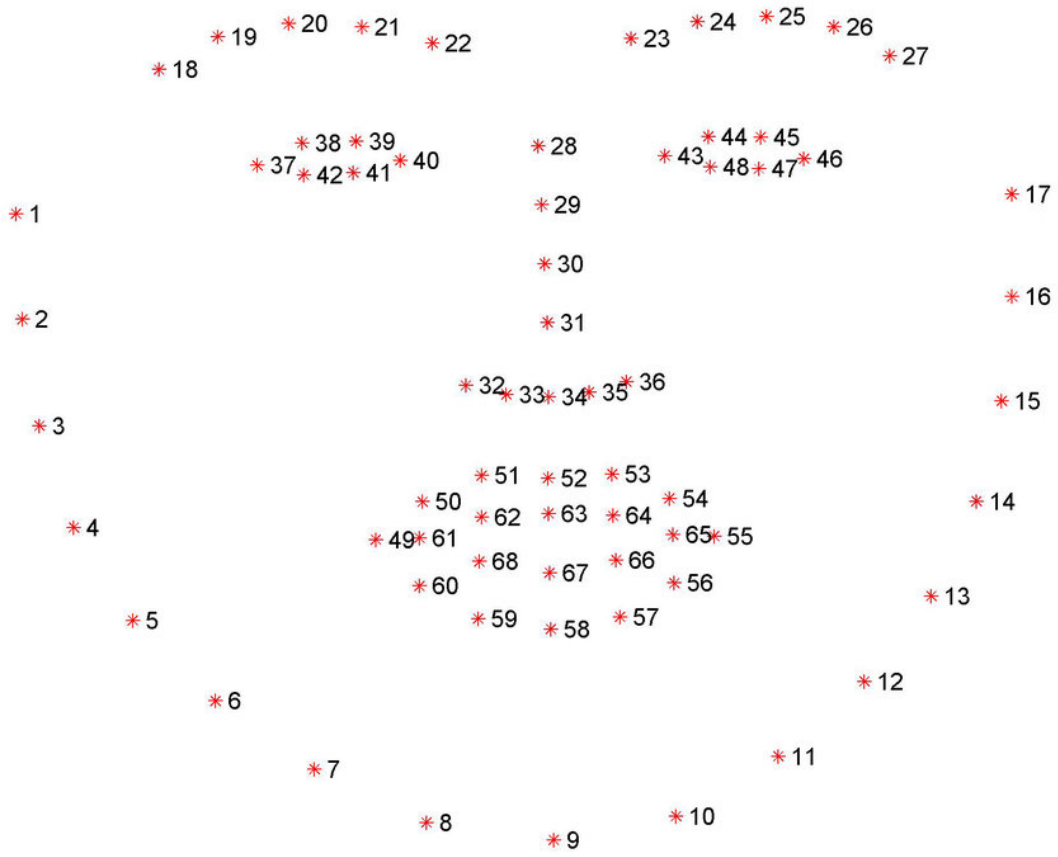


Figure 2.1: The 68-point landmark make-up[1]

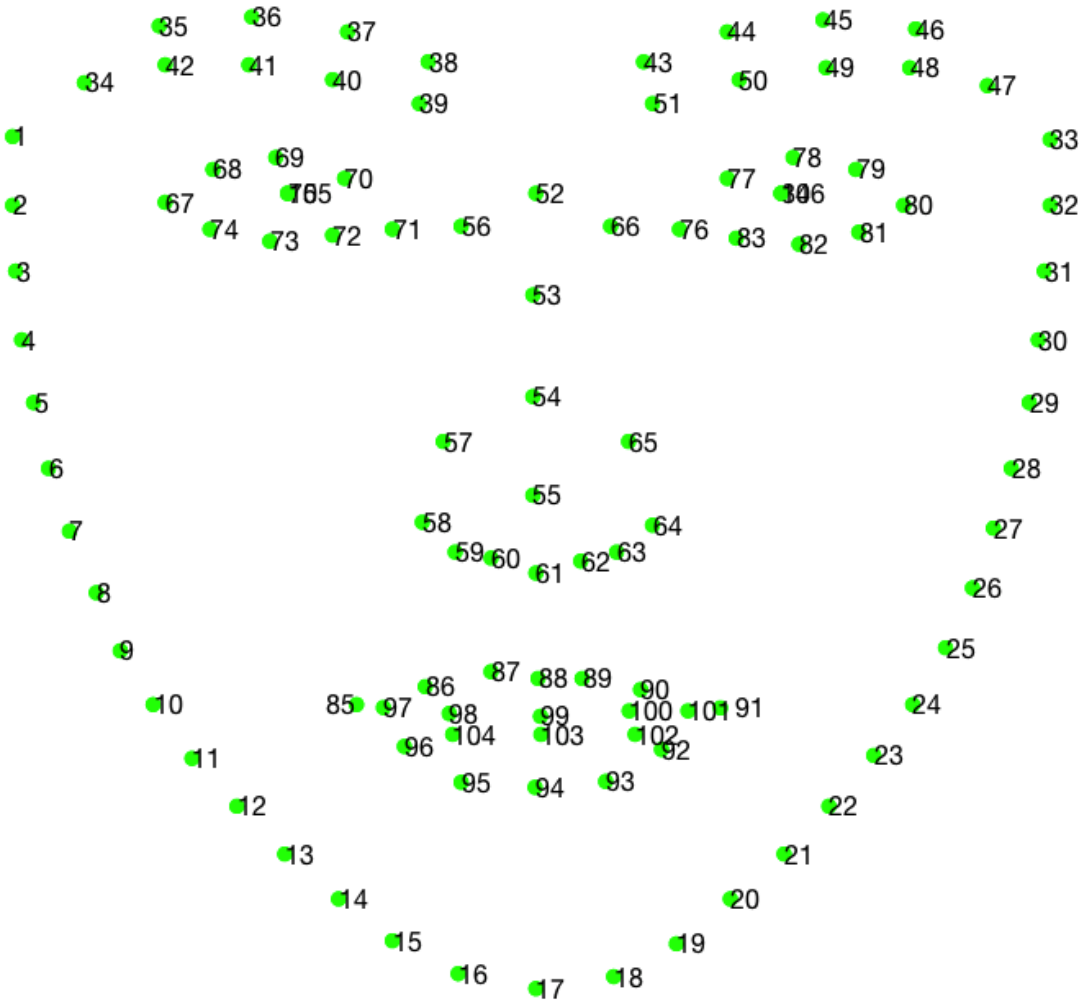


Figure 2.2: The 106-point landmark make-up[2]

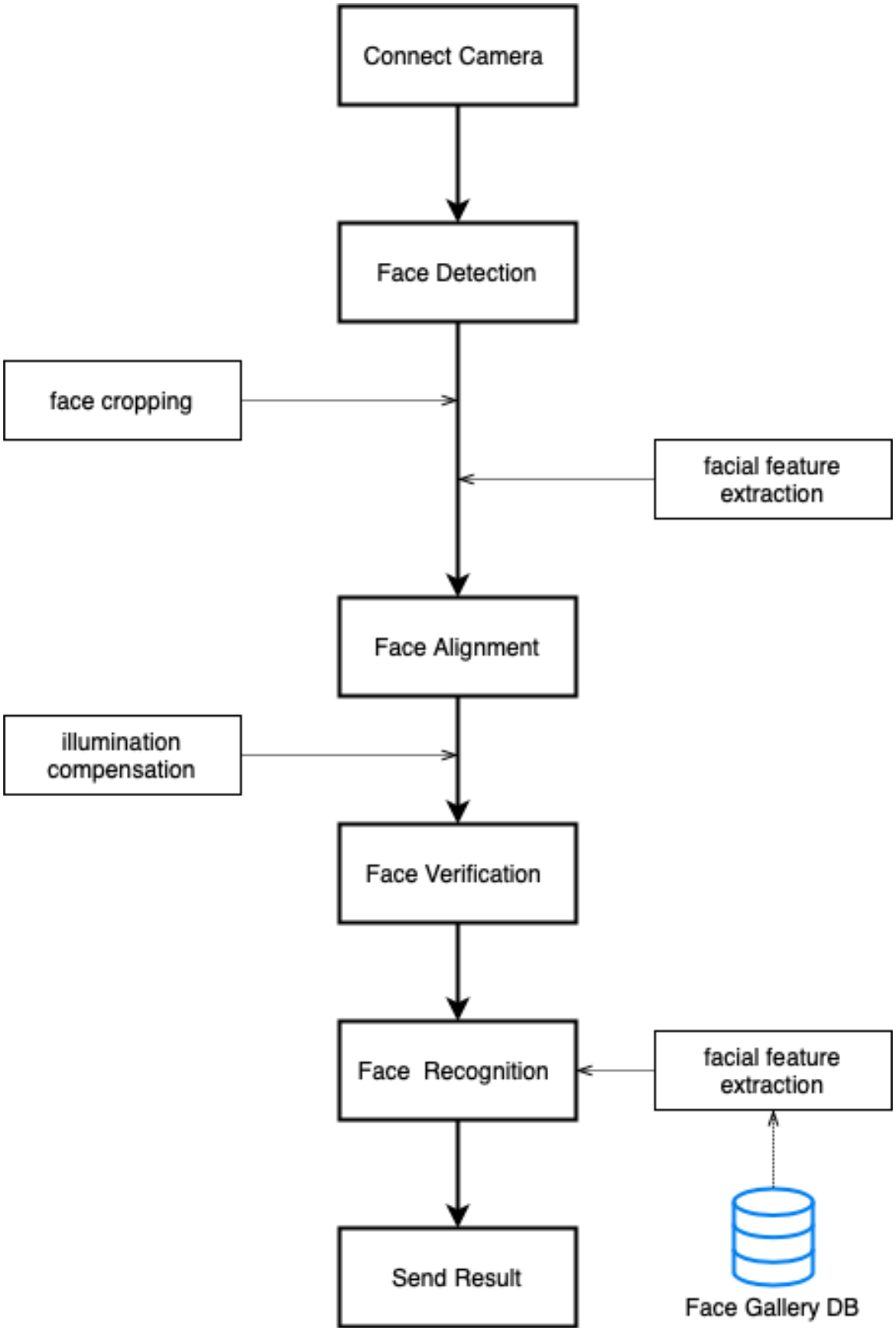


Figure 2.3: Facial recognition processing flowchart

2.4 Algorithms of Facial Recognition

Facial recognition technology can be traced back to 1965; from 1964 to 1966 Woodrow Bledsoe, along with Helen Chan and Charles Bisson of Panoramic Research, Palo Alto, California, researched programming computers to recognize human faces [38]. Research on automated facial recognition has been going on for over 50 years. Now facial recognition algorithms can do more than identify human faces – they can also describe emotions. Since the early 1970s, Paul Ekman and his colleagues performed extensive studies of human facial expressions. They found evidence to support universality in facial expressions. These "universal facial expressions" are those representing happiness, sadness, anger, fear, surprise, and disgust [39].

Typically, the recognition is performed based on an abstract representation of the face image after suitable geometric and photo-metric transformations and corrections [40]. The facial recognition algorithm is a method of building a biometric face model for further analysis and the face recognition process. From different angles, the industry of facial recognition technology has many different classifications. According to the different application scenarios, facial recognition also can be divided into two-dimensional image of face recognition, face recognition for surveillance video, in view of the near infrared, thermal infrared imaging or sketch of multi-modal face recognition and 3D face recognition in depth information, etc. The most common classification is divided facial recognition algorithms into two categories. The geometric approach focuses on distinguishing features based on individual appearance. This method captures the local facial features and their geometric relationships. They often locate anchor points of key facial features (eyes, nose, mouth, etc.), then connect these points to form a net and then measure the distances and angles of the net to create a unique face-print. The photo-metric statistical methods are used to extract face features as values from an image. These values are then compared to templates to eliminate variances.[34]Various face recognition algorithm exist and each has advantages and limitations about which lots of research work has been published [34].

- **EigenFace**

EigenFace is a facial recognition algorithm based on PCA (Principal Component Analysis). The principal elements are selected to represent the human face, because of the shape of the principal element, it is estimated to be a feature face. EigenFace refers to a face recognition method based on appearance, which aims to capture changes in a collection of face images, and use this information to encode and compare the image of a single face

as a whole. A set of characteristic faces is a collection of standardized face components determined by statistical analysis of a large number of face images. It treats face images as random vectors and uses statistical methods to distinguish different face feature. Facial features are assigned mathematical values because this method does not use digital pictures, but uses statistical databases. Each face is a combination of these values in different percentages. As more and more feature vectors are introduced, the reconstructed effect is getting closer and closer to the original image.[41]

Advantages: 1)EigenFace was invented for making the system very efficient specifically. 2) It is efficient in processing time and storage.[42]

Limitations: 1)It is sensitive for lightening conditions and the position of the head. 2)the eigenvectors and eigenvalues are time consuming.[42]

- **FisherFace**

FisherFace is considered as an improvement to the EigenFace algorithm, it is considered more successful in classifying distinction in the training process. R.A Fisher derived linear discriminant analysis (LDA) for face recognition in 1936. It is used to find a subspace that maps sample vectors of the same class to a single point represented by a feature, and combines different classes. The sample vectors are mapped to as far away from each other as possible. The resulting basis vectors that define this space are called FisherFace.[43] LDA averages each category sample, while PCA averages all sample to get the mean face. Since FisherFace only focuses on the different features between various targets, it is unrealistic to hope to reconstruct the original image.

Advantages: 1)It enhances better classification of different classes image than Eigenface. 2) It can classify the training set to deal with different people and different facial expression. 3) It has better accuracy in facial expression than Eigenface. 4) It is more invariant to light intensity.[42]

Limitations: 1)It is more complex than Eigenface to finding the projection of face space. 2)The calculation of ratio requires a lot of processing time. 3) It needs larger storage of the face and more processing time in recognition than Eigenface. [42]

- **Elastic Bunch Graph Matching (EBGM)**

EBGM is an algorithm in computer vision for recognizing objects or object classes in an image based on a graph representation extracted from other similar images[44].The more important part of EBGM is to determine the location of the extracted feature points, so

a template image is needed for positioning. First, the feature points are roughly located according to the face elastic bunch graph (template), and then each point is finely located. After the face to be recognized is extracted as a face image, it is compared with the existing face database in the database, the person with the highest similarity and greater than the preset value is considered the same person. [45]

Advantages: 1) Changes in one feature (eyes open or closed) does not necessarily mean that the person is not recognized any more. 2) In addition this algorithm makes it possible to recognise faces up to a rotation of 22 degrees.

Limitations: 1) It is very sensitive to lightening conditions. 2) A lot of graphs have to be placed manually on the face.

- **Local Binary Patterns Histograms (LBPH)**

LBPH is a efficient texture operator which labels the pixels of an image by threshold the neighborhood of each pixel and considers of the result as a binary number. LBP is to sum the results of the comparison between the pixels of the image and the pixels around it. With this pixel as the center, threshold comparisons are performed on adjacent pixels. If the brightness of the center pixel is greater than or equal to its neighboring pixels, mark it as 1, otherwise mark it as 0. You would use binary numbers to represent each pixel, such as 11001111. Therefore, due to the surrounding 8 pixels, you may eventually get 2^8 combinations, which is called a local binary pattern. The LBP image is divided into multiple blocks, and a histogram is extracted from each block. By connecting local special histograms, these histograms are called local binary patterns histograms.[46]

Advantages: 1) It produces better recognition rates in controlled environments. 2) It is not profound to illumination.

Limitations: 1) It is difficult to do the face identification when the poses of the probe are different. 2)It becomes more difficult when illumination is coupled with pose variation. 3)Faces under extreme facial expressions cause problems for the algorithms 4)Due to other objects or accessories (e.g., sunglasses, scarf, etc.), the performance of face recognition algorithms gets affected. 5)Human face changes over time, like makeup, facial hair or aging, these factors afftect the result.

- **Support Vector Machine (SVM)**

SVMs are a binary classification method. SVM-based face recognition algorithm reformulates the face recognition problem and reinterprets the output of the SVM classifier [47].

Advantages: 1) High recognition rate ; 2) Good performance on computation speed and memory.

Limitations: 1) Need massive training samples (300 each class); 2) Time-consuming; 3) Methods complex; 4) No unified theory.

Facial recognition history is lengthy and this technology is getting more mature over time. In this section, we aim to summarise the most common facial recognition algorithms to the general public. Most facial recognition products on the market applied one or combinations of two or more algorithms on the list. No matter which methods were adopted on the surveillance cameras, we can tell that this technology is not perfect yet; there is still room for improvement to overcome the existing limitations.

2.5 The Public Concerns and Attitudes Toward Facial Recognition

In the last two decades, if people's concerns about being watched over by cameras and invasion of privacy, the new higher concern should turn toward facial recognition technology applied on surveillance cameras. People who behind the camera not only monitoring your action, they also know your identify. The public concerns of facial recognition technology can be divided into two main parts: ethical concerns and technical concerns. The ethical concerns with facial recognition technologies mainly include discrimination against national origin, race, color, religion, disability and sex; transparency and privacy. The technical concerns focus on accuracy and security [8]. The low accuracy could identify your face with the wrong ones, even worse, it could be accused as a criminal. Individual face as unique identify, it could be misused in the wrong hands if the system is hacked, therefore, the security concern is highly regarded.

2.5.1 Ethical Concerns: Discrimination

Joy Buolamwini and Timnit Gebru measured the accuracy of 3 commercial gender classification algorithms (MSTF, Face++ and IBM) on the new Pilot Parliaments Benchmark(PPB) in 2018 which is balanced by gender and skin type[3]. All of the companies offered free trail of facial analysis API services. Microsoft and IBM have made large investments in artificial intelligence and provide public demonstrations of their facial analysis technology. Face++ is a Chinese computer vision company with facial analysis technology.[3] Based on collected data from the report, we illustrate the results with column charts (see Figures 2.4, 2.5, 2.6). These figures presents the results of gender classification

performance[1] as measured by 3 evaluated commercial classifiers on the PPB dataset. All classifiers performed the best for lighter individuals and males overall. The classifiers performed worst for darker females, with error rates of up to 34.7%. The same group error rate for lighter females is 7.1% and for lighter males is only 0.3%.(see table 2.1)

From the Gender Shades report, we can see that automated facial recognition technology exhibits gender bias and discrimination issues. The substantial disparities in the accuracy of classifying darker females (DF), lighter females (LF), darker males (DM), and lighter males (LM) in gender classification systems require urgent attention. Commercial companies need genuine and accountable facial analysis algorithms for their products [3].

Classifier	Metric	All	F	M	Darker	Lighter	DF	DM	LF	LM
MSFT	PPV(%)	93.7	89.3	97.4	87.1	99.3	79.2	94.0	98.3	100
	Error Rate(%)	6.3	10.7	2.6	12.9	0.7	20.8	6.0	1.7	0.0
	TPR(%)	93.7	96.5	91.7	87.9	99.3	92.1	83.7	100	98.7
	FPR(%)	6.3	8.3	3.5	12.9	0.7	16.3	7.9	1.3	0.0
Face++	PPV(%)	90.0	78.7	99.3	83.5	95.3	65.5	99.3	94.0	99.2
	Error Rate(%)	10.0	21.3	0.7	16.5	4.7	34.5	0.7	6.0	0.8
	TPR(%)	90.0	98.9	85.1	83.5	95.3	98.8	76.6	98.9	92.9
	FPR(%)	10.0	14.9	1.1	16.5	4.7	23.4	1.2	7.1	1.1
IBM	PPV(%)	87.9	79.7	94.4	77.6	96.8	65.3	88.0	92.9	99.7
	Error Rate(%)	12.1	20.3	5.6	22.4	3.2	34.7	12.0	7.1	0.3
	TPR(%)	87.9	92.1	85.2	77.6	96.8	82.3	74.8	99.6	94.8
	FPR(%)	12.1	14.8	7.9	22.4	3.2	25.2	17.7	5.2	0.4

Table 2.1: Gender classification performance: MSFT, Face++ and IBM[3]

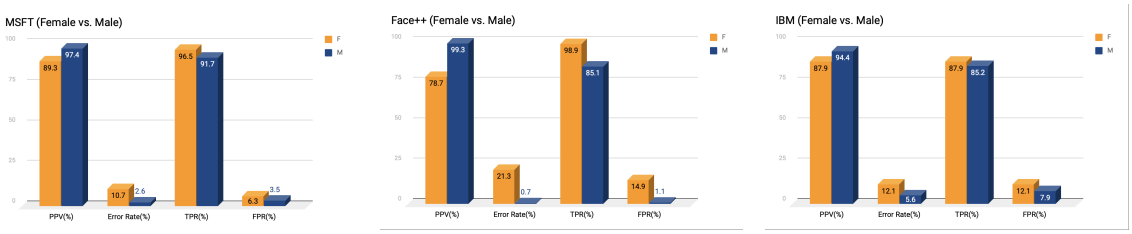


Figure 2.4: Gender classification performance: Female vs. Male[3]

2.5.2 Ethical Concerns: Transparency & Privacy

It is common knowledge that organizations and governments are storing our personal data. Every individual's face is unique and it can be used as our identification like fingerprints.

[1]PPV: positive predictive value; Error Rate: (1 - PPV); TPR: true positive rate; FPR: false positive rate

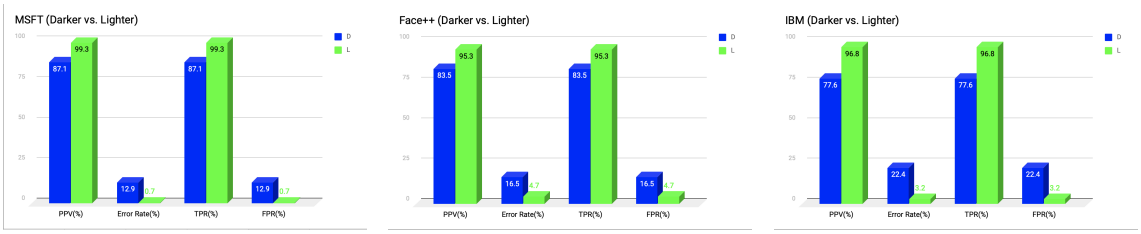


Figure 2.5: Gender classification performance: Darker vs. Lighter[3]

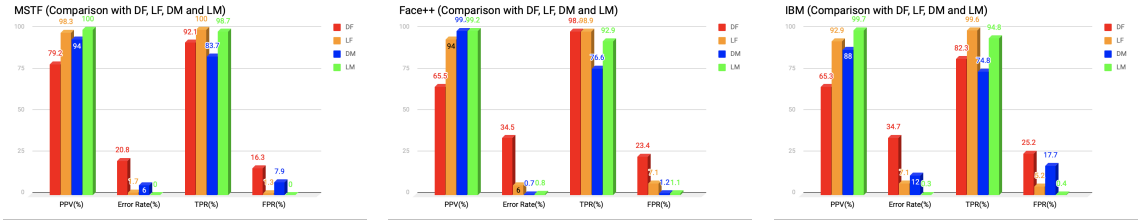


Figure 2.6: Gender classification performance: General comparison[3]

The technology has the potential to be deployed semi-covertly on existing CCTV cameras. The Russian app FindFace applies face recognition with the intention for users to find people on the social network VKontakte but was actually used to harass people by exposing very personal details. Earlier this year, the biometric database of India was leaked and unauthorized access to personal information of India's citizens was enabled. Stored face images are particularly prone to misuse, especially most digital images now contain embedded EXIF data, which likely included date/time/location. Anyone with access to the images can gather personal information and hack into accounts. Stored face images pose the risk of misuse, unauthorized tracking and identity theft.[48]

In specific guidance regarding police use of live facial recognition technology, transparency on the part of a relevant authority is key element of public interest when operating facial recognition technology in public places. Not only are these legislative requirements, they are essential contributing factors to earn the public trust and confidence in the applying of surveillance camera systems.[49]

Facial recognition technology also raises questions of trust and transparency, privacy and autonomy. As the lines between public and private space become increasingly blurred, it is not clear to people how the technology works, when it is being used, and by whom it is being deployed. This troublesome reality signals the end of our basic public anonymity as we know it. This is one of the many reasons why face images are now considered as sensitive personal information. This not only undermines public trust in the technology,

but also normalises surveillance and deprives individuals of agency when it comes to the privacy and protection of their personal data.

2.5.3 Technical Concerns: Accuracy

The GaussianFace algorithm developed in 2014 by researchers at The Chinese University of Hong Kong achieved facial identification scores of 98.52% compared with the 97.53% achieved by humans [50]. In June 2015, FaceNet achieved a new record accuracy of 99.63% ± 0.9% [51]. According to a 2018 NIST report, NIST found a 0.2% of searches error rate in searches of a database containing 26.6 million photos [52].

Those results were obtained under good stable environment. However, the situation in reality is more complex; facial recognition accuracy can vary significantly based on a wide range of factors, such as camera quality, light, distance, database size, algorithm, the subject's race and gender [19]. In July 2018, Newsweek reported that Amazon's facial recognition technology falsely identified 28 members of the US Congress as people arrested for crimes [19]. Trials of live facial recognition technology in policing contexts in the UK have reported more than 90% incorrect matches [53]. This exceptionally high error rate reflects the challenges of deploying the technology outside of controlled development environments. Much more work needs to be done to design and conduct rigorous field tests of live facial recognition technology in a range of policing contexts before the technology can be said to be fit for purpose. Facial recognition matches should be viewed in the context of other compelling evidence, and not be used as the sole determinant for taking action.

2.5.4 Technical Concerns: Security

With the growing use of face images, the databases get larger and consequently, also the risk of hacking and violation of privacy rights grows. Biometric data can reveal a range of intimate information about an individual and the context in which they live. The consequences of its misuse, abuse, loss, or theft are potentially more grave than the loss of other personal data. For instance, if one's bank details are stolen, they can be changed, but one can't easily change biometric data such as one's face or fingerprints. Usually three methods of spoofing attacks are used against the facial recognition systems: image-spoofing, video-spoofing and 3D-mask spoofing. An image of the person's that was initially authenticated, a pre-recorded video of the victim or a 3D-masked printed are the usual methods of hacking the live facial recognition systems [54]. Earlier in 2018,

DeepFake technology boomed on the internet. DeepFake takes someone's existing images or videos and replaces them with someone else's by using a pre-trained generative adversarial network[55]. According to an experiment by Korshunov and Marcel, "the state of the art face recognition systems based on VGG and Facenet neural networks are vulnerable to Deepfake videos and fail to distinguish such videos from the original ones, with 85.62% and 95.00% false acceptance rates (on high quality 128 * 128 model) respectively[55]."

There are still a lot of challenges for existing facial recognition algorithms. The use of intrusive new facial recognition technologies must be subjected to a process of thoughtful and deliberate security. In particular, a technology's intrusiveness must be balanced against the security benefits it would bring. The burden is on the technologists to demonstrate that their solutions will actually be effective in making people safer.

2.6 Relevant Article

In September 2019, the Ada Lovelace Institute summarized a report from a survey of public attitudes toward the use of facial recognition technology in the UK. British public attitudes toward facial recognition technology are valuable for those countries or commercial companies which are trying to apply this technology in real life. The key messages of this report can be concluded as follows [8]: 1) General public's awareness of facial recognition technology is high, but knowledge about it is low, particularly with respect to the limitations of the technology. 2) Consent is an important safeguard for many people, with nearly half of the public expressing the belief that they should be able to opt out of, or consent to, facial recognition technology. 3) People fear the normalisation of surveillance, but the majority support facial recognition technology when there is a demonstrable public benefit and there are appropriate safeguards in place, warranting greater investment in testing and articulating the potential public benefits of such technologies. 4) There is no unconditional support for police to deploy facial recognition technology; rather, support is conditional upon limitations and subject to appropriate safeguards. 5)The public does not trust the private sector to use facial recognition technology ethically, necessitating further dialogue between the public, private sector and policy-makers in order to understand and address this lack of trust. 6) The public expects the government to be placing limits on the use of facial recognition technology, including by the police, and supports companies pausing sales of the technology in the intervening time.

2.7 Summary

Facial recognition technology development has a short history compared with the growth of CCTV cameras, but there is no doubt that it bring surveillance cameras to a higher controversial level. This technology can bring convenience and multiple assistance to our lives in different domains. However, it did not affect the general public's concerns. The accuracy facial recognition technology has achieved amazing success, to the point it could deliver a zero error rate under some condition (see Table 2.1). However, it causes discrimination problems at the same time. When a new technology is being applied, we expect everyone to be treated equally so our privacy is secured. Our face as biometric data is our identity like fingerprints; we desire thoughtful and highly intensive security measures to protect it. Based on the British report from the Ada Lovelace Institute in 2019, the general public does not have enough correct awareness and impartial perception of facial recognition technology. All these years with many different facial recognition algorithms getting mature, the public starts to come into contact with products with facial recognition function. Ethical problems and technical problems are still two main issues to deal with. The general public has conflicting attitudes when they face this technology. The public's attitude depends on how they provide better services to life, also with correct regulations just in case it is abused in wrong hands under wrong circumstances.

3

Research Plan

In this section, we present how we are going to answer the second research question. By referring Goodman, Elizabeth, et al., editors *Observing the User Experience: A Practitioner's Guide to User Research.* 2nd ed., Elsevier, 2012. "User research is the process of figuring out how people interpret and use products and services[22]."

3.1 Research Goals

In this thesis, one of our goal is to disclose the general public attitudes and perceptions about facial recognition technology applied to surveillance cameras. It is necessary to know what the public want and think directly. More specifically, we aim to figure out what factors influence their attitudes. And, how informed is the general public concerning facial recognition technologies and how does that impact their attitudes.

Our goal can be formalized by following the Goal-Question-Metric approach as follows [56]:

Purpose	Identify and access
Issue	the public attitudes and influencing factors
Object	of applying facial recognition technology on surveillance cameras techniques
Viewpoint	from all the survey respondents' point of view.

3.2 Questionnaire Design

3.2.1 Questionnaire Introduction

Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours[4].

Facial recognition is mostly used for security purposes, though there is increasing interest in other areas of use, like entertainment, mobile payment, immigration control and others[57]. In fact, facial recognition technology has received significant attention as it has potential for a wide range of applications related to law enforcement as well as other enterprises.

In the questionnaire, we want to learn the general public's attitudes and perceptions of facial recognition technology applied to Closed Circuit Television (CCTV) cameras. Participation in this questionnaire is very important to us. The questionnaire is to help us understand the needs and desires of the people experiencing facial recognition technology. All answers are confidential and will be used strictly for university education research. There will be no sales or marketing follow-up because of one's participation in this questionnaire. This questionnaire is being administered for a master thesis research. This questionnaire runs from October 23, 2019, until November 6, 2019. This questionnaire is expected to take approximately 10 minutes to complete.

3.2.2 Questionnaire Audience

This questionnaire is designed for everyone who is willing to tell the attitude towards facial recognition technology. In order to reduce the bias of the questionnaire results, some criteria are set out for target audience:

- No family or same group members - Since your family or your team members could know what you are doing, their answers could be affected by your daily communication.

- No facial recognition algorithms developers - they know too much about this technology.

- No people who depend on facial recognition technology for a living - their attitudes and opinions are influenced by their benefits, their knowledge could affect their attitudes.

- No audience under 18 years old - Since facial recognition technology is controversial, we do not want to influence juveniles.

- Limit to one response - Each respondent can only fill in the questionnaire once.

3.2.3 Questionnaire Timetable

We have decided the overall goals for the questionnaire, then we need to set the schedule for the process. We saved 2 weeks for writing questions and making online form. Once the questionnaires have been sent out, no changes can be made to maintain statistical validity; therefore, we did 6 pre-tests and redesigned the questionnaire after receiving feedback from the respondents. We followed the schedule as below(Table 3.1).

Timing	Activity
t-1 week	Determine target audience and research goals, start writing questions.
t-2 week	Finish writing questions. Write report draft. Choose an online questionnaire provider.
t-1 week	Do some pre-testing. Improve the questionnaire based on feedback.
t-2 week	Fielding questionnaire and collecting data.
t-4 week	Analyse data.
t-6 week	Write report.

Table 3.1: Questionnaire schedule

3.2.4 Questionnaire Method

According to Goodman, Elizabeth, et al., editors *Observing the User Experience: A Practitioner's Guide to User Research.* 2nd ed., Elsevier, 2012. In our questionnaire all questions are chosen as *closed ended questions*. In general, open-ended questions require much more effort from the person answering them and from the analyst[22]. For the closed-ended questions, we apply a *single answer with multiple-choice* questions and *checklist* questions (see Appendix - 1). Single answer with multiple-choice has a range of choices for the respondent, only one of which may be picked. Checklist question provides options for the respondent, one or multiples of which may be picked.[22]

3.2.4.1 Likert Scales

For some questions which have multiple-choice answers, we apply Likert Scaled. Normally, it consists of one or more statements followed by a choice of three, five or seven options which define a possible range of answers, including a neutral choice [22]. Well-designed Likert items exhibit both symmetry and balance[58]. Symmetry means that they contain equal numbers of positive and negative positions whose respective distances apart are bilaterally symmetric about the "neutral". Balance means that the distance between each

candidate value is the same[58]. In this questionnaire, for any questions applying Likert scales, we illustrate the typical five-level Likert items: strongly agree, agree, neutral, disagree and strongly disagree. For instance, question 12 states: How much do you agree with the statement: “The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology?"

3.2.4.2 Scale from 1 to 5

For some questions on rating typically applied a scale from one to ten[22]. It is a general and largely vernacular concept used for rating things, people, places, ideas, and so on. The scale has 10 as a maximum score, as a denotation of exceptionally high quality or of another attribute, usually accompanying 1 as its minimum. For matching the Likert Scale, we will illustrate five options 1 - 5 which 1 stands for not comfortable at all, 5 stands for very comfortable. For instance, question 15 states: “On a scale of 1 to 5, where 1 is very comfortable and 5 is not at all comfortable, how comfortable are you with the police using facial recognition technology?”

3.2.5 Questionnaire Criteria

Based on Goodman, Elizabeth, et al., editors *Observing the User Experience: A Practitioner's Guide to User Research.* 2nd ed., Elsevier, 2012. Some criteria were applied before finishing the final questions:

- No negative questions - Negative questions are more difficult to answer and easier to misunderstand compared to the positive versions.

- No overload questions - Each individual question only contains one concept. If there are multiple concepts linked, we divided them into separate individual questions. This whole questionnaire contains 27 questions; some two or more multiple questions can be combined together when analysing data, for instance, question 9 “What would be the primary reason for you to use FaceID to unlock your mobile phone?” and question 10 “What would be the primary reason for you to NOT use FaceID to unlock your mobile phone?”.

- Avoid bias - The last thing we want is that the survey respondent feels offended after finishing the questionnaire. To avoid this, we tried to provide comprehensive options for each question.

- Avoid extremes - Since facial recognition technology is controversial, we avoided asking extreme questions which related to the need or behaviour in real life.

- Be specific - In this questionnaire, we do not use fuzzy meaning words in the questions, like “sometimes”, “any”, or confusing abbreviations like “k” which could be abbreviation of kilo or thousand.

- Stay consistent - We use similar wording for all questions and the answer options are in the same order.

- Make questions relevant - although facial recognition technology has developed so fast in recent years, some people still do not notice it. We make the questions list related to people’s experience and life which can be easier to confront.

- Comments - At the end of the questionnaire, we leave space for any comments for people to provide their extra opinions about the questionnaire or the questions.

3.2.6 Questionnaire Text

According to Goodman, et,al., “There are three question categories are included in this questionnaire: characteristic, behavioral and attitudinal categories.”[22]First step is brainstorming to list all the highlights of public concerns about facial recognition. Combing with literature work has done in Chapter 2, we list the scenarios could apply facial recognition technology in public. Then we talk with the person whose working field related to facial recognition about the current situation developing this technology. We modified the questionnaire referring to British survey Beyond face value: public attitudes to facial recognition technology in September 2019[8]. Then we start the pre-test, their feedback and comments help to improve the questionnaire again. After the final typing and peer review, the questionnaire is translated into Chinese and Dutch version.

This questionnaire is divided into four parts: First, an introduction that presents the purpose and basic information about this questionnaire. Second, we start from the easy basic questions about the survey respondent, for instance, their age, gender and working field. Third, we provide a surveillance camera applied facial recognition to survey respondents who are optional to experience it. Since the face will be collected, and this technology is controversial in Europe, the survey respondent’s permission is required. Therefore, we attract respondent’s interest with alternative question which is close to reality, like whether they use FaceID to unlock their phone. The follow-up questions will be level up to the

situation in the society and what kind of area they want or do not want facial recognition technology are applied. Finally, we ask objective questions based on respondent's experience and life to express their attitudes and opinions.

The whole questionnaire will be attached in an Appendix. The questions marked with red asterisk (*) are required. The online questionnaire was performed using Google Forms in two different languages, English[1] and Dutch[2]; and Tencent Questionnaire in Chinese[3], respectively.

3.3 Questionnaire Responses

3.3.1 Valid Questionnaire Criteria

- Questionnaire respondent must answer all required questions.
- Questionnaire respondent has potential positive or negative prejudice of facial recognition technology, for example, all questions about attitudes and opinions for this technology only limited to "strongly agree" or "strongly disagree".

3.3.2 Valid Responses

We have received the replies from all the survey respondents, the Chinese version responses are 180, English and Dutch versions are 56 and 20, respectively. Based on the inclusion and exclusion criteria, in total we received 251 valid responses during two open weeks. Each respondent spent 7 minutes and 14 seconds to complete the questionnaire on average.

3.4 Follow-up Questions

We proceed with follow-up questions with people chosen from among the survey respondents. Each one will answer the same questions, but the details could be different based on their answers if necessary. We cannot share any information or opinions during the process. Because of COVID-19 situation and the fact that our survey respondents are from different countries, it is not suitable to have face-to-face meeting now. We conducted to do the interviews one by one.

[1] https://docs.google.com/forms/d/1Iyj5kcXkGJmeQRBl4m6162_vkVw01dzmYfmqtzFXQ1g/edit?usp=sharing

[2] https://docs.google.com/forms/d/1ypMC6bD74pSLOnGNjcdDxSd3UiEW7W0sCaq7B-Vqqcg/edit?usp=sharing

[3] https://docs.google.com/document/d/1otRTz4RqvObDHGS6n0ZmReg0Z7JORZ6bzL0I9QnvCD0/edit?\usp=sharing

4

Research Analysis & Results

In this section, we present how we analyzed the collected data from the surveys. All the data and output aim to help us address second and third research question: what attitudes exist toward using facial recognition technologies on CCTV cameras as one security measure? What factors affect the public's attitudes? To answer these questions, we clarified the public's attitudes of facial recognition technology as one security measures on different purposes into five levels: *Strongly agree, Agree, Neutral, Disagree and Strongly disagree.* Based on the literature study, the public's concerns focus on privacy, accuracy, security, convenience and if they can believe facial recognition technology is being used by the right hands under appropriate regulations. First, we chose the survey respondents from different backgrounds - *Age range, Gender, Education level, Nationality and Working field* are all considered as one security measures on different scenarios. The general public attitudes could change depending on the various situations; for example, using facial recognition to help identify criminals, helping prevent crimes occurring, deterring terrorists or bringing criminals to justice.

First, we are going to present the general result about the survey which it can provide the direct simple information about the response from the survey respondents. We transform these into a form that is easier to work with. All approaches to coding aim to help researchers organise their data in order to make sense of it. During the report, we put the most important focus on the significant results of the study. To view the full output of the data, researchers and readers can find it from Google drive[1].

[1] `https://docs.google.com/spreadsheets/d/1LXXJ_Xq9ZLkNy1Cj7Wr2pqrHeVdDTZi1JInmpf2ClNA/edit?usp=sharing`

4.1 Analysis Tool

When we start to analyse the valid data, there chose two different analysis software tools: Microsoft Excel and IBM SPSS during this process. We aim to analyze all the data thoroughly, each question from questionnaire is presented by tables, histogram and pie chart. Each statistical test compares each variable and each group. We select the best quality graphs and the most appropriate results to display.

To better analyze the collected data, we set up a few measurements. We apply numbers to objects according to a set of rules[59].

Nominal Data: assign numbers to objects where different numbers indicate different objects. The numbers have no real 'meaning' other than differentiating between objects.For instance, on question 2 we assign different genders, Male = 1; Female = 2 ; Prefer not to say = 3. It does not matter what number we come up with as long as same object got the same number. It does not mean that because females have a higher number that they are better than males or males are worse than females or vice versa or anything like that. All it does is differentiate between two groups. It is nominal because the number just simply differentiates between objects.

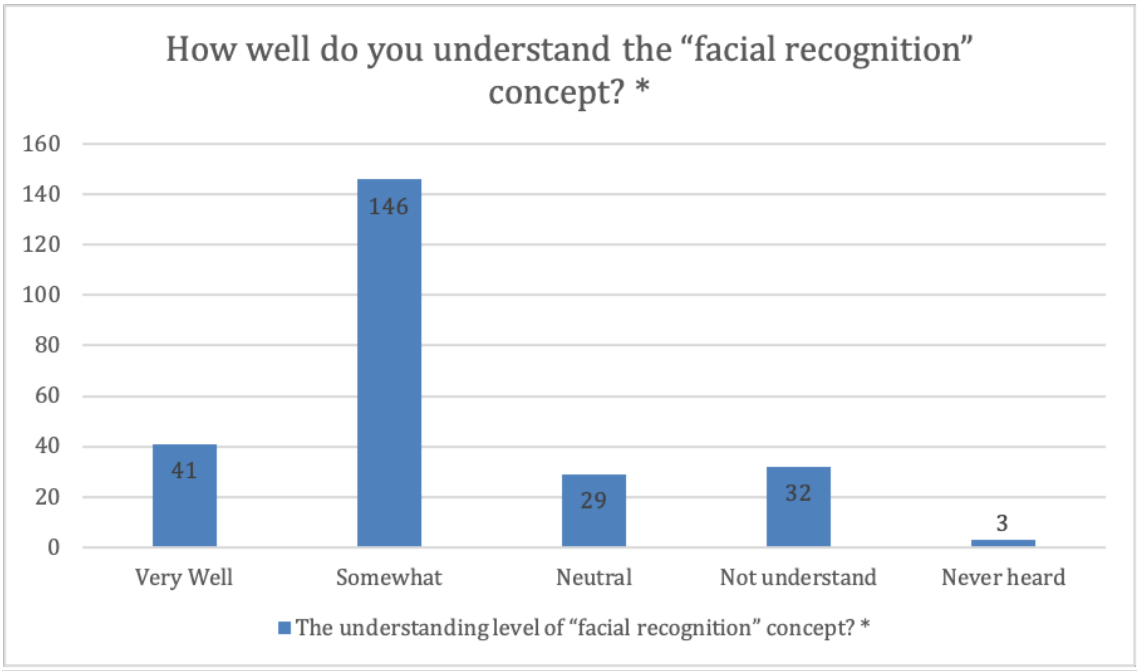
Ordinal Data: assign numbers to objects (like nominal data), but here the numbers also have meaningful order. For instance, question 13, number indicates the feeling strength: 5 is better than 4, and so on.

Interval: numbers have order (like ordinal), but there are also equal intervals between adjacent categories, in our case we assign one.

4.2 General Results

In 251 valid responses from all the survey respondents, we received 103 (41%) replies from male, 144 (57.4%) replies from female, respectively. For the age difference, between 18 to 30 years old are majorities which occupied 61.4%, respondents from 61 to 70 years old and over 70 are minorities, both take up 4% separately. We aim to receive fair data from the population, we handed over surveys to people who have different education level and working field. Bachelor or equivalent education accounts for the biggest number, 47,8%. People who have computer science and engineering background take up 29,5% in all respondents; remainder from different work fields. Because of the high population mobility and high development of facial recognition, the valid Chinese version survey replies take up 70,9%.

All the valid responses, survey respondents chose option of understanding the facial recognition concept *Very well* and *Somewhat* account for 74.6% (16.3% and 58.6% separately), and 201 respondents chose *Internet* as the sources for knowing about facial recognition technology (see figure 4.1).



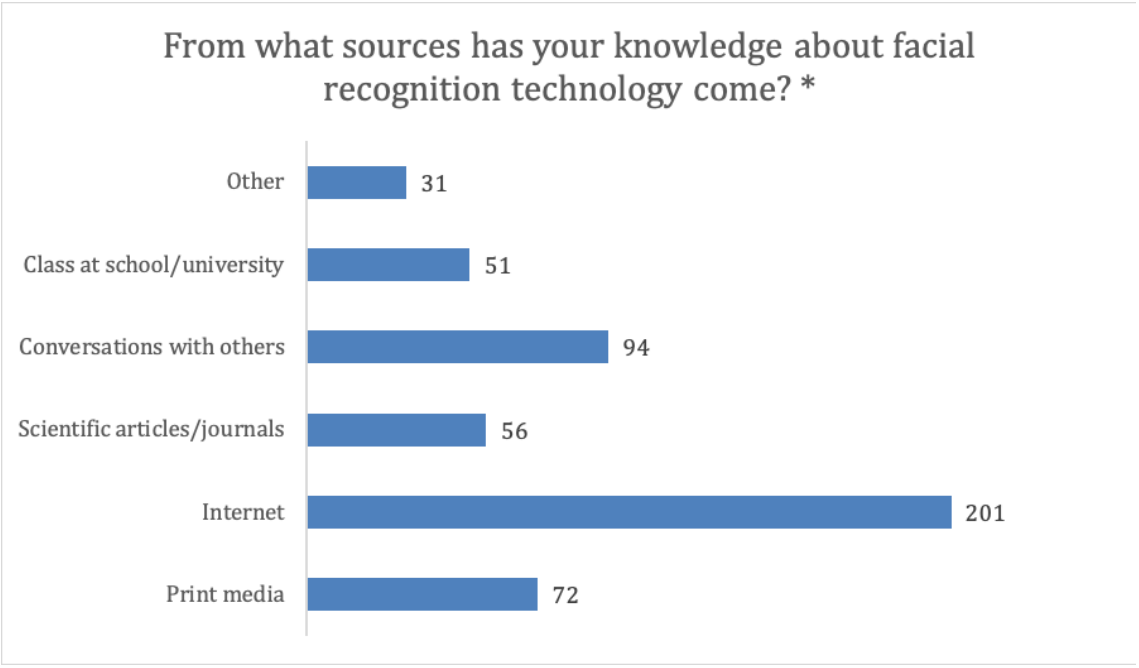


Figure 4.1: How well the survey respondents understand the "facial recognition" concept and from what sources

The closest experience of using facial recognition for the public is on Apple products which provide FaceID function to unlock your phone. Comparing traditional methods to unlock your mobile phone, survey respondents willing to use *FaceID*(81) only takes up half percentage of *Finger prints*, the second popular measures are *Passwords* which are 155 still is far ahead of *FaceID*(see figure 4.2). The primary reason of using *FaceID* is *Faster* which it proves that facial recognition technology did bring convenience to our life. However, the public concerns about security issues occupied the biggest numbers (see figure 4.3).

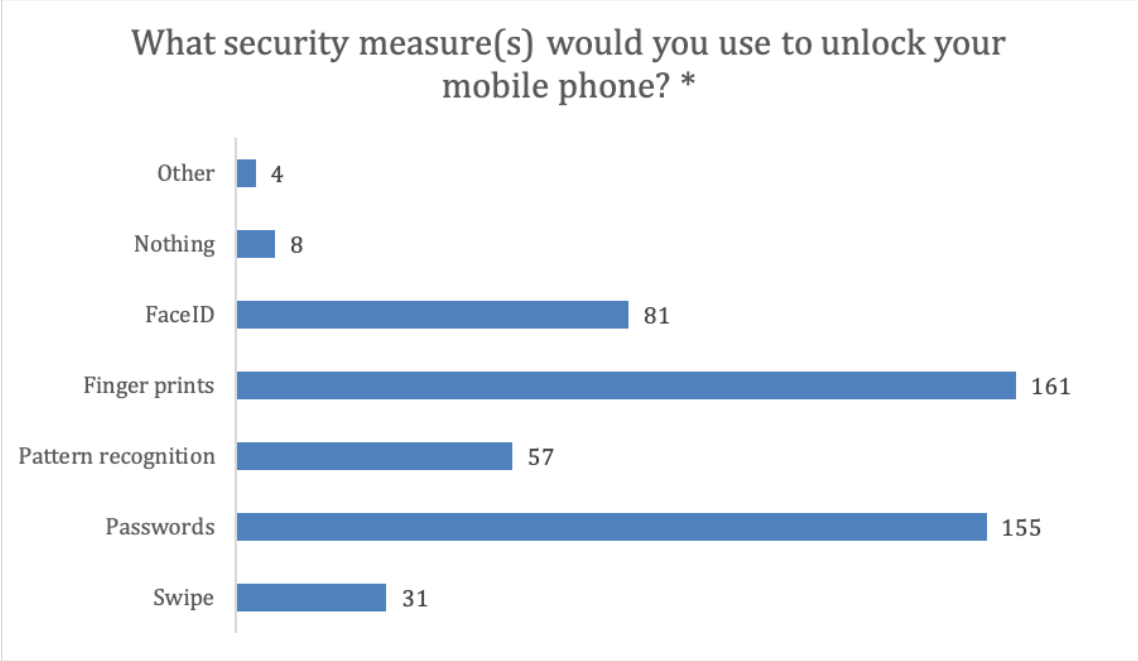


Figure 4.2: Security measures to unlock your mobile phone

Facial recognition technology applied on surveillance cameras is a controversial application. However, people's attitudes could be changed based on different purposes (see figure4.4). The bar chart illustrates that when facial recognition is applied to protect the public's safety and serve public service, for example by police in a criminal investigation, in airports checkpoints, on public transport to identify persons of interest for the police, the public highly supports this application. When it is related to personal privacy, especially when it is applied at work to monitor personality traits and mood of candidates when hiring for a job, in schools to monitor pupils' expressions and behavior, and in supermarkets to track shopper behaviour around the store and target products at shoppers, the public's attitudes change to unsupported. People are concerned about violations of their personal

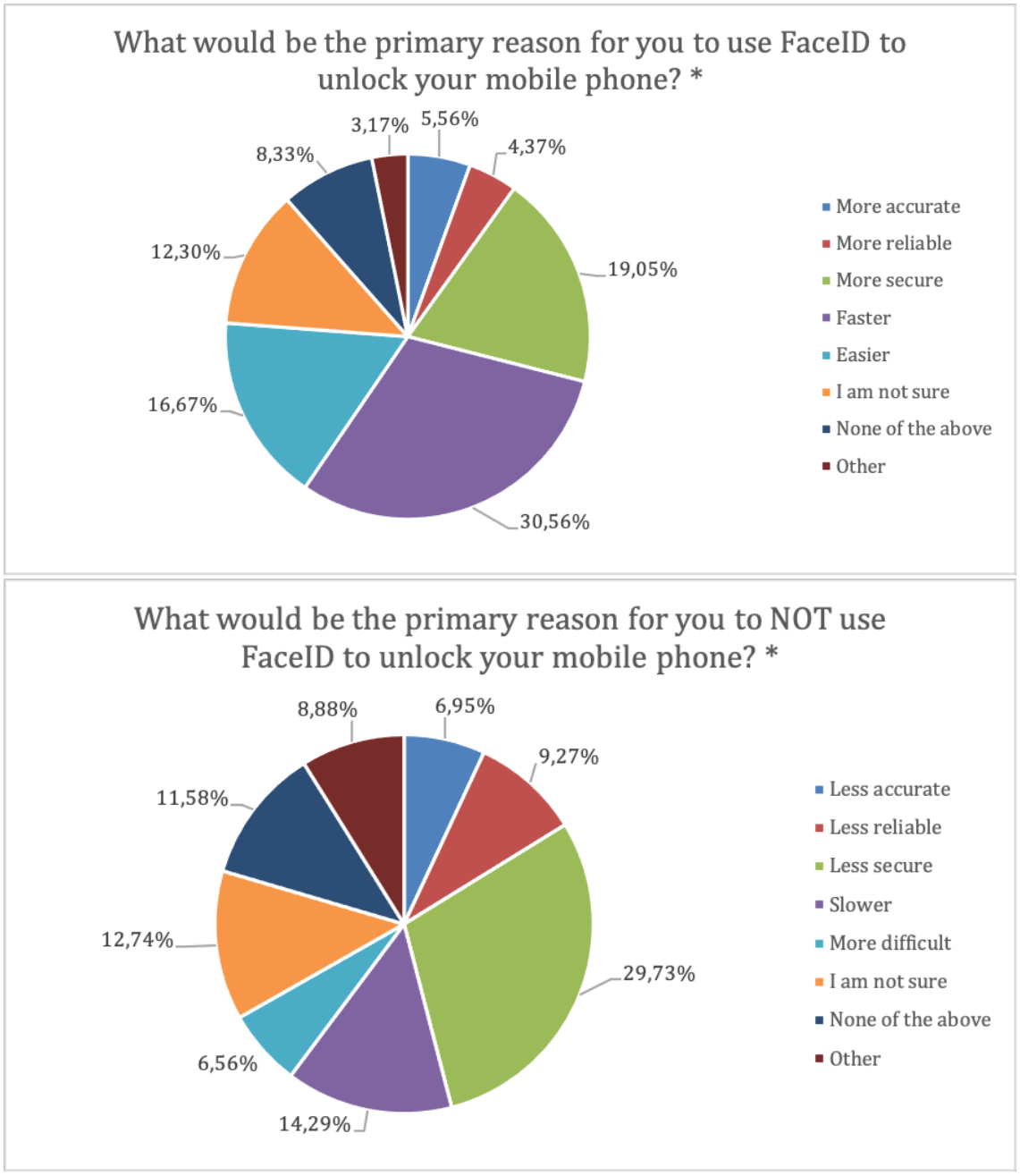


Figure 4.3: Comparison of the primary reason for survery respondents to use or not use FaceID

privacy obviously.

For police using facial recognition technology to investigate crimes and identify persons of interest, the public are willing to support it, but when it comes to day to day policing, the numbers of supporting this technology drop. We list the reasons why the public agreeing

and disagreeing with police using of facial recognition technology. For agreeing reasons, the public believe it is beneficial for the security and it enhances existing security systems. Of course, personal security benefit is a good reason too (see figure 4.5). For disagreeing using the technology, the most significant reason is that is will be misused or hacked (see figure 4.6). Facial recognition technology applied by police still needs better technical and ethical regulations.

From the general result, we acquire some information to answer the research question. 74.6% survey respondent understand the facial recognition concept on *Very well* or *Somewhat* level. The general public require information about facial recognition technology from *Internet*(201). In our daily life, the public experienced or willing to experience *FaceID* to unlock phone only takes up 81 respondents which only occupied half of *Finger prints*. The survey respondent chose *Faster* as the primary reasons willing to use facial recognition which indicates the general public think it is convenient. And concerns of why the public not to use facial recognition, we concluded that *Less secure* is the primary reason. The security concerns can divided into personal information secure and public security, *By police in criminal investigation* and *In airports security checkpoint* are the most supported scenarios. *At work to monitor personality trails and mood of candidates when hiring for a job* and *In supermarkets to track shopper behaviour around the store and target products at shoppers* are the most unsupported scenarios on applying facial recognition in different purposes. The general public agree with police use of facial recognition technology because *It is beneficial for the security of society* and the disagree reason is *It will be misused or hacked* which reflects back to public security and personal information secure concerns.

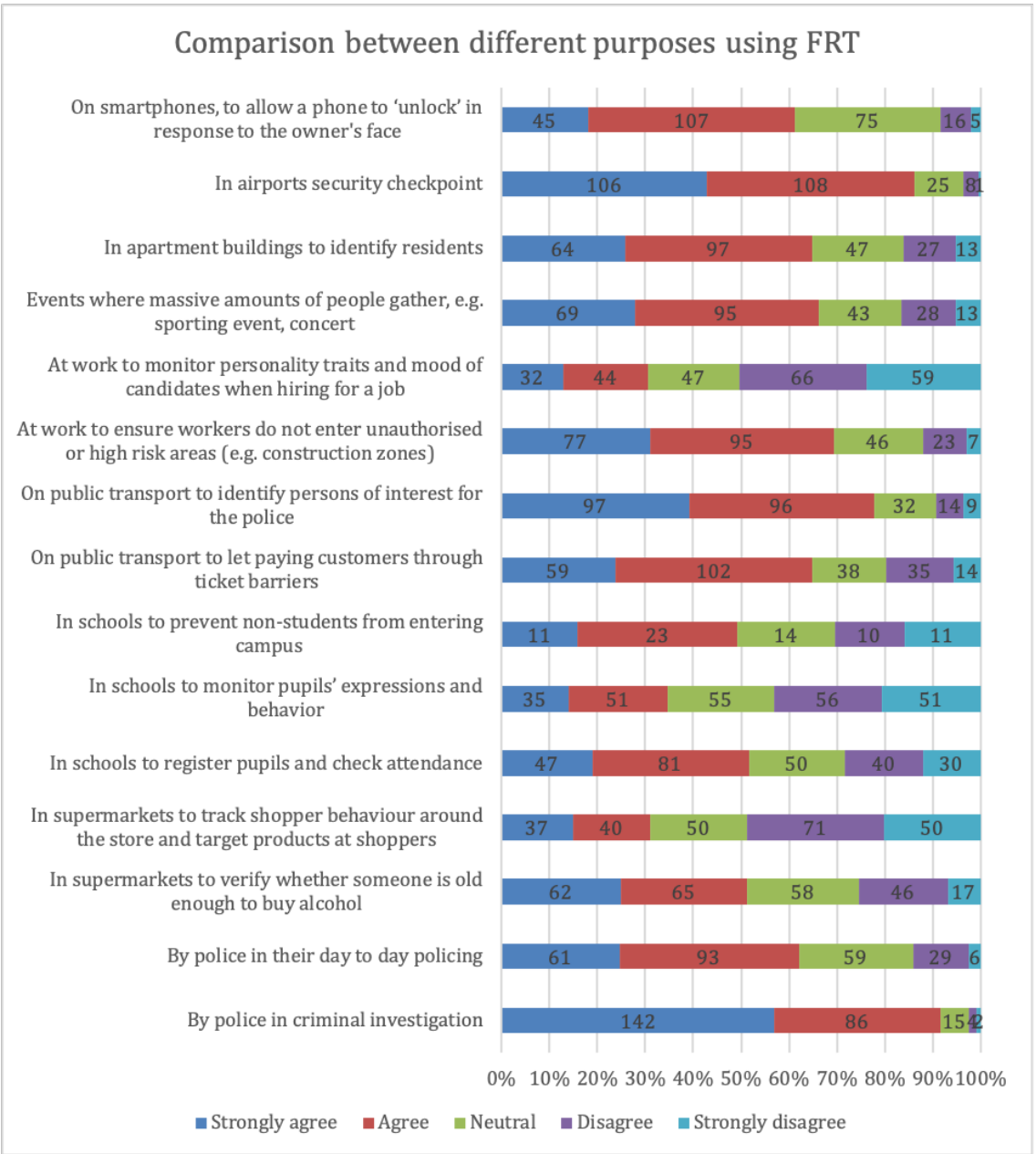


Figure 4.4: Comparison between different purposes using facial recognition technology

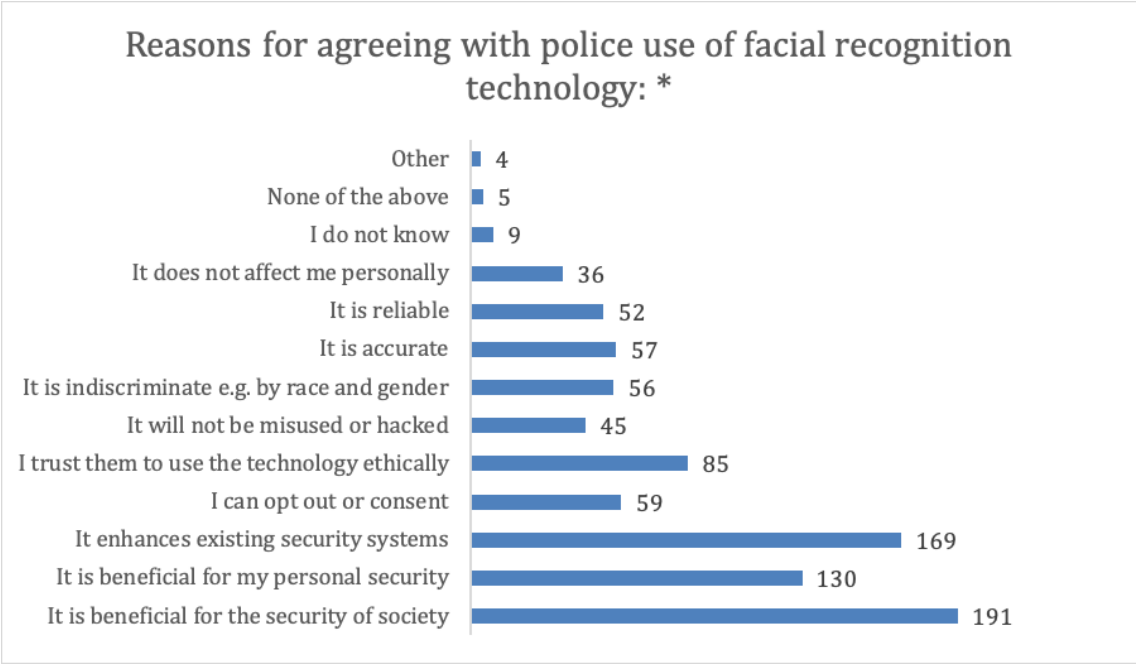


Figure 4.5: Reasons for agreeing with police use of facial recognition technology

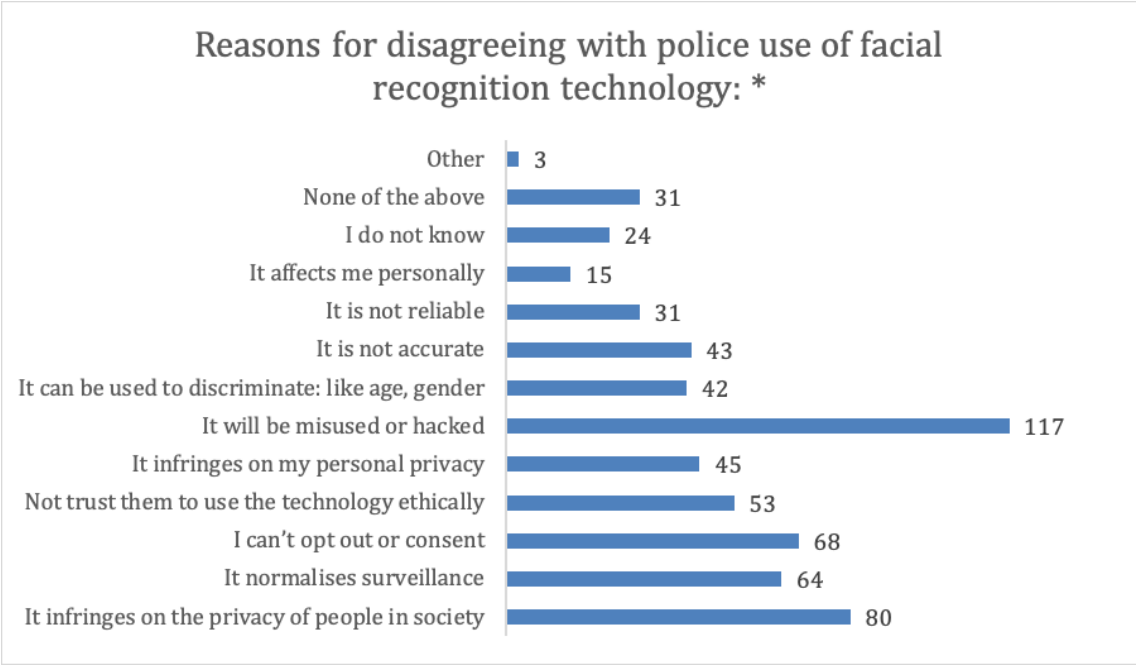


Figure 4.6: Reasons for disagreeing with police use of facial recognition technology

4.3 Analyzing Data

4.3.1 One-Sample t-test

The One Sample t Test examines whether the mean of a population is statistically different from a known or hypothesized value[60]. In our case, we assume the survey respondents hypothesized attitudes toward facial recognition technology is *Neutral*. One-sample t-test aims to check the mean value of normally distributed data against a test value which is 3 in our test. We explain two examples throughout; the others are executed in the same way. For survey question 12 *How much do you agree with the statement: "The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology"?*. We will test if the mean attitudes of our sample data is significantly different than neutral attitude which is 3 through a one-sample t-test. The null and alternative hypotheses of this test will be:

$\mathbf{H}_0$: $\mu = 3$ ("the mean attitude of the sample is equal to 3")

$\mathbf{H}_1$: $\mu \neq 3$ ("the mean attitude of the sample is not equal to 3")

For all the data on the table (see figure 4.7), reading tables from left to right[60].

Test Value = 3: The number we entered which indicates "Neutral" as the test value in the One-Sample t-Test.

t Statistic: The test statistic of the one-sample t-test, denoted t. In this example, t is calculated by dividing the mean difference by the standard error mean (from the One-Sample Statistics box).

df: The degrees of freedom for the test. For a one-sample t-test, df = N - 1; so here, df = 251 - 1 = 250.

Sig. (2-tailed): The two-tailed p-value corresponding to the test statistic.

Mean Difference: The difference between the "observed" sample mean (from the One Sample Statistics box) and the "expected" mean (the specified test value which is 3 in our sample). The sign of the mean difference corresponds to the sign of the t value. The positive t value in this example indicates that the mean level of attitudes of each question of the sample is greater than the hypothesized value which is 3 in our test.

Confidence Interval for the Difference: The confidence interval for the difference between the specified test value and the sample mean.

The one sample t-test result for question 6 *How well do you understand the "facial recognition" concept?*, t = -16,177, df = 250, Sig(2-tailed) = 0,000, Mean Difference = -0,99203, 95% Confidence Intercal of the Difference Lower = -1,1128, Upper = -0,8713.

Decision rule for assessing if the test is significant (for α =.05):

- If p $\leq$ .05, the test is significant (the sample is significant different than $\mu = 3$)
- If p $>$ .05, the test is not significant (the sample is significant different than $\mu = 3$)
- If the confidence interval includes the value of zero,particular 95% confidence interval, that means the test is not statistically significant.

These two outcomes will always agree(see figure4.7).

People who were surveyed on question 12 had a significant effect for agreeing with the public should have a opportunity to consent or opt of being subjected by facial recognition. Since p = 0.000 (which indicates highly significant) is less than 0.05, we reject the null hypothesis that the mean attitude is equal to the mean neutral attitude. Results in APA format:t(250) = -13.08, p = .000

Based on the results, we can state the following: There is a significant difference in mean attitude between the sample and the general public (p $<$ .005). The average attitude of the sample is about -0,99203 smaller than Neutral which means the respondents are more supportive to question 12.

For the other questions, we follow the same rules to test them and summarise the results overview below (see figure 4.7).

4.3.2 Independent Samples t-test

The independent t-test, is an inferential statistical test that determines whether there is a statistically significant difference between the means in two unrelated groups. In our cases, we aimed to choose two factors to do the independent samples t-test: *Gender*(male, female) and *Working field*(related to computer science and IT, unrelated to computer science and IT). The independent t-test assumes the variances of the two groups you are measuring are equal in the population[60].

The null hypothesis H_0 and alternative hypothesis H_1 of the Independent Samples t-test can be expressed[60]:

$\mathbf{H}_0$: $\mu_1 = \mu_2$ ("the paired population means are equal")

$\mathbf{H}_1$: $\mu_1 \neq \mu_2$ ("the paired population means are not equal")

We can check whether there is a statistically significant difference between the means of gender and the public's attitudes of facial recognition technology in different scenarios. The assumption of homogeneity of variance can be tested using Levene's Test of Equality of Variances. We are primarily concerned with the significance value(p-value) - if it is greater than 0.05 (i.e., p $>$ .05), our group variances can be treated as equal. However, if p

Question No.	Test Value = 3						
	t	df	Sig.(2-tailed)	Mean Difference	95% Confidence Interval of the Difference		Significant?
					Lower	Upper	
6. FR concept	-13,080	250	0,000	-0,75697	-0,8710	-0,6430	Yes
11.FR using status	-0,264	250	0,792	-0,01992	-0,1658	0,1286	No
12.Opinions of statement	-16,177	250	0,000	-0,99203	-1,1128	-0,8713	Yes
13. Attitudes of invasion	-1,247	250	0,214	-0,08765	-0,2261	0,0508	No
15. Attitudes for police using FRT	-11,811	250	0,000	-0,77689	-0,9064	-0,6473	Yes
16. Opinions for police using FR	-19,452	250	0,000	-1,02390	-1,1276	-0,9209	Yes
20. Identify criminals	-21,155	250	0,000	-1,06773	-1,1671	-0,9683	Yes
21. Prevent crimes	-11,721	250	0,000	-0,70120	-0,8190	-0,5834	Yes
22. Deter terrorists	-12,005	250	0,000	-0,74502	-0,8672	-0,6228	Yes
23. Crime evidence	-19,275	250	0,000	-1,01195	-1,1154	-0,9086	Yes
24. No notifying	-11,619	250	0,000	-0,69323	-0,8107	-0,5757	Yes
25. Attitudes now	-15,582	250	0,000	-0,76096	-0,8571	-0,6648	Yes
26. Future	-25,293	250	0,000	-1,15538	-1,2453	-1,06253	Yes

Figure 4.7: One-Sample Test significant results overview

< 0.05, we have unequal variances and we have violated the assumption of homogeneity of variances. If the Levene's Test for Equality of Variances is statistically significant, which indicates that the group variances are unequal in the population

For all the results of Independent sample t-test are shown below (see figure 4.8, figure 4.10. First, reading tables from up to down then left to right.

Levene's Test for Equality of of Variances: This section has the test results for Levene's Test.

t-test for Equality of Means:It provides the results for the actual Independent Samples t-test.

F: it is the test statistic of Levene's test.

Sig.: it is the p-value corresponding to this test statistic.

t: it is the computed test statistic.

df: it is the degrees of freedom.

Sig (2-tailed): it is the p-value corresponding to the given test statistic and degrees of freedom.

Mean Difference: it is the difference between the sample means; it also corresponds to

the numerator of the test statistic.

Std. Error Difference: it is the standard error; it also corresponds to the denominator of the test statistic.

95%Confidence Interval for the Difference: The confidence interval for the difference between the specified test value and the sample mean.

Decision Rule for Levene's test (for α =.05):

- If p $\leq$ .05, the variance are significantly different. Interpret the bottom row ("Equal variances not assumed") of results for t.
- If p $>$ .05, the variance are significantly different. Interpret the bottom row ("Equal variances assumed") of results for t.

We illustrate from one sample(see figure 4.8, the first test is "6. FR concept"*(6. How well do you understand the "facial recognition" concept?)*). The p-value of Levene's test for Equality of Variables is 0.003 which is lower than 0.05, then we look through the bottom row (Equal variances not assumed) of results for t-test, which t = -3,169, df = 239,033, sig(2-tailed) = 0,002.

Decision Rule for assessing if the test is significant (for α =.05):

- If p $\leq$ .05, the test is significant (the testing variables differ significantly for the grouping variable.)
- If p $>$ .05, the test is not significant (the testing variables not differ significantly for the grouping variable.)

Since the p-value = 0.002 which is less than 0.05, we can reject the null hypothesis, then the mean understand level of the facial recognition concept for male and female is significantly different.

Based on the results, we can state the following: There was a significant difference in the level of understand the facial recognition concept for male and female. Results in APA format: t(245)[1] = -3.169, p = 0.002. The average understand level for male is -0,35976 (somewhat level) which is higher than female.

For the other independent samples with *Gender* factor as grouping variable are illustrated in the same way. So does table of *Working field* and *Nationality* factor as grouping variable.

[1]the survey sample is 251, the test statistic (N-2) should be 249, but there are 4 respondents are not willing to reveal their gender, we only use 247 samples for the independent test

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
6.FR concept	Equal variances assumed	8,962	0,003	-3,077	245	0,002	-0,35976	0,11693	-0,59007	-0,12946
	Equal variances not assumed			-3,169	239,033	0,002	-0,35976	0,11352	-0,58339	-0,13613
11.FR using status	Equal variances assumed	0,075	0,784	-2,348	245	0,020	-0,35801	0,15250	-0,65839	-0,05763
	Equal variances not assumed			-2,329	213,434	0,021	-0,35801	0,15371	-0,66100	-0,05502
12.Opinions of statement	Equal variances assumed	1,200	0,274	1,149	245	0,252	0,14293	0,12443	-0,10215	0,38802
	Equal variances not assumed			1,130	205,834	0,260	0,14293	0,12654	-0,10655	0,39242
13.Attitudes of invasion	Equal variances assumed	2,252	0,135	1,356	245	0,176	0,19579	0,14444	-0,08870	0,48029
	Equal variances not assumed			1,313	193,010	0,191	0,19579	0,14906	-0,09821	0,48980
15.Attitudes for police using FRT	Equal variances assumed	2,116	0,147	0,428	245	0,669	0,05798	0,13547	-0,20885	0,32482
	Equal variances not assumed			0,418	199,964	0,676	0,05798	0,13871	-0,21553	0,33150
16.Opinions for police using FR	Equal variances assumed	1,867	0,173	0,761	245	0,447	0,08192	0,10762	-0,13006	0,29390
	Equal variances not assumed			0,742	198,273	0,459	0,08192	0,11041	-0,13580	0,29964
19.Feel safer	Equal variances assumed	0,823	0,365	0,263	245	0,793	0,03081	0,11712	-0,19989	0,26151
	Equal variances not assumed			0,264	223,208	0,792	0,03081	0,11662	-0,19901	0,26063
20.Identify criminals	Equal variances assumed	0,136	0,713	0,566	245	0,572	0,05839	0,10313	-0,14475	0,26153
	Equal variances not assumed			0,553	200,575	0,581	0,05839	0,10552	-0,14969	0,26646
21.Prevent crimes	Equal variances assumed	0,004	0,951	-0,219	245	0,827	-0,02677	0,12244	-0,26793	0,21440
	Equal variances not assumed			-0,218	216,676	0,828	-0,02677	0,12293	-0,26905	0,21552
22.Deter terrorists	Equal variances assumed	0,295	0,587	0,391	245	0,696	0,04962	0,12700	-0,20052	0,29977
	Equal variances not assumed			0,389	215,693	0,698	0,04962	0,12766	-0,20199	0,30124
23.Crime evidence	Equal variances assumed	4,611	0,033	-0,542	245	0,588	-0,05825	0,10738	-0,26977	0,15326
	Equal variances not assumed			-0,533	204,925	0,595	-0,05825	0,10933	-0,27380	0,15729
24.No notifying	Equal variances assumed	0,114	0,735	-3,598	245	0,000	-0,43062	0,11967	-0,66634	-0,19491
	Equal variances not assumed			-3,547	207,862	0,000	-0,43062	0,12142	-0,67000	-0,19125
25.Attitudes now	Equal variances assumed	3,754	0,054	0,301	245	0,764	0,03020	0,10041	-0,16757	0,22798
	Equal variances not assumed			0,296	205,314	0,768	0,03020	0,10218	-0,17125	0,23166
26.Future	Equal variances assumed	0,600	0,439	-2,042	245	0,042	-0,18851	0,09232	-0,37035	-0,00667
	Equal variances not assumed			-2,064	227,768	0,040	-0,18851	0,09135	-0,36851	-0,00851

Figure 4.8: Independent t-test - Gender as grouping variable

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
6.FR concept	Equal variances assumed	2,981	0,085	3,363	249	0,001	0,41996	0,12489	0,17400	0,66593
	Equal variances not assumed			3,515	148,025	0,001	0,41996	0,11947	0,18388	0,65604
11.FR using status	Equal variances assumed	2,413	0,122	-4,007	249	0,000	-0,64622	0,16128	-0,96386	-0,32858
	Equal variances not assumed			-3,793	119,746	0,000	-0,64622	0,17037	-0,98355	-0,30889
12.Opinions of statement	Equal variances assumed	0,007	0,932	0,798	249	0,426	0,10782	0,13513	-0,15833	0,37396
	Equal variances not assumed			0,803	135,796	0,423	0,10782	0,13430	-0,15778	0,37342
13.Attitudes of invasion	Equal variances assumed	3,332	0,069	-2,574	249	0,011	-0,39403	0,15307	-0,69551	-0,09255
	Equal variances not assumed			-2,416	117,795	0,017	-0,39403	0,16309	-0,71699	-0,07106
15.Attitudes for police using FRT	Equal variances assumed	3,345	0,069	-2,661	249	0,008	-0,38079	0,14311	-0,66265	-0,09893
	Equal variances not assumed			-2,511	119,004	0,013	-0,38079	0,15166	-0,68110	-0,08048
16.Opinions for police using FR	Equal variances assumed	4,406	0,037	-4,826	249	0,000	-0,53594	0,11106	-0,75467	-0,31721
	Equal variances not assumed			-4,473	115,041	0,000	-0,53594	0,11982	-0,77329	-0,29859
19.Feel safer	Equal variances assumed	0,416	0,519	-3,694	249	0,000	-0,45229	0,12243	-0,69342	-0,21115
	Equal variances not assumed			-3,709	135,155	0,000	-0,45229	0,12195	-0,69345	-0,21112
20.Identify criminals	Equal variances assumed	0,045	0,832	-2,809	249	0,005	-0,30799	0,10963	-0,52392	-0,09206
	Equal variances not assumed			-2,763	129,381	0,007	-0,30799	0,11146	-0,52850	-0,08748
21.Prevent crimes	Equal variances assumed	0,454	0,501	-3,318	249	0,001	-0,42858	0,12917	-0,68299	-0,17417
	Equal variances not assumed			-3,464	147,627	0,001	-0,42858	0,12371	-0,67305	-0,18411
22.Deter terrorists	Equal variances assumed	4,275	0,040	-5,596	249	0,000	-0,72218	0,12905	-0,97635	-0,46801
	Equal variances not assumed			-5,468	127,615	0,000	-0,72218	0,13207	-0,98350	-0,46086
23.Crime evidence	Equal variances assumed	0,819	0,366	-1,317	249	0,189	-0,15207	0,11543	-0,37942	0,07528
	Equal variances not assumed			-1,282	126,595	0,202	-0,15207	0,11859	-0,38675	0,08261
24.No notifying	Equal variances assumed	5,243	0,023	3,203	249	0,002	0,41327	0,12901	0,15918	0,66735
	Equal variances not assumed			3,283	141,489	0,001	0,41327	0,12587	0,16444	0,66209
25.Attitudes now	Equal variances assumed	2,421	0,121	-4,786	249	0,000	-0,49354	0,10311	-0,69661	-0,29046
	Equal variances not assumed			-4,785	133,906	0,000	-0,49354	0,10314	-0,69754	-0,28953
26.Future	Equal variances assumed	0,094	0,760	1,864	249	0,064	0,18655	0,10009	-0,01058	0,38368
	Equal variances not assumed			2,001	157,717	0,047	0,18655	0,09322	0,00243	0,37066

Figure 4.9: Independent t-test - Nationality as grouping variable

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
6.FR concept	Equal variances assumed	9,592	0,002	-2,723	249	0,007	-0,34270	0,12583	-0,59052	-0,09487
	Equal variances not assumed			-2,887	152,996	0,004	-0,34270	0,11869	-0,57718	-0,10822
11.FR using status	Equal variances assumed	2,696	0,102	-1,463	249	0,145	-0,24234	0,16568	-0,56866	0,08398
	Equal variances not assumed			-1,521	146,212	0,130	-0,24234	0,15934	-0,55725	0,07257
12.Opinions of statement	Equal variances assumed	0,351	0,554	-0,369	249	0,713	-0,04987	0,13527	-0,31628	0,21654
	Equal variances not assumed			-0,360	127,298	0,720	-0,04987	0,13859	-0,32411	0,22437
13.Attitudes of invasion	Equal variances assumed	0,528	0,468	0,923	249	0,357	0,14291	0,15483	-0,16203	0,44786
	Equal variances not assumed			0,912	130,643	0,363	0,14291	0,15668	-0,16704	0,45287
15.Attitudes for police using FRT	Equal variances assumed	1,643	0,201	0,761	249	0,447	0,11036	0,14496	-0,17515	0,39586
	Equal variances not assumed			0,717	118,453	0,475	0,11036	0,15400	-0,19459	0,41531
16.Opinions for police using FR	Equal variances assumed	0,000	0,998	0,623	249	0,534	0,07234	0,11604	-0,15621	0,30089
	Equal variances not assumed			0,603	125,112	0,547	0,07234	0,11991	-0,16497	0,30965
19.Feel safer	Equal variances assumed	9,661	0,002	-1,635	249	0,103	-0,20448	0,12507	-0,45081	0,04185
	Equal variances not assumed			-1,720	150,335	0,087	-0,20448	0,11885	-0,43932	0,03036
20.Identify criminals	Equal variances assumed	0,332	0,565	1,208	249	0,228	0,13414	0,11103	-0,08454	0,35282
	Equal variances not assumed			1,150	121,141	0,252	0,13414	0,11660	-0,09670	0,36497
21.Prevent crimes	Equal variances assumed	0,994	0,320	0,907	249	0,365	0,11952	0,13178	-0,14003	0,37906
	Equal variances not assumed			0,874	123,919	0,384	0,11952	0,13681	-0,15128	0,39031
22.Deter terrorists	Equal variances assumed	0,935	0,335	0,902	249	0,368	0,12336	0,13670	-0,14588	0,39261
	Equal variances not assumed			0,871	124,313	0,386	0,12336	0,14170	-0,15710	0,40383
23.Crime evidence	Equal variances assumed	0,177	0,674	0,981	249	0,327	0,11344	0,11561	-0,11427	0,34114
	Equal variances not assumed			0,933	120,924	0,352	0,11344	0,12152	-0,12715	0,35402
24.No notifying	Equal variances assumed	0,909	0,341	-1,236	249	0,218	-0,16215	0,13124	-0,42063	0,09633
	Equal variances not assumed			-1,197	125,375	0,234	-0,16215	0,13547	-0,43025	0,10595
25.Attitudes now	Equal variances assumed	13,046	0,000	0,997	249	0,320	0,10720	0,10753	-0,10459	0,31900
	Equal variances not assumed			0,890	107,536	0,376	0,10720	0,12050	-0,13166	0,34607
26.Future	Equal variances assumed	0,032	0,857	-0,894	249	0,372	-0,08996	0,10063	-0,28815	0,10822
	Equal variances not assumed			-0,933	147,513	0,352	-0,08996	0,09640	-0,28047	0,10054

Figure 4.10: Independent t-test - Working Field as grouping variable

After we finished all the independent samples test, we present the result overview in a clear way (see figure 4.11). During the test, the independent variable is divided into two categories: male and female, countries support facial recognition technology for use and countries restricted to use it, working field related to computer science or engineering and unrelated group. The check mark in the table indicates that we reject the null of Levene's test and conclude that the former group variance is significantly different than that of latter group variance. For instance, there was a significant difference in mean attitudes towards using facial recognition technology as evidence to bring criminals to justice between males and females.

Independent Samples Test Result Overview			
Test Variable / Grouping Variable	Levene's Test result significant?		
	Gender	Nationality	Working field
6.FR concept	✓		✓
11.FR using status			
12.Opinions of statement			
13.Attitudes of invasion			
15.Attitudes for police using FRT			
16.Opinions for police using FR		✓	
19.Feel safer			✓
20.Identify criminals			
21.Prevent crimes			
22.Deter terrorists		✓	
23.Crime evidence	✓		
24.No notifying		✓	
25.Attitudes now	✓		✓
26.Future			

Figure 4.11: Significant results overview of Independent Samples Test

4.3.3 Paired Samples t-test & Pearson Correlation

The Paired Samples t-test compares two means that are from the same individual, object, or related units. The purpose of the test is to determine whether there is statistical evidence that the mean difference between paired observations on a particular outcome is significantly different from zero. When we run a Paired t-test is finding out if the means of the two variables are significantly different, it's also important to consider how strongly the two variables are associated with one another, especially when the variables being compared are pre-test measures. Therefore, we present Pearson correlation and Paired samples t-test together[60].

The null hypothesis H_0 and alternative hypothesis H_1 of the Paired Samples t-test can be expressed:

$\mathbf{H}_0$: $\mu_1 = \mu_2$ ("the two groups means are equal")

$\mathbf{H}_1$: $\mu_1 \neq \mu_2$ ("the two groups means are not equal")

Reading tables from top to bottom then from left to right (see figure 4.12, also applies to figures 4.13, 4.14, figure 4.15, figure 4.16, and figure 4.17):

Paired Samples Correlations: It shows the bivariate Pearson correlation coefficient (with a two-tailed test of significance) for each pair of variables entered.

N: It shows the size of the samples.

Correlation: It gives Pearson correlation coefficient for the correlation between two variables. The direction of the relationship is positive, meaning that these variables tend to increase together,vice versa.

Sig.: It is p-value

Paired Samples Test: It gives the hypothesis test results.

First column: The series number of the two groups.

Second column: The pair of variables being tested, and the order the subtraction was carried out. (If you have specified more than one variable pair, this table will have multiple rows.)

Mean: The average difference between the two variables.

Standard deviation: The standard deviation of the difference scores.

Standard error mean: The standard error (standard deviation divided by the square root of the sample size).

95%Confidence Interval for the Difference: it is used in computing both the test statistic and the upper and lower bounds of the confidence interval.

t: The test statistic for the paired t-test.

df: The degrees of freedom for this test.
Sig. (2-tailed): The p-value corresponding to the given test statistic t with degrees of freedom df.

We started to explain one sample from figure 4.12, the other tests are all executed in the same way. Also, it is applied to figure 4.14, figure 4.15, figure 4.17. For instance, pair 5, we want to find out whether there is statistical evidence that the mean difference between age range and the attitudes of police using FRT. All the tests are from same sample, the sample size is 251. r = 0,131, p = 0,039 which is less than 0.05. Then we can state the *Age range* and the feeling of police using FRT have a statistically significant linear relationship. The direction of the relationship is positive, meaning that these variables tend to increase together, in this case means that the older survey respondents feel less comfortable for police using facial recognition. Then we see pair 5 on Paired Samples Test. The P-value is 0.000.

Decision Rule for assessing if the test is significant (for α =.05):

- If p $\leq$ .05, the test is significant (the testing variables differ significantly for the grouping variable.)
- If p $>$ .05, the test is not significant (the testing variables not differ significantly for the grouping variable.)

From the Pair 5 result, we can say that:

Age range and attitudes of police using FRT were weakly and positively correlated (r = 0.131, p = 0,039 which is less than 0.05). There was a significant average difference between *Age range* and attitudes of police using FRT (t(250) = -3,590, p $<$ 0.000 whcih is less than 0.05).

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	1.Age & 6.FR concept	251	-0,051	0,418
Pair 2	1.Age & 11.FR using status	251	0,238	0,000
Pair 3	1.Age & 12.Opinions of statement	251	-0,023	0,717
Pair 4	1.Age & 13.Attitudes of invasion	251	0,091	0,152
Pair 5	1.Age & 15.Attitudes for police using FRT	251	0,131	0,039
Pair 6	1.Age & 16.Opinions for police using FR	251	0,198	0,002
Pair 7	1.Age & 19.Feel safer	251	0,117	0,065
Pair 8	1.Age & 20.Identify criminals	251	0,143	0,023
Pair 9	1.Age & 21.Prevent crimes	251	0,042	0,507
Pair 10	1.Age & 22.Deter terrorists	251	0,219	0,000
Pair 11	1.Age & 23.Crime evidence	251	0,068	0,282
Pair 12	1.Age & 24.No notifying	251	-0,205	0,001
Pair 13	1.Age & 25.Attitudes now	251	0,152	0,016
Pair 14	1.Age & 26.Future	251	-0,106	0,092

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Lower	95% Confidence Upper			
Pair 1	1.Age - 6.FR concept	-0,38645	1,69648	0,10708	-0,59735	-0,17556	-3,609	250	0,000
Pair 2	1.Age - 11.FR using status	-1,12351	1,59646	0,10077	-1,32197	-0,92504	-11,149	250	0,000
Pair 3	1.Age - 12.Opinions of statement	-0,15139	1,70675	0,10773	-0,36357	0,06078	-1,405	250	0,161
Pair 4	1.Age - 13.Attitudes of invasion	-1,05578	1,69378	0,10691	-1,26634	-0,84522	-9,875	250	0,000
Pair 5	1.Age - 15.Attitudes for police using FRT	-0,36653	1,61775	0,10211	-0,56764	-0,16543	-3,590	250	0,000
Pair 6	1.Age - 16.Opinions for police using FR	-0,11952	1,46481	0,09246	-0,30162	0,06257	-1,293	250	0,197
Pair 7	1.Age - 19.Feel safer	0,06773	1,55929	0,09842	-0,12611	0,26157	0,688	250	0,492
Pair 8	1.Age - 20.Identify criminals	-0,07570	1,49340	0,09426	-0,26135	0,10995	-0,803	250	0,423
Pair 9	1.Age - 21.Prevent crimes	-0,44223	1,64184	0,10363	-0,64633	-0,23813	-4,267	250	0,000
Pair 10	1.Age - 22.Deter terrorists	-0,39841	1,51018	0,09532	-0,58614	-0,21067	-4,180	250	0,000
Pair 11	1.Age - 23.Crime evidence	-0,13147	1,56290	0,09865	-0,32576	0,06282	-1,333	250	0,184
Pair 12	1.Age - 24.No notifying	-0,45020	1,82661	0,11529	-0,67727	-0,22313	-3,905	250	0,000
Pair 13	1.Age - 25.Attitudes now	-0,38247	1,47687	0,09322	-0,56606	-0,19888	-4,103	250	0,000
Pair 14	1.Age - 26.Future	0,01195	1,62599	0,10263	-0,19018	0,21409	0,116	250	0,907

Figure 4.12: Paired Samples Test + Pearson Correlation - Age range

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	2.Gender & 6.FR concept	251	0,193	0,002
Pair 2	2.Gender & 11.FR using status	251	0,148	0,019
Pair 3	2.Gender & 12.Opinions of statement	251	-0,057	0,369
Pair 4	2.Gender & 13.Attitudes of invasion	251	-0,087	0,168
Pair 5	2.Gender & 15.Attitudes for police using FRT	251	-0,014	0,824
Pair 6	2.Gender & 16.Opinions for police using FR	251	-0,031	0,625
Pair 7	2.Gender & 19.Feel safer	251	-0,042	0,511
Pair 8	2.Gender & 20.Identify criminals	251	-0,016	0,796
Pair 9	2.Gender & 21.Prevent crimes	251	0,045	0,476
Pair 10	2.Gender & 22.Deter terrorists	251	0,010	0,878
Pair 11	2.Gender & 23.Crime evidence	251	0,072	0,255
Pair 12	2.Gender & 24.No notifying	251	0,230	0,000
Pair 13	2.Gender & 25.Attitudes now	251	-0,003	0,958
Pair 14	2.Gender & 26.Future	251	0,144	0,022

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Lower	95% Confidence Upper			
Pair 1	2.Gender - 6.FR	-0,63745	0,96334	0,06081	-0,75721	-0,51769	-10,483	250	0,000
Pair 2	2.Gender - 11.FR using status	-1,37450	1,23093	0,07770	-1,52752	-1,22148	-17,691	250	0,000
Pair 3	2.Gender - 12.Opinions of statement	-0,40239	1,12847	0,07123	-0,54267	-0,26211	-5,649	250	0,000
Pair 4	2.Gender - 13.Attitudes of invasion	-1,30677	1,27024	0,08018	-1,46468	-1,14886	-16,299	250	0,000
Pair 5	2.Gender - 15.Attitudes for police using FRT	-0,61753	1,17181	0,07396	-0,76320	-0,47186	-8,349	250	0,000
Pair 6	2.Gender - 16.Opinions for police using FR	-0,37052	0,99708	0,06294	-0,49447	-0,24657	-5,887	250	0,000
Pair 7	2.Gender - 19.Feel safer	-0,18327	1,06126	0,06699	-0,31520	-0,05134	-2,736	250	0,007
Pair 8	2.Gender - 20.Identify criminals	-0,32669	0,96169	0,06070	-0,44624	-0,20714	-5,382	250	0,000
Pair 9	2.Gender - 21.Prevent crimes	-0,69323	1,06090	0,06696	-0,82511	-0,56134	-10,352	250	0,000
Pair 10	2.Gender - 22.Deter terrorists	-0,64940	1,10842	0,06996	-0,78719	-0,51161	-9,282	250	0,000
Pair 11	2.Gender - 23.Crime evidence	-0,38247	0,94928	0,05992	-0,50048	-0,26446	-6,383	250	0,000
Pair 12	2.Gender - 24.No notifying	-0,70120	0,96869	0,06114	-0,82162	-0,58077	-11,468	250	0,000
Pair 13	2.Gender - 25.Attitudes now	-0,63347	0,93441	0,05898	-0,74963	-0,51731	-10,740	250	0,000
Pair 14	2.Gender - 26.Future	-0,23904	0,82863	0,05230	-0,34205	-0,13603	-4,570	250	0,000

Figure 4.13: Paired Samples Test + Pearson Correlation - Gender

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	3.Education & 6.FR concept	251	-0,139	0,028
Pair 2	3.Education & 11.FR using status	251	-0,006	0,924
Pair 3	3.Education & 12.Opinions of statement	251	-0,029	0,645
Pair 4	3.Education & 13.Attitudes of invasion	251	0,143	0,023
Pair 5	3.Education & 15.Attitudes for police using FRT	251	-0,100	0,115
Pair 6	3.Education & 16.Opinions for police using FR	251	-0,095	0,135
Pair 7	3.Education & 19.Feel safer	251	0,062	0,330
Pair 8	3.Education & 20.Identify criminals	251	-0,087	0,169
Pair 9	3.Education & 21.Prevent crimes	251	0,071	0,265
Pair 10	3.Education & 22.Deter terrorists	251	0,046	0,464
Pair 11	3.Education & 23.Crime evidence	251	-0,029	0,647
Pair 12	3.Education & 24.No notifying	251	-0,117	0,065
Pair 13	3.Education & 25.Attitudes now	251	0,024	0,706
Pair 14	3.Education & 26.Future	251	-0,176	0,005

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Lower	95% Confidence Upper			
Pair 1	3.Education - 6.FR concept	0,97610	1,48574	0,09378	0,79140	1,16079	10,408	250	0,000
Pair 2	3.Education - 11.FR using status	0,23904	1,59456	0,10065	0,04082	0,43727	2,375	250	0,018
Pair 3	3.Education - 12.Opinions of statement	1,21116	1,45025	0,09154	1,03087	1,39144	13,231	250	0,000
Pair 4	3.Education - 13.Attitudes of invasion	0,30677	1,41616	0,08939	0,13072	0,48282	3,432	250	0,001
Pair 5	3.Education - 15.Attitudes for police using FRT	0,99602	1,55048	0,09787	0,80327	1,18876	10,177	250	0,000
Pair 6	3.Education - 16.Opinions for police using FR	1,24303	1,40025	0,08838	1,06896	1,41710	14,064	250	0,000
Pair 7	3.Education - 19.Feel safer	1,43028	1,34094	0,08464	1,26358	1,59698	16,899	250	0,000
Pair 8	3.Education - 20.Identify criminals	1,28685	1,37309	0,08667	1,11616	1,45755	14,848	250	0,000
Pair 9	3.Education - 21.Prevent crimes	0,92032	1,36295	0,08603	0,75089	1,08975	10,698	250	0,000
Pair 10	3.Education - 22.Deter terrorists	0,96414	1,40382	0,08861	0,78963	1,13866	10,881	250	0,000
Pair 11	3.Education - 23.Crime evidence	1,23108	1,35735	0,08567	1,06234	1,39981	14,369	250	0,000
Pair 12	3.Education - 24.No notifying	0,91235	1,49140	0,09414	0,72695	1,09775	9,692	250	0,000
Pair 13	3.Education - 25.Attitudes now	0,98008	1,28826	0,08131	0,81993	1,14023	12,053	250	0,000
Pair 14	3.Education - 26.Future	1,37450	1,37520	0,08680	1,20355	1,54546	15,835	250	0,000

Figure 4.14: Paired Samples Test + Pearson Correlation - Education level

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	4.Nationality & 6.FR concept	251	0,036	0,573
Pair 2	4.Nationality & 11.FR using status	251	-0,056	0,379
Pair 3	4.Nationality & 12.Opinions of statement	251	0,000	0,997
Pair 4	4.Nationality & 13.Attitudes of invasion	251	-0,018	0,781
Pair 5	4.Nationality & 15.Attitudes for police using FRT	251	-0,015	0,809
Pair 6	4.Nationality & 16.Opinions for police using FR	251	-0,053	0,404
Pair 7	4.Nationality & 19.Feel safer	251	-0,027	0,665
Pair 8	4.Nationality & 20.Identify criminals	251	-0,171	0,007
Pair 9	4.Nationality & 21.Prevent crimes	251	-0,038	0,546
Pair 10	4.Nationality & 22.Deter terrorists	251	-0,054	0,396
Pair 11	4.Nationality & 23.Crime evidence	251	-0,183	0,004
Pair 12	4.Nationality & 24.No notifying	251	0,094	0,137
Pair 13	4.Nationality & 25.Attitudes now	251	-0,079	0,211
Pair 14	4.Nationality & 26.Future	251	0,050	0,429

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper			
Pair 1	4.Nationality - 6.FR concept	0,78486	1,25600	0,07928	0,62872	0,94100	9,900	250	0,000
Pair 2	4.Nationality - 11.FR using status	0,04781	1,53026	0,09659	-0,14242	0,23804	0,495	250	0,621
Pair 3	4.Nationality - 12.Opinions of statement	1,01992	1,31894	0,08325	0,85596	1,18388	12,251	250	0,000
Pair 4	4.Nationality - 13.Attitudes of invasion	0,11554	1,43896	0,09083	-0,06334	0,29442	1,272	250	0,205
Pair 5	4.Nationality - 15.Attitudes for police using FRT	0,80478	1,38193	0,08723	0,63299	0,97657	9,226	250	0,000
Pair 6	4.Nationality - 16.Opinions for police using FR	1,05179	1,25272	0,07907	0,89606	1,20752	13,302	250	0,000
Pair 7	4.Nationality - 19.Feel safer	1,23904	1,28632	0,08119	1,07914	1,39895	15,261	250	0,000
Pair 8	4.Nationality - 20.Identify criminals	1,09562	1,29569	0,08178	0,93455	1,25669	13,397	250	0,000
Pair 9	4.Nationality - 21.Prevent crimes	0,72908	1,32601	0,08370	0,56424	0,89393	8,711	250	0,000
Pair 10	4.Nationality - 22.Deter terrorists	0,77291	1,36243	0,08600	0,60354	0,94228	8,988	250	0,000
Pair 11	4.Nationality - 23.Crime evidence	1,03984	1,32605	0,08370	0,87499	1,20469	12,424	250	0,000
Pair 12	4.Nationality - 24.No notifying	0,72112	1,23690	0,07807	0,56735	0,87488	9,237	250	0,000
Pair 13	4.Nationality - 25.Attitudes now	0,78884	1,22606	0,07739	0,63643	0,94126	10,193	250	0,000
Pair 14	4.Nationality - 26.Future	1,18327	1,11995	0,07069	1,04404	1,32249	16,739	250	0,000

Figure 4.15: Paired Samples Test + Pearson Correlation - Nationality

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	5.Work & 6.FR concept	251	0,170	0,007
Pair 2	5.Work & 11.FR using status	251	0,092	0,145
Pair 3	5.Work & 12.Opinions of	251	0,023	0,713
Pair 4	5.Work & 13.Attitudes of	251	-0,058	0,357
Pair 5	5.Work & 15.Attitudes for	251	-0,048	0,447
Pair 6	5.Work & 16.Opinions for	251	-0,039	0,534
Pair 7	5.Work & 19.Feel safer	251	0,103	0,103
Pair 8	5.Work & 20.Identify	251	-0,076	0,228
Pair 9	5.Work & 21.Prevent crimes	251	-0,057	0,365
Pair 10	5.Work & 22.Deter terrorists	251	-0,057	0,368
Pair 11	5.Work & 23.Crime evidence	251	-0,062	0,327
Pair 12	5.Work & 24.No notifying	251	0,078	0,218
Pair 13	5.Work & 25.Attitudes now	251	-0,063	0,320
Pair 14	5.Work & 26.Future	251	0,057	0,372

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Lower	95% Confidence Upper			
Pair 1	5.Work - 6.FR concept	-0,53386	0,95176	0,06007	-0,65218	-0,41555	-8,887	250	0,000
Pair 2	5.Work - 11.FR using status	-1,27092	1,23867	0,07818	-1,42490	-1,11693	-16,255	250	0,000
Pair 3	5.Work - 12.Opinions of statement	-0,29880	1,06318	0,06711	-0,43097	-0,16664	-4,453	250	0,000
Pair 4	5.Work - 13.Attitudes of invasion	-1,20319	1,22742	0,07747	-1,35577	-1,05060	-15,530	250	0,000
Pair 5	5.Work - 15.Attitudes for police using FRT	-0,51394	1,15707	0,07303	-0,65778	-0,37010	-7,037	250	0,000
Pair 6	5.Work - 16.Opinions for police using FR	-0,26693	0,96564	0,06095	-0,38697	-0,14689	-4,379	250	0,000
Pair 7	5.Work - 19.Feel safer	-0,07968	0,96831	0,06112	-0,20006	0,04069	-1,304	250	0,194
Pair 8	5.Work - 20.Identify criminals	-0,22311	0,94975	0,05995	-0,34117	-0,10504	-3,722	250	0,000
Pair 9	5.Work - 21.Prevent crimes	-0,58964	1,07468	0,06783	-0,72324	-0,45604	-8,693	250	0,000
Pair 10	5.Work - 22.Deter terrorists	-0,54582	1,10675	0,06986	-0,68340	-0,40823	-7,813	250	0,000
Pair 11	5.Work - 23.Crime evidence	-0,27888	0,97258	0,06139	-0,39979	-0,15798	-4,543	250	0,000
Pair 12	5.Work - 24.No notifying	-0,59761	1,01658	0,06417	-0,72398	-0,47123	-9,314	250	0,000
Pair 13	5.Work - 25.Attitudes now	-0,52988	0,92201	0,05820	-0,64450	-0,41526	-9,105	250	0,000
Pair 14	5.Work - 26.Future	-0,13546	0,83281	0,05257	-0,23899	-0,03193	-2,577	250	0,011

Figure 4.16: Paired Samples Test + Pearson Correlation - Working field

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	6.FR concept & 11.FR using status	251	0,348	0,000
Pair 2	6.FR concept & 12.Opinions of statement	251	0,065	0,304
Pair 3	6.FR concept & 13.Attitudes of invasion	251	0,021	0,741
Pair 4	6.FR concept & 15.Attitudes for police using FRT	251	-0,049	0,443
Pair 5	6.FR concept & 16.Opinions for police using FR	251	-0,060	0,341
Pair 6	6.FR concept & 19.Feel safer	251	0,014	0,826
Pair 7	6.FR concept & 20.Identify criminals	251	-0,070	0,268
Pair 8	6.FR concept & 21.Prevent crimes	251	-0,010	0,872
Pair 9	6.FR concept & 22.Deter terrorists	251	-0,056	0,380
Pair 10	6.FR concept & 23.Crime evidence	251	-0,054	0,395
Pair 11	6.FR concept & 24.No notifying	251	0,144	0,022
Pair 12	6.FR concept & 25.Attitudes now	251	-0,082	0,194
Pair 13	6.FR concept & 26.Future	251	0,069	0,275

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Lower	95% Confidence Upper			
Pair 1	6.FR concept - 11.FR using status	-0,73705	1,22743	0,07747	-0,88964	-0,58447	-9,513	250	0,000
Pair 2	6.FR concept - 12.Opinions of statement	0,23506	1,29171	0,08153	0,07448	0,39564	2,883	250	0,004
Pair 3	6.FR concept - 13.Attitudes of invasion	-0,66932	1,42766	0,09011	-0,84680	-0,49185	-7,428	250	0,000
Pair 4	6.FR concept - 15.Attitudes for police using FRT	0,01992	1,42113	0,08970	-0,15675	0,19659	0,222	250	0,824
Pair 5	6.FR concept - 16.Opinions for police using FR	0,26693	1,27611	0,08055	0,10829	0,42557	3,314	250	0,001
Pair 6	6.FR concept - 19.Feel safer	0,45418	1,27785	0,08066	0,29533	0,61304	5,631	250	0,000
Pair 7	6.FR concept - 20.Identify criminals	0,31076	1,25819	0,07942	0,15435	0,46717	3,913	250	0,000
Pair 8	6.FR concept - 21.Prevent crimes	-0,05578	1,32547	0,08366	-0,22055	0,10900	-0,667	250	0,506
Pair 9	6.FR concept - 22.Deter terrorists	-0,01195	1,38125	0,08718	-0,18366	0,15976	-0,137	250	0,891
Pair 10	6.FR concept - 23.Crime evidence	0,25498	1,27072	0,08021	0,09701	0,41295	3,179	250	0,002
Pair 11	6.FR concept - 24.No notifying	-0,06375	1,21816	0,07689	-0,21518	0,08769	-0,829	250	0,408
Pair 12	6.FR concept - 25.Attitudes now	0,00398	1,24739	0,07873	-0,15108	0,15905	0,051	250	0,960
Pair 13	6.FR concept - 26.Future	0,39841	1,12811	0,07121	0,25817	0,53865	5,595	250	0,000

Figure 4.17: Paired Samples Test + Pearson Correlation - The understanding level of FRT concept

On one sample t-test, we figure out whether the mean attitudes of facial recognition is significant than the *Neutral* (neither agree or disagree). All the results are present on figure 4.7. There are too many results during paired-samples t-test and Pearson Correlation test, therefore we only present the results with significant differences (see figure 4.18). The first column presents the abbreviation of the survey questions. The first row gives the factors could affect the attitudes of facial recognition technology applied in different situation. The second row we shows the test what we have done, we only present the significant correlation, "+" means positive correlation, "-" means negative correlation. For the paired samples t-test result, we use red mark expresses significant effects. Those results can answer the research question, how each factors: *Age range, Gender, Education level, Nationality , Working field and the understanding level of facial recognition* affect the attitudes of facial recognition technology applied in different scenarios.

Pearson Correlation + Paired Samples Test												
#	Age range		Gender		Education level		Nationality		Working field		The understanding level of FR concept	
	Significant correlation (+/-)	t-test	Significant correlation (+/-)	t-test	Significant correlation (+/-)	t-test	Significant correlation (+/-)	t-test	Significant correlation (+/-)	t-test	Significant correlation (+/-)	t-test
6. FR concept		✓	+	✓	-	✓		✓	+	✓		
11.FR using status	+	✓	+	✓		✓				✓	+	✓
12.Opinions of statement				✓		✓		✓		✓		✓
13. Attitudes of invasion		✓		✓	+	✓				✓		✓
15. Attitudes for police using FRT	+	✓		✓		✓		✓		✓		
16.opinions for police using FR	+			✓		✓		✓		✓		✓
19. Feel safer				✓		✓		✓				✓
20. Identify criminals	+			✓		✓	-	✓		✓		✓
21.Prevent crimes		✓		✓		✓		✓		✓		
22.Deter terrorists	+	✓		✓		✓		✓		✓		
23.Crime evidence				✓		✓	-	✓		✓		✓
24.No notifying	-	✓	+	✓		✓		✓		✓	+	
25.Atitudes now	+	✓		✓		✓		✓		✓		
26. Future			+	✓	-	✓		✓		✓		✓

Figure 4.18: The overall significant results of Pearson Correlation and Paired Sample t-test

4.4 Analysis of Variance

One-Way ANOVA (analysis of variance) compares the means of two or more independent groups in order to determine whether there is statistical evidence that the associated population means are significantly different[60]. Post Hoc Tests (also known as multiple comparisons) tests, they are typically conducted after a significant ANOVA. Post Hoc Tests are used to dive in and look for differences between groups, it tests each possible pair of each group [60]. The total alpha level we used α =0.05 in our test. We will elaborate one sample first. For survey question 16, we wanted to figure out whether the different age range has an impact on attitudes of police using facial recognition technology to better serve the public. And which age range group means were significant different from one another. The other tests were all executed in the same method.

The null hypothesis H_0 and alternative hypothesis H_1 of the Paired Samples t-test can be expressed[60]:

$\mathbf{H}_0$: $\mu_1 = \mu_2 = \mu_3 ... = \mu_k$ ("all k population means are equal")

$\mathbf{H}_1$: At least one μ_i different ("at least one of the k population means is not equal to the others")

where

μ_i is the population mean of the ith group (i = 1, 2, ..., k)

The ANOVA result is presented in figure 4.19. First, reading tables from up to down then left to right:

IV: Independent variables of the test.

DV: Dependent variables of the test.

df: It is the degrees of freedom.

F: The F statistic evaluates whether the group means are significantly different.

Sig.: It is the p-value corresponding to this test statistic.

Mean Difference: it is the difference between the sample means; it also corresponds to the numerator of the test statistic.

Std. Error Difference: it is the standard error; it also corresponds to the denominator of the test statistic.

95%Confidence Interval for the Difference: The confidence interval for the difference between the specified test value and the sample mean.

ANOVA

IV: Age range; DV: 16.Opinions for police using FR

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	10,984	5	2,197	3,305	0,007
Within Groups	162,872	245	0,665		
Total	173,857	250			

Post Hoc Tests

Multiple Comparisons

IV: Age range; DV: 16.Opinions for police using FR

(I) 1.Age		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Lower Bound	95% Confidence Upper Bound
18 - 30	31 - 40	-0,22078	0,13938	0,610	-0,6211	0,1796
	41 - 50	-0,12987	0,20310	0,988	-0,7133	0,4535
	51 - 60	-0,19654	0,22054	0,948	-0,8300	0,4369
	61 - 70	-0,12987	0,26607	0,997	-0,8941	0,6344
	Over 70	-1.02987*	0,26607	0,002	-1,7941	-0,2656
31 - 40	18 - 30	0,22078	0,13938	0,610	-0,1796	0,6211
	41 - 50	0,09091	0,22813	0,999	-0,5644	0,7462
	51 - 60	0,02424	0,24378	1,000	-0,6760	0,7245
	61 - 70	0,09091	0,28563	1,000	-0,7296	0,9114
	Over 70	-0,80909	0,28563	0,056	-1,6296	0,0114
41 - 50	18 - 30	0,12987	0,20310	0,988	-0,4535	0,7133
	31 - 40	-0,09091	0,22813	0,999	-0,7462	0,5644
	51 - 60	-0,06667	0,28505	1,000	-0,8854	0,7521
	61 - 70	0,00000	0,32158	1,000	-0,9237	0,9237
	Over 70	-0,90000	0,32158	0,061	-1,8237	0,0237
51 - 60	18 - 30	0,19654	0,22054	0,948	-0,4369	0,8300
	31 - 40	-0,02424	0,24378	1,000	-0,7245	0,6760
	41 - 50	0,06667	0,28505	1,000	-0,7521	0,8854
	61 - 70	0,06667	0,33286	1,000	-0,8895	1,0228
	Over 70	-0,83333	0,33286	0,127	-1,7895	0,1228
61 - 70	18 - 30	0,12987	0,26607	0,997	-0,6344	0,8941
	31 - 40	-0,09091	0,28563	1,000	-0,9114	0,7296
	41 - 50	0,00000	0,32158	1,000	-0,9237	0,9237
	51 - 60	-0,06667	0,33286	1,000	-1,0228	0,8895
	Over 70	-0,90000	0,36463	0,138	-1,9474	0,1474
Over 70	18 - 30	1.02987*	0,26607	0,002	0,2656	1,7941
	31 - 40	0,80909	0,28563	0,056	-0,0114	1,6296
	41 - 50	0,90000	0,32158	0,061	-0,0237	1,8237
	51 - 60	0,83333	0,33286	0,127	-0,1228	1,7895
	61 - 70	0,90000	0,36463	0,138	-0,1474	1,9474

*. The mean difference is significant at the 0.05 level.

Figure 4.19: ANOVA Test + Post Hoc Test - Age range as independent variable

Decision Rule for assessing if the test is significant (for α =.05):

- If p $\leq$ .05, the test is significant (the test scores differ significantly somewhere between the groups.)
- If p $>$ .05, the test is not significant (the test scores do not differ significantly somewhere between the groups.)

The mean attitudes of police using facial recognition technology to better serve the public is significantly different for at least one of the age range groups, F(5,245) = 3,305, p = 0.007 which is lower than 0.05. Note that the ANOVA alone does not tell us specifically which means were different from one another. To determine that, we follow up with multiple multiple comparisons (or Post Hoc) tests [60]. Each individual groups will be compared with each other(see figure 4.19. We picked up first pair of each groups and conducted their results (see table 4.1). The other individual groups are explained in the same way. We use the same way decision rules, we concluded that there a significant difference between age range group 18 - 30 and group Over 70.

Multiple comparisons table		
Test groups	p-value (sig.)	Significant?
18 - 30 vs. 31 - 40	0.610	No
18 - 30 vs. 41 - 50	0.988	No
18 - 30 vs. 51 - 60	0.948	No
18 - 30 vs. 61 - 70	0.997	No
18 - 30 vs. Over 70	0.002	Yes

Table 4.1: Partial Significant result of Post Hoc test on age range groups

In last section we explained how we did ANOVA and Post Hoc Test. However, there are a lot of data to organize, to be easier check the results, we only summarise the result with significant difference and which mean groups were different from one another. The full data is posted on Google Drive[1]. The overall result of ANOVA and Post Hoc Test is present on figure4.20. The first column and row present the dependent variables(DV) and independent variables(IV). The black check mark means the test is significant which the test scores differ significantly somewhere between the groups. Later, we displayed which individual mean group were significant differ from another group.

[1] `https://docs.google.com/spreadsheets/d/1LXXJ_Xq9ZLkNy1Cj7Wr2pqrHeVdDTZi1JInmpf2ClNA/edit?usp=sharing`

DV \ IV	ANOVA + Post Hoc Test									
	Age range	Individual age range groups	Gender	Education level	Individual education group	Nationality	Individual nationality group	Working field	FR Concept	Individual understanding level group
6. FR concept	✓	41-50 vs. 51-60	✓			✓	China vs. NL	✓		
11.FR using status	✓					✓	USA vs. China;		✓	Very well vs. Somewhat; Very well vs. Neutral; Very well vs. Know about but don't understand; Very well vs. Never heard about it
12.Opinions of statement										
13. Attitudes of invasion	✓	18-30 vs. Over 70; 31-40 vs. Over 70; 41-50 vs. Over 70;								
15. Attitudes for police using FRT	✓	18-30 vs. Over 70; 41-50 vs. Over 70; 61-70 vs. Over 70;								
16.opinions for police using FR	✓	18-30 vs. Over 70;				✓	USA vs. China; UK vs. China;			
19. Feel safer	✓	41-50 vs. 51-60;				✓	USA vs. China;			
20. Identify criminals						✓	USA vs. China;			
21.Prevent crimes						✓				
22.Deter terrorists	✓	18-30 vs. 61-70; 31-40 vs. 61-70; 41-50 vs. 61-70				✓	USA vs. China; China vs. China			
23.Crime evidence						✓	UK vs. China; UK vs. NL; UK vs. Other;		✓	Somewhat vs. Neutral; Neutral vs. Know about but don't understand;
24.No notifying	✓	18-30 vs. Over 70;	✓			✓	USA vs. China;			
25.Atitudes now	✓	41-50 vs. Over 70;				✓	USA vs. China; China vs. NL;			
26. Future				✓	Primary education vs. Other					

Figure 4.20: The overall result of ANOVA and Post Hoc Test

4.5 Results Overview

The key results of this thesis can be concluded as follows:

- 74.6% respondents chose the option of understanding the facial recognition concept on *Very well* or *Somewhat* level which indicates the facial recognition technology is no longer unacquainted for the public.

- 30,68% respondents choose *Faster* (8 options) as the primary reason willing to use facial recognition comparing with other options, which indicates this technology do bring convenience to the public.

- 27.09% respondents choose *Less secure* (8 options) as the biggest concern not willing to use facial recognition comparing with other primary reasons, which indicates that the public care about the security issues while applying this technology in daily life.

- 228 respondents (90.84%) and 214 respondents (85.26%) choose *Strong Agree* and *Agree* attitude as using facial recognition technology on *By police in criminal investigation* and *In airports security checkpoint* scenarios, respectively. Which it indicates that the public supports applying this technology when it related to public society safety. 191 respondents choose *It is beneficial for the security of society* as the agreeing reason with police using of facial recognition can prove that point too.

- 125 respondents (49.80%) and 121 respondents (48.20%) choose *Strongly Disagree* and *Disagree* attitudes as using facial recognition technology on *In supermarkets to track shopper behaviour around the store and target products at shoppers* and *At work to monitor personality traits and mood of candidates when hiring for a job* scenarios. Which it indicates that the public shows concerns about the privacy invasion. The biggest reason disagreeing with police using facial recognition technology (117 respondents) is *It will be misused or hacked* can prove this point too.

- Survey question *6. How well do you understand the "facial recognition" concept?*
  1) *Very well* : 41, *Somewhat* : 146, *Know about but don't understand* : 32, *Never heard about it* : 3.
  2)The sample mean understanding level of "facial recognition" concept is significant different from a hypothesized population mean *Neutral*.
  3)There was a significant difference in mean understanding level of FRT concept between males and females. There was a significant difference in mean understanding

level of FRT concept between working field related to computer science or engineering and unrelated ones.

4)Each individual factor of *Age range, Gender, Education level, Nationality and Working field* have a significant average difference with the understanding level of FRT concept.

5)More specifically, the *Age range* group 41-50 and group 51-60 were different from one another. *Nationality* group China and Netherlands were different from one another.

- Survey question *11. How knowledgeable are you about the usage of facial recognition technology by your country's government?*

  1) *Very knowledgeable* : 17, *Somewhat knowledgeable* : 99, *Neutral* : 38, *Slightly knowledgeable* : 66, *Not knowledgeable at all* : 31.

  2)The sample mean knowing level about the usage of FRT by your country's government is Not significant different from a hypothesized population mean *Neutral*.

  3)Each individual factor of *Age range, Gender, Education level, Working field and the understanding level of FRT concept* have a significant average difference with the knowing level about the usage of FRT by your country's government.

  4)More specifically, the *Nationality* group USA and group China were different from one another. *The understanding level of FRT concept* group Very well and group Somewhat, Group Very well and group Neutral, group Very well and group Know about but don't understand, group Very well and group Never heard about it were different from one another.

- Survey question *12. How much do you agree with the statement: "The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology"?*

  1)*Strongly agree* : 94, *Agree* : 81, *Neutral* : 59, *Disagree* : 14, *Strongly disagree* : 3.

  2)The sample mean attitude of the statement is significant different from a hypothesized population mean *Neutral*.

  3)Each individual factor of *Gender, Education level, Nationality, Working field and the understanding level of FRT concept* have a significant average difference with attitude of the statement.

- Survey question *13. On a scale of 1 to 5, where 1 is not at all and 5 is very strongly, how strongly do you feel that use of facial recognition on surveillance cameras is an*

invasion of your privacy?

1)*1 (not at all)* : 35, *2* : 39, *3* : 113, *4* : 41, *5 (very strongly)* : 23.

2)The sample mean feeling of FRT is an invasion of your privacy is Not significant different from a hypothesized population mean *Neutral*.

3)Each individual factor of *Age range, Gender, Education level, Working field and the understanding level of FRT concept* have a significant average difference with feeling of FRT is an invasion of your privacy.

4) More specifically, the *Age range* group 18-30 and group Over 70, group 31-40 and Over 70, group 41-50 and Over 70 were different from one another.

- Survey question *15. On a scale of 1 to 5, where 1 is very comfortable and 5 is not at all comfortable, how comfortable are you with the police using facial recognition technology?*

  1)*1 (very comfortable)* : 75, *2* : 76, *3* : 77, *4* : 15, *5 (not at all comfortable)* : 8.

  2)The sample mean feeling of police using FRT is significant different from a hypothesized population mean *Neutral*.

  3)Each individual factor of *Age range, Gender, Education level, Nationality and Working field* have a significant average difference with feeling of police using FRT.

  4)More specifically, the *Age range* group 18-30 and group Over 70, group 41-50 and Over 70, group 61-70 and Over 70 were different from one another.

- Survey question *16. Do you agree that police should use facial recognition technology to better serve the public?*

  1)*Strongly agree* : 75, *Agree* : 119, *Neutral* : 48, *Disagree* : 6, *Strongly disagree* : 3.

  2)The sample mean attitude of police using FRT serve the public is significant different from a hypothesized population mean *Neutral*.

  3)There was a significant difference in mean attitude of police using FRT serve the public between countries support facial recognition technology for use and countries restricted it to use.

  4)Each individual factor of *Gender, Education level, Nationality, Working field and the understanding level of FRT concept* have a significant average difference with attitude of police using FRT serve the public.

  5)More specifically, the *Age range* group 18-30 and group Over 70 were different from one another. The *Nationality* group USA and group China, group UK and group China were different from one another.

- Survey question *20. Do you agree that the use of facial recognition technology can help identify criminals more efficiently in your city?*

  1)*Strongly agree* : 76, *Agree* : 127, *Neutral* : 39, *Disagree* : 7, *Strongly disagree* : 2.

  2)The sample mean attitude of using FRT to identify criminals is significant different from a hypothesized population mean *Neutral*.

  3)Each individual factor of *Gender, Education level, Nationality, Working field and the understanding level of FRT concept* have a significant average difference with attitude of using FRT to identify criminals.

  4)More specifically, the *Nationality* group USA and group China were different from one another.

- Survey question *21. Do you agree that the facial recognition technology can help prevent crimes from occurring in your city?*

  1)*Strongly agree* : 57, *Agree* : 90, *Neutral* : 77, *Disagree* : 26, *Strongly disagree* : 1.

  2)The sample mean attitude of using FRT prevent crimes is significant different from a hypothesized population mean *Neutral*.

  3)Each individual factor of *Age range, Gender, Education level, Nationality and Working field* have a significant average difference with attitude of using FRT prevent crimes.

- Survey question *22. Do you agree that the use of facial recognition technology will deter terrorists in your city?*

  1)*Strongly agree* : 56, *Agree* : 112, *Neutral* : 50, *Disagree* : 29, *Strongly disagree* : 4.

  2)The sample mean attitude of using FRT deter terrorists is significant different from a hypothesized population mean *Neutral*.

  3)There was a significant difference in mean attitudes towards using facial recognition technology to deter terrorists in your city between countries support facial recognition technology for use and countries restricted it to use.

  4)Each individual factor of *Age range, Gender, Education level, Nationality and Working field* have a significant average difference with attitude of using FRT deter terrorists.

  5)More specifically, the *Age range* group 18-30 and group 61-70, group 31-40 and 61-70, group 41-50 and 61-70 were different from one another. The *Nationality* group USA and group China, group China and group Other were different from one another.

- Survey question *23. Do you agree with using facial recognition technology as evidence to bring criminals to justice?*
  1)*Strongly agree* : 74, *Agree* : 118, *Neutral* : 49, *Disagree* : 8, *Strongly disagree* : 2.
  2)The sample mean attitude of using FRT bring criminals to justice is significant different from a hypothesized population mean *Neutral*.
  3)There was a significant difference in mean attitudes towards using facial recognition technology as evidence to bring criminals to justice between male and female.
  4)Each individual factor of *Gender, Education level, Nationality, Working field and the understanding level of FRT concept* have a significant average difference with attitude of using FRT bring criminals to justice.
  5)More specifically, the *Nationality* group UK and group China, group UK and Group Netherlands, group UK and group Other were different from one another. *The understanding level of FRT concept* group Somewhat and group Neutral, Group Neutral and group Know about but don't understand were different from one another.

- Survey question *24. Do you believe that the government will use facial recognition technology without notifying the public?*
  1)*Strongly agree* : 54, *Agree* : 92, *Neutral* : 84, *Disagree* : 16, *Strongly disagree* : 5.
  2)The sample mean attitude of the government using FRT without notifying the public is significant different from a hypothesized population mean *Neutral*.
  3)There was a significant difference in mean attitudes towards believing that the government will use facial recognition technology without notifying the public between countries support facial recognition technology for use and countries restricted it to use.
  4)Each individual factor of *Age range, Gender, Education level, Nationality and Working field* have a significant average difference with attitude of the government using FRT without notifying the public.
  5)More specifically, the *Age range* group 18-30 and group Over 70 were different from one another. The *Nationality* group USA and group China were different from one another.

5

Discussion

In this section, we discuss different opinions of facial recognition technology based on our result.

5.1 Comparison with Relevant Article

In our work, there are some results are in common and some are different comparing with the British Ada Lovelace Institute survey report *Beyond face value: public attitudes to facial recognition technology*[8]. The awareness of facial recognition technology is high, the public understands concept better now. The public can evaluate this technology more objective. The data from both research agree that the public should given the opportunity to consent or op out of being subjected to facial recognition technology. But in our research, the public also show another concern that they believe the government will use facial recognition technology without notifying the public. In Ada Lovelance Institute survey, people fear the normalisation of surveillance, however, in our research, the public opinion changed because over 45 percent people feel neutral about using facial recognition on surveillance cameras is an invasion of privacy, the other left in agreeing and disagreeing this statement are almost same. On police to deploy facial recognition technology, both results present that the public agree it but with limitations, our research shows that the public concerns misused and security issues more than the accuracy of this technology. As for other purposes using facial recognition, when it concerns benefit to the society, like criminal investigation and airport security checkpoint are more acceptable. When it applies to work places, supermarkets or schools, the supportive number drops quickly. Both research proves that the public does not trust the private sector to use faecal recognition technology ethically. The Ada Lovelance Institute thinks that the public expects the

government to be placing limits on the use of facial recognition technology, surprising found in our research is that the public believes that facial recognition technology will be more widely used in the future (see figure 5.1).

In our research, We also find that as for agreeing with police deploying facial recognition technology, the public attitudes are different based on different purpose. The public is more supportive on using facial recognition technology to help identify criminals and to bring criminals to justice. The support rate drops whether the public agree with using facial recognition technology will deter terrorists. The support rate drops more whether the public agree facial recognition technology can help prevent crimes from occurring. There are still more concerns on details for the public as police deploying facial recognition technology.

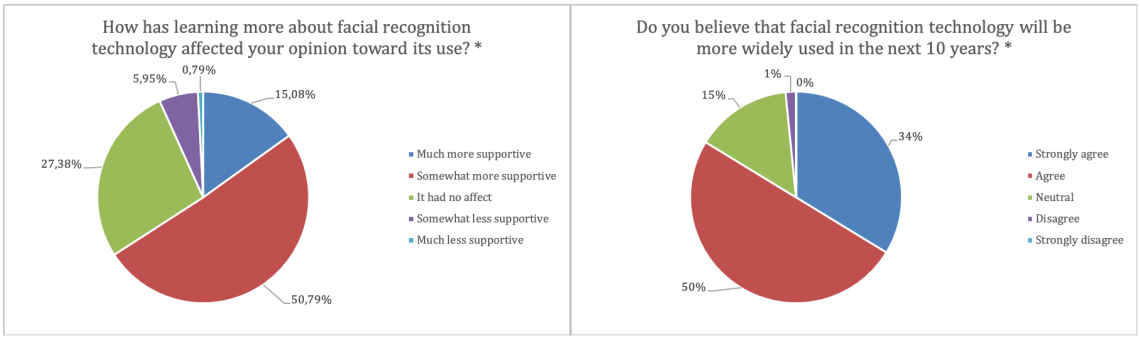


Figure 5.1: The possibility of facial recognition technology in the future

5.2 Follow-up Questions Interview

The survey comments can be conducted as follow: 1)Support for facial recognition technology; 2)Concerns about privacy violations and appropriate regulations; 3)Disagreement on how facial recognition technology is applied; 4)No comments. Combined with the survey results and all survey comments(see Appendix-2) from all the survey respondents, we did interviews (see Appendix-3) with follow-up questions chose from the survey respondents. At first, we planned to do focus group interview, since COVID-19 happened, it was difficult to let people sit down to talk about their feelings toward facial recognition technology. Therefore we did follow-up questions to talk with the survey respondents one-to-one who are volunteered to share their further opinions. We received four respondents from different background: age range, gender, education level, country, working field. Their replays could always classify into two groups to do cross-contrast, for example, each interviewee from different age range, you can compare their current attitudes on facial recognition.

- What do you think the BEST thing about facial recognition technology?
- What do you think the WORST thing about facial recognition technology?
- Does your behavior change when you realize that you are in surveillance with facial recognition technology? Why or why not?
- Have you had any real-life experiences or heard any real stories about the use of facial recognition technology?
- Have your attitudes changed about facial recognition technology due to COVID-19 pandemic? Why or why not?

The responses from the interviewees reflect back to the general result of the survey. The best thing about facial recognition technology is helping police improve public security and make personal life more convenient. The worst thing is still about privacy violation. All the survey respondents already had real-life experiences about using facial recognition technology. And they do not think there is behavior change when you are in surveillance with facial recognition technology. All the survey respondents' attitudes have changed due to COVID-19 pandemic. In the future, we should do more research on how people's attitudes changed on Facial Recognition Technology before and after COVID-19.

5.3 Drawbacks of Research

There are some drawbacks in our research need to address in the future. First, since facial recognition technology is controversial and it is prohibited in Europe, the number of questionnaire response is less than China. The European survey response about experience of facial recognition technology mostly from mobile phone, like FaceID to unlock phone. We provide a surveillance camera with facial recognition, but only very rare survey respondents are willing to sign the permission paper and try it for real. In the future, if the policy changes in Europe, we could collect data from the public who has experience of facial recognition technology on surveillance camera, then comparing with our current work.

6

Conclusion

Facial recognition technology can provide convenient and fast service on different occasions, for instance, it can provide assistance measures for improving security by police and airport checkpoints. However, it also bring certainty risks on the public's privacy. Face-print is unique ID like fingerprint, but it is much easier to be stolen or misused because each individual may post photos or videos with clear face feature of themselves or others on social media on purpose or unintentionally. Without mature techniques and impeachable regulation system, misused facial recognition technology could cause dramatic damage to individuals and the public.

This project aims to assess the public's knowledge and attitudes concerning about Facial recognition technologies. Our goal is to address the changes of attitudes toward using facial recognition technology as a security measure and what factors caused it. To address research questions, we started with a literature review to figure out the most important public's concerns about facial recognition technology. By introducing the architecture of facial recognition system and different algorithms, we aim to provide a general idea how the system works. Later we designed a questionnaire gathering the survey respondents from different background: age range, gender, education level, nationality, working fields and the understanding level of facial recognition concept. We classify the public's attitudes towards different scenarios applying facial recognition technology into five levels: strongly agree, agree, neutral, disagree and strong disagree.

We collect 251 valid responses from all the different background. Through the data analysis, up to 74.6% survey respondents *Somewhat* understand the facial recognition concept which indicates that facial recognition technology is not unfamiliar to the public anymore. By listing all the popular reasons why you are willing or not willing to use facial recognition technology: *Faster*(30.56%) and *Less secure*(29.73%) are chosen. By comparing the

different purposes support or nonsupport to use facial recognition technology, *By police in criminal investigation* and *In school to monitor pupil's expressions and behavior* show the strongest attitudes. By comparing the reasons for agreeing and disagreeing with police using facial recognition technology: *It is beneficial for the security of society* and *It will be misused or hacked* are the most prominent options. Through these three comparisons, the public concerns the security issues is the most important no matter when it is related to personal security or the public security.

With statistical tests for comparing means, by Independent Samples T-test, we find out that there is a significant difference of *the understanding level of facial recognition concept* and *using facial recognition technology as evidence to bring criminals to justice* between male and female. There is a significant difference of *attitudes for police should use facial recognition technology to better serve the public* and *the government will use facial recognition technology without notifying the public* between the between countries support facial recognition technology for use and countries restricted it to use. There is a significant difference of *the understanding level of facial recognition concept* between working field related to computer science or engineering and unrelated ones. By paired Sample T-test, We figure out the two factor *Gender* and *Education level* affected the public's attitudes stronger than the other factors. By ANOVA test, we figure out the two factor age range and the country where people live most has affected the public's attitudes stronger than the other factors.

200 survey respondents (79.68%) believe the facial recognition technology will be widely used in the next 10 years. In our daily life, the facial recognition system not always about the higher accuracy, it should also consider the security issue which is the public concerns most. There are still limitations in our work, we could not provide surveillance cameras to each survey respondents especially those who never had experienced facial recognition technology before. Facial recognition technology is a double-edged sword, the public wants to use facial recognition technology as a security measure but also worry about it could be misused in the wrong hands. Like most technology developing progress, any controversial technology needs correct regulation system, more mature technical support and the public's support.

7

Appendix

7.1 Facial Recognition Survey

All the survey questions are attached below.

7.2 Survey Comments

You can find all the survey comments from all the testers on Google drive link[1].

7.3 Follow-up Questions

You can find all the interviewees' replies on Google Drive link[2]

[1] https://drive.google.com/drive/folders/1kqHExjpOqIcXm9WBhVnyNWVwE9ZWomvq
[2] https://drive.google.com/drive/folders/1kqHExjpOqIcXm9WBhVnyNWVwE9ZWomvq

Facial Recognition Survey

Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours. In this survey, we want to assess the general public's attitude and perceptions of facial recognition technology applied to surveillance cameras. Your participation in this survey is very important to us. All of your answers are confidential and will be used strictly for education research. There will be no sales or marketing follow-up because of your participation in this survey. This survey is being administered for a master thesis research on Vrije Universiteit Amsterdam and Universiteit Van Amsterdam. This survey will run from October 23, 2019, until November 6, 2019. It will take approximately 8 minutes to complete. If you have any questions or comments about this survey, you may enter them into the form at the bottom of the survey or e-mail them to Chao Zhang at yellywong7@gmail.com.

Basic information questions:

1. What is your age range? *
   - ○ 18 - 30
   - ○ 31 - 40
   - ○ 41 - 50
   - ○ 51 - 60
   - ○ 61 - 70
   - ○ Over 70

2. What is your gender? *
   - ○ Male
   - ○ Female
   - ○ Prefer not to say

3. What is your education level? *
   - ○ Primary education
   - ○ Secondary education
   - ○ Bachelor or equivalent
   - ○ Master or equivalent
   - ○ Doctor or equivalent
   - ○ Other (please specify) _____

4. In which country have you lived most of your life? *
   - ○ United States
   - ○ United Kingdom
   - ○ China
   - ○ Netherlands
   - ○ Other (please specify) _____

5. Which of the following categories best describes the industry you primarily work in? *
   - ○ Computer science & IT
   - ○ Engineering & Technology
   - ○ Education & Training
   - ○ Government & Public officer
   - ○ Business & Finance & Insurance

○ Journalism & Media
○ Arts & Entertainment & Recreation
○ Law & Legal services
○ Medicine & Health care & Social assistance
○ Agriculture & Forestry & Fishing & Hunting & Mining & Real Estate
○ Homemaker & Freelancer
○ Retired & Unemployed
○ Prefer not to say
○ Other (please specify)_____

Objective judgment questions:

6. How well do you understand the “facial recognition” concept? *

   (*Facial recognition is a category of biometric software that maps an individual's facial features mathematically and stores the data as a faceprint. The software uses deep learning algorithms to compare a live capture or digital image to the stored faceprint in order to verify an individual's identity.*)

   ○ Very well
   ○ Somewhat
   ○ Neutral
   ○ Know about but don’t understand
   ○ Never heard about it

7. From what sources has your knowledge about facial recognition technology come? *

   (Please select all that apply)

   ☐ Print media
   ☐ Internet
   ☐ Scientific articles/journals
   ☐ Conversations with others
   ☐ Class at school/university
   ☐ Other (please specify) _____

8. What security measure(s) would you use to unlock your mobile phone? *

   (Select all that apply)

   ☐ Swipe
   ☐ Passwords
   ☐ Pattern recognition
   ☐ Finger prints
   ☐ Face ID
   ☐ I do not use any security measures
   ☐ Other (please specify) _____

9. What would be the primary reason for you to use FaceID to unlock your mobile phone? *

   ○ More accurate
   ○ More reliable
   ○ More secure

- ○ Faster
- ○ Easier
- ○ I am not sure
- ○ None of the above
- ○ Other (please specify) _____

10. What would be the primary reason for you to NOT use FaceID to unlock your mobile phone? *
    - ○ Less accurate
    - ○ Less reliable
    - ○ Less secure
    - ○ Slower
    - ○ More difficult
    - ○ I am not sure
    - ○ None of the above
    - ○ Other (please specify) _____

11. How knowledgeable are you about the usage of facial recognition technology by your country's government? *
    - ○ Very knowledgeable
    - ○ Somewhat knowledgeable
    - ○ Neutral
    - ○ Slightly knowledgeable
    - ○ Not knowledgeable at all

12. How much do you agree with the statement: "The public should be given the opportunity to consent or opt out of being subjected to facial recognition technology"? *
    - ○ Strongly agree
    - ○ Agree
    - ○ Neutral
    - ○ Disagree
    - ○ Strongly disagree

13. On a scale of 1 to 5, where 1 is not at all and 5 is very strongly, how strongly do you feel that use of facial recognition on surveillance cameras is an invasion of your privacy? *

○ 1 (not at all)
○ 2
○ 3
○ 4
○ 5 (very strongly)

14. How much do you agree the following purposes of using facial recognition technology? *

1) By police in criminal investigation
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
2) By police in their day to day policing
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
3) On smartphones, to allow a phone to 'unlock' in response to the owner's face
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
4) In airports security checkpoint
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
5) In supermarkets to verify whether someone is old enough to buy alcohol
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
6) In supermarkets to track shopper behaviour around the store and target products at shoppers
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
7) In schools to register pupils and check attendance
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
8) In schools to monitor pupils' expressions and behavior
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
9) In schools to prevent non-students from entering campus
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
10) On public transport to let paying customers through ticket barriers
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
11) On public transport to identify persons of interest for the police
○Strongly agree ○Agree ○Neutral ○Disagree ○Strongly disagree
12) At work to ensure workers do not enter unauthorised or high risk areas (e.g. construction zones)

〇Strongly agree 〇Agree 〇Neutral 〇Disagree 〇Strongly disagree

13) At work to monitor personality traits and mood of candidates when hiring for a job

〇Strongly agree 〇Agree 〇Neutral 〇Disagree 〇Strongly disagree

14) Events where massive amounts of people gather, e.g. sporting event, concert

〇Strongly agree 〇Agree 〇Neutral 〇Disagree 〇Strongly disagree

15) In apartment buildings to identify residents

〇Strongly agree 〇Agree 〇Neutral 〇Disagree 〇Strongly disagree

15. On a scale of 1 to 5, where 1 is very comfortable and 5 is not at all comfortable, how comfortable are you with the police using facial recognition technology? *

〇 1 (very comfortable)
〇 2
〇 3
〇 4
〇 5 (not at all comfortable)

16. Do you agree that police should use facial recognition technology to better serve the public? *

〇 Strongly agree
〇 Agree
〇 Neural
〇 Disagree
〇 Strongly disagree

17. Reasons for agreeing with police use of facial recognition technology: *

(Please select all that apply)

☐ It is beneficial for the security of society
☐ It is beneficial for my personal security
☐ It enhances existing security systems e.g. CCTV and others
☐ I can opt out or consent
☐ I trust them to use the technology ethically
☐ It will not be misused or hacked
☐ It is indiscriminate e.g. by race and gender
☐ It is accurate
☐ It is reliable
☐ It does not affect me personally

☐ I do not know

☐ None of the above

☐ Other (please specify) _____

18. Reasons for disagreeing with police use of facial recognition technology: *

(Please select all that apply)

☐ It infringes on the privacy of people in society

☐ It normalises surveillance

☐ I can't opt out or consent

☐ I do not trust them to use technology ethically

☐ It infringes on my personal privacy

☐ It will be misused or hacked

☐ It can be used to discriminate e.g. by race and gender

☐ It is not accurate

☐ It is not reliable

☐ It affects me personally

☐ I do not know

☐ None of the above

☐ Other (please specify) _____

Subjective judgement questions:

19. Would you feel safer if facial recognition technology was added to surveillance cameras **in your city**? *
    - ○ Yes
    - ○ No
    - ○ I am not sure

20. Do you agree that the use of facial recognition technology can help identify criminals more efficiently **in your city**? *
    - ○ Strongly agree
    - ○ Agree
    - ○ Neutral
    - ○ Disagree
    - ○ Strongly disagree

21. Do you agree that the facial recognition technology can help prevent crimes from occurring **in your city**? *
    - ○ Strongly agree
    - ○ Agree
    - ○ Neutral
    - ○ Disagree
    - ○ Strongly disagree

22. Do you agree that the use of facial recognition technology will deter terrorists **in your city**? *
    - ○ Strongly agree
    - ○ Agree
    - ○ Neutral
    - ○ Disagree
    - ○ Strongly disagree

23. Do you agree with using facial recognition technology as evidence to bring criminals to justice? *
    - ○ Strongly agree
    - ○ Agree

○ Neutral
○ Disagree
○ Strongly disagree

24. Do you believe that the government will use facial recognition technology without notifying the public? *
    ○ Strongly believe
    ○ Believe
    ○ Neutral
    ○ Disbelieve
    ○ Strongly disbelieve

25. How has learning more about facial recognition technology affected your opinion toward its use? *
    ○ I am now much more supportive of using facial recognition technology
    ○ I am now somewhat more supportive of using facial recognition technology
    ○ It had no affect
    ○ I am now somewhat less supportive of using facial recognition technology
    ○ I am now much less supportive of using facial recognition technology

26. Do you believe that facial recognition technology will be more widely used in the next 10 years? *
    ○ Strongly believe
    ○ Believe
    ○ Neutral
    ○ Disbelieve
    ○ Strongly disbelieve

27. Please list any additional comments you would like to share here:

    _____

Note: Thanks for taking the time to complete this survey. Your response is valuable for our research.

References

[1] Giuseppe Amato, Fabrizio Falchi, Claudio Gennaro, and Claudio Vairo. **A Comparison of Face Verification with Facial Landmarks and Deep Features**. *Tenth International Conference on Advances in Multimedia*, pages 1–6, 2018. vi, 13, 14

[2] Yinglu Liu, Hao Shen, Yue Si, Xiaobo Wang, Xiangyu Zhu, Hailin Shi, Zhibin Hong, Hanqi Guo, Ziyuan Guo, Yanqin Chen, Bi Li, Teng Xi, Jun Yu, Haonian Xie, Guochen Xie, Mengyan Li, Qing Lu, Zengfu Wang, Shenqi Lai, Zhenhua Chai, and Xiaoming Wei. **Grand Challenge of 106-Point Facial Landmark Localization**. *ICME Workshops*, pages 613–616, 2019. vi, 13, 15

[3] Joy Buolamwini and Timnit Gebru. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification**. *FAT*, pages 77–91, 2018. vi, viii, 20, 21, 22

[4] Jeffrey C.Price and Jeffrey S.Forrest. **Practical Aviation Security (Third Edition):Chapter 5 - Commercial aviation airport security**. *Butterworth-Heinemann*, pages 205–263, 7 2016. 1, 26

[5] Christopher Libby and Jesse M. Ehrenfeld. **Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare**. *J. Medical Syst.*, **45**:39, 2021. 1

[6] Antoaneta Roussi. **Resisting the rise of facial recognition**. *Nature 587*, pages 350–353, 11 2020. 1

[7] **Beijing Daxing International Airport to use facial recognition at security checkpoints [Online]**. 6 2019. 1

[8] **Beyond face value: public attitudes to facial recognition technology**. *Ada Lovelace Institute*, 9 2019. 1, 20, 24, 30, 66

[9] M. S. Lew N. Sebe and T. S. Huang. **The State-of-the-Art in Human-Computer Interaction**. *ECCV Workshop on HCI*, pages 1–6, 2004. 2

[10] Linda A. Bertram and Gunther van Dooble. **Nomenclatura - Encyclopedia of modern Cryptography and Internet Security: From AutoCrypt and Exponential Encryption to Zero-Knowledge-Proof Keys [Paperback]**. *Books on Demand*, 2019. 2

[11] Clive Norris and Gary Armstrong. **The Maximum Surveillance Society: The Rise of CCTV**. *Berg Publishers*, pages 1–6, 1999. 2

[12] N. Sebe, M. S. Lew, and T. S. Huang. **245 million video surveillance cameras installed globally in 2014 [Online]**. *IHS Technology*, pages 1–6, 6 2015. 2

[13] STEPHEN GRAHAM. **Planning Theory & Practice : CCTV - The Stealthy Emergence of a Fifth Utility?** *Taylor & Francis (Routledge)*, pages 237–241, 1 2002. 3

[14] Rahul Paliwal, Shalini Yadav, and Neeta Nain. **FaceID: Verification of Face in Selfie and ID Document**. *CPIV(2)*, pages 443–454, 2019. 3

[15] Feifei Liu. **Making Cutting-Edge Technology Approachable: A Case Study of Facial-Recognition Payment in China [Online]**. 5 2020. 3

[16] **GDPR Enforcement Tracker - list of GDPR fines [Online]**. 2021. 4

[17] Elliot Markowitz. **Tech giants press pause on facial recognition [Online]**. 6 2020. 4

[18] Lucas D. Introna. **Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems**. *Ethics and Information Technology*, pages 75–86, 5 2005. 4

[19] JAKE LAPERRUQUE. **Unmasking the Realities of Facial Recognition [Online]**. 12 2018. 5, 23

[20] **Future of Privacy Forum: PRIVACY PRINCIPLES FOR FACIAL RECOGNITION TECHNOLOGY [Online]**. 12 2015. 5

[21] Roberto Verdecchia, Ivano Malavolta, and Patricia Lago. **Architectural technical debt identification: the research landscape**. *TechDebt@ICSE 2018*, pages 11–20. 5, 6

[22] Elizabeth Goodman, Mike Kuniavsky, and Andrea Moed. **Observing the User Experience: A Practitioner's Guide to User Research**. *ACM SIGSOFT Softw. Eng. Notes 38(2): 35 (2013)*. 7, 26, 28, 29, 30

[23] Clive Norris, Mike McCahill, and David Wood. **The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space**. *Surveillance and Society 2(2)*, pages 110–135, 09 2004. 9, 10

[24] **Video Surveillance-Global Market Outlook (2016-2022): Video Surveillance-Global Market Outlook: Global Video Surveillance Market 2017 Analysis, Segmentation, Competitors Analysis, Product Research, Trends and Forecast by 2022 [Online]**. *Stratistics MRC*, 1 2017. 9

[25] **A Timeline Of CCTV [Online]**. 4 2018. 9

[26] Chris A Williams. **Police Surveillance and the Emergence of CCTV In the 1960s**. *Crime Prevention and Community Safety 5*, pages 27–37, 2003. 9

[27] Steven M. Cox, David Massey, Connie M. Koski, and Brian D. Fitch. **Introduction to Policing**. *SAGE Publications*, 2020. 10

[28] James Treadwell and Adam Lynes. **50 Facts Everyone Should Know about Crime and Punishment**. *JSTOR*, pages 264–267, 2019. 10

[29] Jess Young. **A History of CCTV Surveillance in Britain [Online]**. 1 2018. 10

[30] M. Nieto, K. Johnston-Dodds, and C. Simmons. **Public and Private Applications of Video Surveillance and Biometric Technologies**. *California State Library, California Research Bureau*, 2002. 10

[31] PAUL BISCHOFF. **Surveillance camera statistics: which cities have the most CCTV cameras? [Online]**. 5 2021. 10

[32] Brandon C. Welsh, David P. Farrington, and Amanda L. Thomas. **CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis**. *Criminology & Public Policy 18(1)*, pages 135–159, 3 2019. 11

[33] Brandon C. Welsh and David P. Farrington. **Crime prevention effects of closed circuit television: a systematic review**. *SagePublication,Vol. 587*, pages 110–135, 8 2002. 11, 12

[34] Sanjeev Kumar and Harpreet Kaur. **Face Recognition techniques: Classification and Comparisons**. *International Journal of Information Technology and Knowledge Management*, pages 361–363, 2012. 12, 17

[35] Chaochao Lu and Xiaoou Tang. **Surpassing Human-Level Face Verification Performance on LFW with GaussianFace**. *CoRR abs/1404.3840*, 2014. 12

[36] Guangpeng Zhang and Yunhong Wang. **Faceprint: Fusion of Local Features for 3D Face Recognition**. *ICB*, **5558**:394–403, 6 2009. 13

[37] Matthew Pruitt, Jason M. Grant, Jeffrey R. Paone, Patrick J. Flynn, and Richard W. Vorder Bruegge. **Facial recognition of identical twins**. *IJCB*, pages 1–8, 10 2011. 13

[38] Ciprian Adrian Corneanu, Marc Oliu Simon, Jeffrey F. Cohn, and Sergio Escalera Guerrero. **Survey on RGB, 3D, Thermal, and Multimodal Approaches for Facial Expression Recognition: History, Trends, and Affect-Related Applications**. *IEEE Trans. Pattern Anal. Mach. Intell.*, **38**:1548–1568, 2016. 17

[39] Dhanar Intan Surya Saputra and Kamal Miftahul Amin. **Face detection and tracking using live video acquisition in camera closed circuit television and webcam**. *2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, pages 154–157, 8 2016. 17

[40] Jörgen Ahlberg and Igor S. Pandzic. **Handbook of Face Recognition (2nd Edition): Facial Action Tracking**. *Springer*, pages 219–237, 2013. 17

[41] Sheng Zhang and Matthew Turk. **Eigenfaces**. *Scholarpedia*, **9**:4244, 2008. 18

[42] K. Sunil Manohar Reddy. **Comparison of Various Face Recognition Algorithms**. *International Journal of Advanced Research in Science, Engineering and Technology*, **4**, 2 2017. 18

[43] Aleix M. Martínez. **Fisherfaces**. *Scholarpedia*, **6**:4282, 2011. 18

[44] Laurenz Wiskott and Jean-Marc Fellous. **Face Recognition by Elastic Bunch Graph Matching**. *CAIP*, pages 456–463, 1997. 18

[45] Rakesh Saini, Abhishek Saini, and Deepak Agarwal. **Analysis of Different Face Recognition Algorithms**. *International Journal of Engineering Research and Technology (IGERT)*, **3**, 2014. 19

[46] Peace Muyambo. **An Investigation on the Use of LBPH Algorithm for Face Recognition to Find Missing People in Zimbabwe**. *International Journal of Engineering Research and Technology (IJERT)*, **7**, 2018. 19

[47] Deepak Ghimire and Joonwhoan Lee. **Geometric Feature-Based Facial Expression Recognition in Image Sequences Using Multi-Class AdaBoost and Support Vector Machines**. *CoRR*, **abs/1604.03225**, 2016. 19

[48] **The EU General Data Protection Regulation (GDPR) and Face Images [Online]**. 2018. 22

[49] Léa Steinacker, Miriam Meckel, Genia Kostka, and Damian Borth. **Facial Recognition: A cross-national Survey on Public Acceptance, Privacy, and Discrimination**. *CoRR*, **abs/2008.07275**, 2020. 22

[50] Chaochao Lu and Xiaoou Tang. **Surpassing Human-Level Face Verification Performance on LFW with GaussianFace**. *CoRR*, **abs/1404.3840**, 4 2014. 23

[51] Dmitry Kalenichenko Florian Schroff and James Philbin. **FaceNet: A Unified Embedding for Face Recognition and Clustering**. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 815–823, 6 2015. 23

[52] Mei Ngan Patrick Grother and Kayee Hanaoka. **Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification**. *National Institute of Standards and Technology (NIST) Interagency Report, 8238*, 11 2018. 23

[53] Pete Fussey and Daragh Murray. **Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology**. *University of Essex Human Rights Centre, section 2,1.1*, 7 2019. 23

[54] Nesli Erdogmus and Sebastien Marcel. **Spoofing Face Recognition With 3D Masks**. *IEEE Transactions on Information Forensics and Security*, pages 1084–1097, 7 2014. 23

[55] Pavel Korshunov and Sebastien Marcel. **DeepFakes: a New Threat to Face Recognition? Assessment and Detection**. *CoRR*, **abs/1812.08685**, 12 2018. 24

[56] Victor R. Basili, Gianluigi Caldiera, and H. Dieter Rombach. **Encyclopedia of Software Engineering: The Goal Question Metric Approach**. *Wiley*, pages 528–532, 1994. 26

[57] Waldemar Wojcik, Konrad Gromaszek, and Muhtar Junisbekov. **Face Recognition: Issues, Methods and Alternative Applications**. 6 2016. 27

[58] Burns Alvin and Burns Ronald. **Basic Marketing Research (Second ed.)**. *Upper Saddle River, N.J. : Pearson Prentice Hall*, 2008. 28, 29

[59] Thomas Haslwanter. **An Introduction to Statistics with Python**. *Springer Nature*, pages 1431–8784, 2016. 33

[60] Kent State University Libraries. **SPSS TUTORIALS: Analyzing Data [Online]**. 1 2021. 40, 41, 48, 57, 59