

BACHELOR THESIS  
ARTIFICIAL INTELLIGENCE

**Radboud University**



---

**Facial Recognition Technology (FRT)  
used for active criminal case investigation  
may undermine democratic legitimacy.**

---

*Author:*  
Hannah Zwart  
s1036065

*First supervisor:*  
L.M. van Elteren  
Donders Institute  
lotte.vanelteren@donders.ru.nl

*Second reader:*  
A.C.P. Peeters  
Faculty of Social Sciences  
anco.peeters@ru.nl



January 27, 2023

## **Abstract**

Facial recognition technology (FRT) used for active criminal case investigation has been deployed by many police agencies around the world . The use of FRT in this context provides hard evidence as well as economic- and time efficiencies. However, this use of FRT also has some risks attached to it. This thesis will investigate how these risks might undermine the democratic legitimacy. Keeping democratic legitimacy is very important for a regime or government as it means that that regime or government is accepted by the majority of people falling under that regime or government. If this is not the case, that regime or government would face deadlock or collapse. Democratic legitimacy has three different sources: political accountability, voice and due liberation. This thesis will discuss the risks that FRT used in this context poses to the democratic legitimacy by linking the risks to the sources of democratic legitimacy. It will then look into Super-Recognizers as an alternative to the use of FRT in the context of criminal case investigation. The scope of this thesis is limited to the risks associated with FRT in the context of criminal case investigation, these risks might not apply to FRT used in other contexts. It also only mentions risks that can be linked to the three sources of democratic legitimacy.

# Contents

|          |                                    |           |
|----------|------------------------------------|-----------|
| <b>1</b> | <b>Introduction</b>                | <b>2</b>  |
| 1.1      | Overview . . . . .                 | 3         |
| <b>2</b> | <b>FRT</b>                         | <b>4</b>  |
| 2.1      | Intended purpose . . . . .         | 4         |
| 2.2      | Means . . . . .                    | 4         |
| 2.2.1    | Software . . . . .                 | 4         |
| 2.2.2    | Database . . . . .                 | 5         |
| 2.3      | Implementations . . . . .          | 5         |
| <b>3</b> | <b>Democratic legitimacy</b>       | <b>7</b>  |
| 3.1      | Definition . . . . .               | 7         |
| 3.2      | Models and sources . . . . .       | 7         |
| <b>4</b> | <b>Risks</b>                       | <b>9</b>  |
| 4.1      | Technology . . . . .               | 9         |
| 4.1.1    | Accuracy and racial bias . . . . . | 9         |
| 4.1.2    | Rapid development . . . . .        | 10        |
| 4.2      | Use and regulation . . . . .       | 10        |
| 4.2.1    | Overreach . . . . .                | 10        |
| 4.2.2    | Privacy . . . . .                  | 10        |
| 4.2.3    | Database management . . . . .      | 11        |
| <b>5</b> | <b>Solutions</b>                   | <b>12</b> |
| 5.1      | Super-Recognizers . . . . .        | 12        |
| 5.1.1    | Project BeSure . . . . .           | 12        |
| 5.1.2    | Risks addressed . . . . .          | 13        |
| <b>6</b> | <b>Discussion</b>                  | <b>14</b> |
| 6.1      | Findings . . . . .                 | 14        |
| 6.2      | Further research . . . . .         | 14        |
| 6.3      | Limitations . . . . .              | 15        |
| 6.4      | Conclusion . . . . .               | 15        |
| 6.5      | Recommendations . . . . .          | 15        |
| <b>7</b> | <b>Acknowledgments</b>             | <b>16</b> |

# Chapter 1

## Introduction

Police are constantly looking for new technologies that might help them in their criminal case investigation. Facial Recognition Technology (FRT) is an example of such new technology as it can help the police follow and generate leads within an investigation [2]. This is why FRT is now being rapidly introduced in many police authorities around the world [9].

This large scale use of FRT by different police authorities really calls for extensive research into the benefits and, more importantly, the risks of using FRT within the context of active criminal case investigation. There already has been quite some research into the benefits and risks of using FRT in this context [9]. Advocates of the police using FRT are saying it can help solve more criminal cases and can cut back the time and costs it takes to solve a case, as it helps to generate and follow leads [2]. Using these technologies for these purposes however also comes with some costs as it poses the threat to deepen discriminatory policing and can really hurt the relationship between citizens and police [9] [6].

It is also very important to relate the risks posed by using FRT for active criminal case investigation to certain aspects of a society, such as democratic legitimacy, since it could potentially threaten the functioning of a society [4]. The main question this thesis will focus on is if Facial Recognition Technology used for active criminal case investigation may undermine democratic legitimacy.

To answer this we must first know what FRT exactly is. FRT refers to technology that is used to distinguish and identify a person's biometrics [5]. Even though the implementation of this type of technology varies per institution, the main goal stays the same; the identification of a specific subset of people. FRT can be used by the police for active criminal case investigation amongst other applications. It has for example been used to establish probable cause for the arrest of a suspect of a fight that has been posted on YouTube, as well as for passport fraud, identity theft cases and many other cases. [10]

We must also find out what democratic legitimacy exactly is and why it is so important to analyze possible risks to democratic legitimacy. Democratic legitimacy means that a regime or government is accepted by the majority of people falling under that regime or government and that the people follow the rules and decisions of that regime or government voluntarily and not just compliance by means of power alone [23, chapter 11] [4]. Democratic legitimacy is very important to protect within a regime or government, since if there is no democratic legitimacy, that regime or government will face deadlock or

eventually even collapse. This is why it is very important to analyze the risks that FRT used for active criminal case investigation may pose to democratic legitimacy.

As previously mentioned, the objective of this thesis is to find out if the use of Facial Recognition Technology used for active criminal case investigation may undermine democratic legitimacy. This is thus very necessary to analyze since the police's use of FRT is all around the world and could thus pose serious threats to many different governments and regimes all around the world.

## 1.1 Overview

To better assess the risks associated with FRT used for active criminal investigation we must first analyse what FRT exactly entails. To do this, multiple levels of analysis are introduced for a better separation of concerns. A position paper on analysing the impacts of facial recognition [7] introduces multiple levels of separation of which several were useful to better understand the use of FRT used for criminal investigation; namely purpose, means and implementation. The intended purpose justifies the use of the software and describes the ultimate objective. Next up, the means describes the strategy being used to achieve the intended purpose; i.e. it explains how FRT works. The implementation then addresses the existing case uses.

Second, we will look into what democratic legitimacy is exactly and what some of those important values to preserve democratic legitimacy are.

Third, once we know what the sources are for democratic legitimacy we will look into the risks that FRT used for criminal investigation poses for these sources and thus ultimately also to democratic legitimacy itself.

Fourth, we can look at an alternative to the use of FRT and see what risks will be addressed by this alternative.

Last, we will discuss our findings, implication for future research and limitations, conclude our results and mention our recommendations on the matter.

# Chapter 2

## FRT

In this chapter we will explain Facial Recognition Technology (FRT). First, we will dive into what the intended purpose of using FRT used for criminal case investigation is. Second, we will dive into the means used to achieve the purpose; i.e. how FRT works. Third, we will look at some current day implementations of FRT used for criminal case investigation.

### 2.1 Intended purpose

Police authorities all around the world are constantly looking for new technologies to help them in the process of catching and prosecuting criminals [2]. This is also driven by the public's expectation to deliver value for their tax money and reduce (labor)costs along the way. This need for economic efficiencies has driven many new technologies to be used by a lot of police authorities, amongst which is FRT used for active criminal case investigation.

The use of FRT also helps the police follow and generate leads [2]. This is again beneficial from an economic standpoint, since a case can be solved in a shorter amount of time, but is also a huge benefit to the people involved in the case, such as the victims of the crimes that get some form of closure sooner or possible suspects that can be ruled out faster.

### 2.2 Means

The application of FRT for active criminal case investigation is based on identification, meaning that these applications are used to discover the identity of a person by matching their faces to faces stored in a database [8].

#### 2.2.1 Software

There are numerous software developed for facial recognition [5]. The software first has to extract the face(s) out of the footage, it thus has to differentiate faces from the rest of the background. Once a face is extracted it has to measure the various features. These features are distinguishable landmarks made up out of peaks and valleys of the face. Each face has around 80 different landmarks on which the software can be trained, such as distance between the eyes, width of nose, depth of eye sockets, shape of cheekbones and length of jaw line. The different landmarks are then stored as numbers that together,

called a faceprint, represent the face. The faceprints in the database are then compared to the new footage for the purpose of identification. This method can be combined with surface texture analysis, which as the name suggests also analyses the different textures in the face, for even better accuracy. The employment of these technologies can be done through various means, such as body cameras worn by police, closed-circuit television, smart glasses, drones, et cetera [6].

### 2.2.2 Database

The collecting of images varies per company [19]. Historically, the database used by law enforcement agencies consisted of government-stored images, such as mugshots and driver-license photos. These images can be added to or removed from the data base according to laws set by the country [12].

However, there is also a more intrusive way of collecting images called ‘data scraping’ [19]. Data scraping is done by a software that will search multiple sites on the internet, such as employment-, news- and education sites as well as various social media platforms (e.g. linkedin, facebook and instagram). This way of collecting data is of course quite controversial from a privacy standpoint, but has shown better accuracy.

## 2.3 Implementations

Police authorities all over the world make use of FRT for active criminal case investigation.

In 2000, Pinellas County’s Face Analysis Comparison & Examination System (FACES) was arranged [21]. The first arrest attributed to FACES was in 2004, where a wanted woman gave deputies a false name. The number of arrests attributed to FACES grew over the years and the latest list in 2014, which did not have a complete record of all case uses, showed over 400 successful identifications using FACES. These records showed insight into what crimes were most suitable for FRT to solve, which were shoplifting, check forgery and ID fraud.

One example of a specific case where FACES was very useful was a case where the FBI was tracking a fugitive accused of child rape, which typically involved people using multiple fake IDs or aliases [21]. FACES was useful to link these IDs or aliases to track the fugitive.

Other cases involved people that were not able to identify themselves, such as individuals with Alzheimer’s or murder victims.

Since 2019, 600 Law enforcement agencies spread over the United States have been using a FRT called ‘Clearview’[19]. ‘Clearview’ makes use of a software that performs data scraping to collect images for the database. This database is the largest known database of over 30 billion images [1]. Due to the data of a large number of individuals, the software can get an identification on more people and the identification itself is more accurate.

The Dutch police use a FRT called ‘CATCH’ [12]. The images stored in the database used by ‘CATCH’ are mostly from another database that is being kept by ‘Justid’ and ‘Veiligheid’. ‘Justid’ stands for judicial information service, which is an agency that keeps all kinds of data on citizens and makes sure the necessary information about a person is accessible [13]. ‘Veiligheid’ is a knowledge center on injury prevention, which is committed to making living safer by stimulating safe behaviour in a safe environment [22].

One can be stored in that database when they are a suspect of a relatively serious crime. However, one must be deleted from the database once they are no longer a suspect, no appeal has been lodged and is active, they have not been convicted before and there are no other cases active against them.

## Chapter 3

# Democratic legitimacy

In this chapter, we will dive into what democratic legitimacy is. We will first look at its definition. Second, we will look at the different models of democracy. Third, we will look at the different sources of democratic legitimacy.

### 3.1 Definition

Legitimacy on its own means that a regime, system of governance or a government itself is accepted by the majority of people falling under that regime or government [4]. If a regime or government is not considered legitimate it would face deadlock (i.e. an impasse) or collapse at some point. This means that for a regime or government to work it would need to justify itself to the people, which can be done through various means. One of the ways a regime or government can be justified is through democracy, which brings us to democratic legitimacy.

For a regime to be considered democratically legitimate people would need to follow its rules and decisions voluntarily and not just compliance by means of power alone [23, chapter 11]. When the majority of people follow the rules and decisions of a regime or government voluntarily, it means that they essentially accept that regime or government, which is the essence of legitimacy.

It is thus really important to make sure people do feel like they voluntarily follow a regime's or government's rules and decisions and ultimately accept that regime or government. This in itself is a very large objective, which means we need to look at some smaller values to protect this larger objective.

### 3.2 Models and sources

To really understand how we can protect democratic legitimacy and analyze possible risks to it, we must look at the core values of democratic legitimacy. If one or more of those core values are at risk, we can conclude that democratic legitimacy in its entirety is at risk. To understand what the core values are for democratic legitimacy we would need

to look a bit deeper into some of the models for democracy, as these models describe the different sources, and thus core values, of democratic legitimacy.

There are multiple kinds of models that describe democracy, which all highlight different aspects of democracy and democratic legitimacy. It is important to look at all of these different models and aspects to democracy to get a more complete picture of what democracy exactly entails and what values democratic legitimacy stems from. Klijn and Edelenbos [11] described the core focus points of these different models. First, the liberal and competitive models tend to focus more on the accountability on the side of the officeholders. Second, the idealistic models focus more on active participation of citizens and emphasises the importance of this participation in the decision making process. At last the deliberative models introduce the importance of deliberation and rules to open and free discussions.

These different focus points of the models of democracy have then been summarized into 3 different sources of democratic legitimacy: political accountability, voice and due liberation [11]. The first source, political accountability, stresses the formal accountability of officeholders and the procedures to hold them accountable, such as voting to select or remove someone from office. The second source, voice, stresses the active influence of the citizens and their participation in the making of concrete decisions. In essence it looks at the citizens real involvement. The third source, due liberation, stresses the interactions and deliberation processes. This source stresses that there should be a good deliberation process based on clear agreements. In this deliberation process actors share knowledge, explore solutions and exchange their opinions on the matter.

# Chapter 4

## Risks

As with other types of new technology citizens are often sceptical of the new technology itself, how the police might utilise that new technology and how these technologies and their uses might impact the public's privacy and rights [6]. When the public loses confidence in how the police utilises a technology and what technology they use, the police-citizens relationship might deteriorate. This can happen when the use of a certain piece of technology is not legitimized through a democratic process along with clear rules on how it can be used. This plays into the second source mentioned for democratic legitimacy; voice.

When people feel like they did not have an active involvement into the decision making process on regulations/use of a piece of technology it can create distrust of the citizens towards the government and police. And vice versa, distrust of the citizens in the government and police can make the citizens question whether the government has the citizens best interest in mind when legitimizing and regulating the use of FRT used for criminal case investigation.

Furthermore, as previously mentioned (see chapter 3.1) people should follow a regime's rules and decisions voluntarily and not just by means of power alone [23, chapter 11], which is not the case when people feel like the police and government do not have the citizens' best interest in mind.

This chapter explores the different kinds of risks posed by FRT used for criminal case investigation. First, we look into the technological risks posed by FRT. Second, we look at the risks posed by the use and (lack of) regulation of FRT.

### 4.1 Technology

This section explores risks that do not lie with who is using the technology or how it is regulated, but rather with the accuracy of the technology and its biases and advancements.

#### 4.1.1 Accuracy and racial bias

FRT is often used by the police to help follow and generate leads for the investigation [16]. These leads are then presented to eye-witnesses in order to get a positive identification. The problem is that these identification by eye-witnesses are the number one cause for wrongful convictions, and the use of FRT may set up the conditions for these false positive identifications. This is because these FRT try to find matches to an image in a large

data-base and come up with people that closely resemble the original image. Sometimes a person will resemble the individual in the original image so closely that the police will select that person as a lead in their investigation and the eye-witness will mistakenly misidentify the person as they are not able to tell the difference.

FRT can also unintentionally criminalize marginalized communities as these technologies currently still have racial biases due to the way these algorithms are trained. For FRTs created in countries such as Germany and the USA, where the majority of people are Caucasian, the identification of non-Caucasians are consistently less accurate than the identification of Caucasians and white-passing people [20]. It has also been shown that for FRTs created in Asian countries such as China and Korea the identification is most effective for the identification of Asian people [14]. This means the accuracy of the identification of FRTs is related to the training data and we find racial biases in all FRTs. This of course creates more distrust of people in these marginalized communities towards the police and thus hurts the police-citizens relationship even more.

### **4.1.2 Rapid development**

The rapid developments in FRT raises some concerns. First of all, rapidly advancing technology is hard to regulate as it makes things possible that were not previously considered by the law. Second, it makes people question the future use of this technology as the use can expand to different settings and locations and can even be deliberately weaponized to target communities that are already experiencing overpolicing [6].

## **4.2 Use and regulation**

There are also risks that are not strictly technological but are rather related to the use(r) of the technology and its regulation and management. This section will explore those risks and how they might affect the democratic legitimacy.

### **4.2.1 Overreach**

Overreach in this context refers to the fear that the police might extend their legitimate power to illegitimate or excessive forms. More specifically in this case it is the fear that the police might use FRT for other purposes or in other forms than what they were given legitimate permission for [6]. FRT would for example enable the police to create a detailed database on people's actions and whereabouts, which raises questions on having control of personal data and the use of this data [15]. This can also relate to criticism of other countries, such as China and Russia, that have a reputation of state control with very little public oversight or voice and the fear of another country falling into a similar regime.

The fear for overreaching is again a sign of the distrust that citizens have in the police and thus has a negative effect on democratic legitimacy as explained in the introduction of this chapter.

### **4.2.2 Privacy**

There are also concerns on how the use of FRT by the police (for criminal case investigation) might limit a person's privacy in public as well as private spaces. Again this breach in privacy creates a feeling of being distrusted by the police and can create reciprocal feelings of distrust as their values are not respected [6].

### 4.2.3 Database management

Some of the regulations on how FRT can be used are not per se on the technology itself but rather on the databases. This can be regarding how the data is collected or the management of the data. This means that the risks are not directly a result of the technology itself but rather of the use of this technology and thus lie within the scope of this paper.

As mentioned previously (see chapter 2.3) the dutch police make use of a facial recognition software called ‘CATCH’ and the images stored in the database used but this software are mostly from a database kept by ‘Justid’ and ‘Veiligheid’ [12]. One can be stored in that database when they are a suspect of a relatively serious crime. However, one must be deleted from the database once they are no longer a suspect, no appeal has been lodged and is active, they have not been convicted before and there are no other cases active against them.

Unfortunately, the deleting of people in the database has not been well kept by ‘Justid’. Between 2010 and 2019 the judge acquitted 71.000 people. ‘Justid’ then has to evaluate these cases en determine whether they meet all the requirements of being deleted from the database, but in reality only 16.200 cases were treated by ‘Justid’ of which 92,8 percent were actually approved. John Riemen, head of the center of bio metrics of the dutch police and administrator of ‘CATCH’, later acknowledged that it was already internally known that people would be in the CATCH-database unjustified when the police started using facial recognition on the said database because it was badly maintained [12].

As the procedure for managing the database was not properly followed for many of the cases, mistrust was evoked among the people. This mistrust was a product of the government and police authorities not keeping their word, which could result in people thinking the police will not keep their word on matters more often. They might lose faith in the police sticking by their own rules. This can have a negative effect on the previously mentioned police-citizens relationship.

# Chapter 5

## Solutions

We have seen that there are multiple risks regarding democratic legitimacy posed by FRT used for criminal case investigation. In this part we will look at an alternative to the use of FRT for criminal case investigation that would reduce or eliminate some of the risks. Then we will discuss what risks were and what risks were not addressed by this alternative.

### 5.1 Super-Recognizers

Super-Recognizers is a term for people with superior face processing ability [18]. These Super-Recognizers are interesting for cognitive scientists and practitioners as they offer information on the underlying processes involved with superior face processing abilities. But not only are they interesting for insight in brain processes, they are also useful for the identification of individuals from close circuit television (CCTV). This is where the abilities of Super-Recognizers overlap with those of FRT, which means that Super-Recognizers could be deployed as an alternative to the use of FRT for the purpose of identifying individuals from footage.

The definition of what qualifications actually makes an individual a Super-Recognizer slightly varies.[17] Empirically, Super-Recognizers are individuals that possess superior face processing abilities. They would need to be superior in face perception as well as recognition and identification. In law enforcement settings the label of a Super-Recognizer is given to individuals with varying skill sets that range from person recognition or matching to detection of suspicious behaviour.

The problem with using Super-Recognizers as an alternative to FRT in the context of criminal case investigation is that Super-Recognizers would not be able to work on such a large scale as FRT would work. Super-Recognizers would for example not be able to remember and recognize over 30 billion images, as opposed to ‘Clearview’[19].

#### 5.1.1 Project BeSure

Project BeSure is a multi-level tool created in collaboration with The Berlin police used to identify individuals with superior face processing abilities [17]. This project is important for two reasons. The first reason is to assess the skills that were necessary for the intended purpose, in this case to recognize and identify individuals in a certain environment, for

example on CCTV. The second reason is to make sure the procedures are empirically validated in a controlled setting, here the controlled setting would be among police officers.

### 5.1.2 Risks addressed

The first risk of using FRT mentioned was accuracy and racial bias. This risk would not be addressed by using super-Recognizers instead of FRT, as Super-Recognizers, just like typical receivers, suffer from the other-ethnicity effect [3]. This effect refers to the biases in face recognition where individuals are better at recognizing people from their own ethnicity, compared to people with other ethnicities.

The second risk mentioned was rapid development. This risk would be addressed as the deployment of Super-Recognizer would eliminate the use of FRT for the purpose of criminal case investigation. So even though the technology could still be further developed, it would not be in use for criminal case investigation. This solves the issues surrounding regulating such a rapidly evolving technology and weaponizing such technology on this context.

The third risk mentioned was overreach. This risk would be addressed by using Super-Recognizers as an alternative to FRT, as the use of this technology in its entirety would be prohibited, and thus not legitimized, in the context of criminal case investigation. This means that it would be harder to employ the technology for illegitimate use.

The fourth risk was privacy. This risk would still apply as CCTV and databases with biometrics on individuals would still be used.

The last risk was database management. Unfortunately, there would still be a need for a database with information on people's faces, such as images, as this information would still be necessary to identify or recognize individuals.

# Chapter 6

## Discussion

In this chapter we will first summarize the findings of this paper. Second, we will discuss implications for further research and society. Third, we will look at the limitations of this paper. Fourth, we will shortly conclude our findings. And last, we will discuss our recommendations.

### 6.1 Findings

Even though the use of FRT for criminal case investigation does have some nice benefits, such as the economic benefits and hard evidence it can provide, there are also some serious risks attached to it with regards to democratic legitimacy.

Of the three sources of democratic legitimacy we found that the second source, voice, seemed to be at risk due to the risks associated with FRT used for criminal case investigation. When one or more of the sources of democratic legitimacy is undermined, democratic legitimacy as a whole is ultimately also undermined.

We have also looked at some solutions that would address certain risks to democratic legitimacy associated with FRT used for criminal case investigation and found that using Super-Recognizers might be a nice alternative to using FRT in this context. It does have its limitations compared to FRT regarding scale, but it is worth further investigating.

### 6.2 Further research

We believe that FRT in the context of criminal case investigation poses quite some risks to the democratic legitimacy, which is reason enough to ban the use of FRT in this context and look for alternatives that do protect the democratic legitimacy. It would be interesting to further develop ways in which Super-Recognizers could be used on a larger scale or look into other alternative to the use of FRT. The scope of this paper was limited to FRT being used for criminal case investigation, but it would also be interesting to further investigate the risks associated with FRT being used in other contexts, such as facial recognition to unlock your phone.

### **6.3 Limitations**

As mentioned in the previous section, the scope of this paper was limited to FRT being used for criminal case investigation. This means that the risks associated with FRT in this context do not necessarily apply to other FRT used in different contexts. The scope of this paper was also limited to the risks that can be linked to democratic legitimacy. This was done by linking the risks to the sources of democratic legitimacy. In this paper only a link to the second source for democratic legitimacy, voice, was made as we could not find a connection to the other sources, political accountability and due liberation. Also, this paper might not fully encompass all the risks associated with FRT used, as the time scope was limited.

### **6.4 Conclusion**

One of the sources of democratic legitimacy, voice, is at risk by the use of Facial Recognition Technology for active criminal case investigation, which means that democratic legitimacy as a whole is at risk by the use of Facial Recognition Technology for active criminal case investigation. This is why we can conclude that Facial Recognition Technology used for active criminal case investigation does undermine democratic legitimacy.

### **6.5 Recommendations**

We would not recommend FRT to be used by the police in the context of active criminal case investigation due to the serious risks this use poses to democratic legitimacy. We do believe that some of the risks could be (partially) addressed by further research into for example the training of the algorithm, which could eliminate risks regarding lack of accuracy and racial bias. Also the data base management risk that was illustrated with an example of the database kept by ‘Justid’ and ‘Veiligheid’ could possibly be addressed, but since the reasons for this lack of database management could not be found, it is very hard to say if there is a solution to prevent this from happening. However, even with some of these risks addressed, we could not support the use of FRT used for criminal case investigation as it would still pose other risks to democratic legitimacy. We do believe that there is more potential in using Super-Recognizers as an alternative to using FRT in this context, but there are still multiple risks that were not addressed by this alternative, which means that we also could not support this alternative as it is now. We highly recommend finding a solution to address all the risks posed by Facial Recognition Technology in the context of criminal case investigation, may it be via further investigation the use of Super-Recognizers or some other alternative.

## Chapter 7

# Acknowledgments

I would very much like to thank my supervisor, L.M. van Elteren, for all her advise and help on the project. Her guidance helped me get through all the stages of this project and offered me structure.

Next I would like to thank my thesis group members for giving me advise on the project and making the overall project more pleasurable.

# Bibliography

- [1] Clearview AI, *Law enforcement*, Available at: <https://www.clearview.ai/law-enforcement>.
- [2] Denise Almeida, Konstantin Shmarko, and Elizabeth Lomas, *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of us, eu, and uk regulatory frameworks*, *AI Ethics* **2** (2021), Available at: <https://link.springer.com/article/10.1007/s43681-021-00077-w>.
- [3] Sarah Bate, Rachel Bennetts, Nabil Hasshim, Emma Portch, Ebony Murray, Edwin Burns, and Gavin Dudfield, *The limits of super recognition: An other-ethnicity effect in individuals with extraordinary face recognition skills.*, *Journal of Experimental Psychology: Human Perception and Performance* **45** (2019), no. 3, Available at: <https://psycnet.apa.org/record/2018-64938-001>.
- [4] Joachim Blatter, *legitimacy.*, (2018), Available at: <https://www.britannica.com/topic/legitimacy>.
- [5] Kevin Bonsor and Ryan Johnson, *How facial recognition systems work*, (2018), Available at: <https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>.
- [6] Adelaide Bragias, Kelly Hine, and Robert Fleet, *‘only in our best interest, right?’ public perceptions of police use of facial recognition technology*, *Police Practice and Research* **22** (2021), no. 6, Available at: <https://www.tandfonline.com/doi/abs/10.1080/15614263.2021.1942873?journalCode=gppr20>.
- [7] Claude Castelluccia and Daniel le Métayer, *Position paper: Analyzing the impacts of facial recognition*, *Privacy Technologies and Policy* **12121** (2020), Available at: [https://link.springer.com/chapter/10.1007/978-3-030-55196-4\\_3](https://link.springer.com/chapter/10.1007/978-3-030-55196-4_3).
- [8] Claude Castelluccia and Daniel le Métayer Inria, *Impact analysis of facial recognition: Towards a rigorous methodology*, (2020), Available at: <https://hal.inria.fr/hal-02480647/document>.
- [9] Peter Dauvergne, *Facial recognition technology for policing and surveillance in the global south: a call for bans*, *Third World Quarterly* **43** (2022), no. 9, Available at: <https://www.tandfonline.com/doi/abs/10.1080/01436597.2022.2080654?journalCode=ctwq20>.
- [10] Kristine Hamann and Rachel Smith, *Facial recognition technology: Where will it take us?*, (2019), Available at: <https://pceinc.org/wp-content/uploads/2019/11/20190528-Facial-Recognition-Article-3.pdf>.

- [11] Erik Hans Klijn and Jurian Edelenbos, *The influence of democratic legitimacy on outcomes in governance networks*, *Administration Society* **45** (2013), no. 6, Available at: [https://www.researchgate.net/publication/254756883\\_The\\_Influence\\_of\\_Democratic\\_Legitimacy\\_on\\_Outcomes\\_in\\_Governance\\_Networks](https://www.researchgate.net/publication/254756883_The_Influence_of_Democratic_Legitimacy_on_Outcomes_in_Governance_Networks).
- [12] Stan Hulsen, *Tienduizenden mensen mogelijk onterecht in gezichtendatabase van de politie*, (2021), Available at: <https://www.nu.nl/tech/6121460/tienduizenden-mensen-mogelijk-onterecht-in-gezichtendatabase-van-de-politie.html>.
- [13] Justitiële Informatiedienst, *Over ons*, Available at: <https://www.justid.nl/over-ons>.
- [14] P Jonathon Phillips, Fang Jiang, Abhijit Narvekar, Julianne Ayyad, and Alice J O'Toole, *An other-race effect for face recognition algorithms*, *ACM Transactions on Applied Perception* **8** (2011), no. 2, Available at: <https://dl.acm.org/doi/abs/10.1145/1870076.1870082>.
- [15] Sikender Mohsienuddin Mohammad, *Facial recognition technology*, (2020), Available at: <https://deliverypdf.ssrn.com/delivery.php?ID=6170220221210920810930310050730840280160530890470610030650240870880850960290080750661EXT=pdf&INDEX=TRUE>.
- [16] Laura Moy, *Facing injustice: How face recognition technology may increase the incidence of misidentifications and wrongful convictions*, *William Mary Bill of Rights Journal* **30** (2021), no. 2, Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4101826](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4101826).
- [17] Meike Ramon, *Super-recognizers – a novel diagnostic framework, 70 cases, and guidelines for future work*, *Neuropsychologia* **158** (2021), Available at: <https://www.sciencedirect.com/science/article/pii/S0028393221000609>.
- [18] Meike Ramon, Anna K. Kobak, and David White, *Super-recognizers: From the lab to the world and back again*, *British Journal of Psychology* **110** (2019), no. 3, Available at: <https://bpspsychub.onlinelibrary.wiley.com/doi/full/10.1111/bjop.12368>.
- [19] Isadora Neroni Rezende, *Facial recognition in police hands: Assessing the ‘clearview case’ from a european perspective*, *New Journal of European Criminal Law* **11** (2020), no. 3, Available at: [https://journals.sagepub.com/doi/full/10.1177/2032284420948161?casa\\_token=t50ZBkKNqDwAAAAA%3Ap55P8PHsdL06TTYcfTBbdVFiH-VaMLgWI3X4eQ9CTrrZgUQZZNTC8clfGYmzSgauS0IxBHkQeSY-g#tab-contributors](https://journals.sagepub.com/doi/full/10.1177/2032284420948161?casa_token=t50ZBkKNqDwAAAAA%3Ap55P8PHsdL06TTYcfTBbdVFiH-VaMLgWI3X4eQ9CTrrZgUQZZNTC8clfGYmzSgauS0IxBHkQeSY-g#tab-contributors).
- [20] Sarah Valentine, *Impoverished algorithms: misguided governments, flawed technologies, and social control*, *Fordham Urban Law Journal* **46** (2019), no. 2, Available at: [https://heinonline.org/HOL/Page?handle=hein.journals/frdurb46&div=14&g\\_sent=1&casa\\_token=&collection=journals](https://heinonline.org/HOL/Page?handle=hein.journals/frdurb46&div=14&g_sent=1&casa_token=&collection=journals).
- [21] Jennifer Valentino-DeVries, *How the police use facial recognition, and where it falls short*, *The New York Times* (2020), Available at: <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

- [22] Veiligheid, *Over ons*, Available at: <https://www.veiligheid.nl>.
- [23] Bernhard Weßels, *How europeans view and evaluate democracy*, (2016), Available at: <https://academic.oup.com/book/25893/chapter-abstract/193602218?redirectedFrom=fulltext>.