“BUT THEY DO IT TOO”

THE DUTCH NATIONAL POLICE AND REAL-TIME FACIAL RECOGNITION TECHNOLOGY

Student: Eva Krikken
Student number: 4116933
Programme: Applied Ethics MA
Institution: Utrecht University

Supervisor: Jonathan Benson
Second reader: Sven Nyholm
Date: 20.01.2021
Word count: 13.964

Table of contents

Summary

In this thesis, the justification given by the Dutch police for their experiments with real-time facial recognition technology (FRT) is scrutinised with regard to its validity. This justification holds that normalisation of real-time FRT in society provides grounds for experiments with and use of the technology, as it is expected to lead to societal pressure on authorities to use the technology as well. The argument developed in this thesis shows that this justification is fallacious, as it rests on two invalid assumptions, namely 1) that normalisation of a technology within society emerges independent from existing social structures, and 2) that public support can be inferred from private choices. Moreover, a possible more nuanced reading of this justification is also proven to be unconvincing, namely that substantial threats to national security, in addition to the normalisation of real-time FRT in society, will lead to societal pressure to use the technology and therefore provides grounds for the experiments. It is shown that substantial threats to national security only lead to societal pressure to explore ways to counter these threats – real-time FRT is just presented and therefore regarded as the most effective way to do so. To end on a more constructive note, deliberative democracy is proposed as a possible way forward for public authorities to gain a more well-informed understanding of public opinion on whether and when the use of real-time FRT by authorities is justified.

1. Introduction

Ever since humanity exists, the outsourcing of actions to artifacts has been common practice. We crafted spears to improve our ability to catch fish, we invented washing machines to take manual washing off our hands, and we developed a wide range of vehicles to increase our moving speed and space. In the last couple of years, a new tool has entered the scene: facial recognition technology (FRT). As the name already suggests, it allows us to outsource the practice of recognising a person on the basis of their face – automatically and remotely, with the help of cameras and algorithms. The recognition process takes place in two stages: the enrolment stage and the recognition stage (van Rest et al. 2021, 21). In the enrolment stage, biometric descriptions of faces, also known as facial templates, are entered into a database. A facial template consists of a unique collection of data points, analogues to a fingerprint. In the recognition stage, an algorithm is trained to detect faces on photos or video footage, after which it will convert these faces into facial templates as well. Subsequently, these templates are compared to the templates already in the database, leading to a match when the template of the detected face corresponds to one of the templates in the dataset. This process can be used either for authentication (verifying a person's identity) or identification (searching for a person's identity) (Louradour and Madzou 2021, 7), and can take place after an event, or in real-time with the use of a camera's live stream (Louradour and Madzou 2021, 12).

Even though this process is quite complex, it underlies several of our daily practices. The software is installed into our phones to recognise our faces as we try to unlock them (authentication), online cloud services use it to organise our online photo galleries on the basis of our friends' faces, and we can even get facial recognition installed into our doorbell to be notified of who is at the door (identification). However, it is not only in the private sphere that FRT has gathered interest; public authorities in several parts of the world have also discovered the great potential that the software holds. The use of facial recognition systems by authorities is often associated with tracking down terrorists, but the software can also come in handy in multiple other domains of interest for police departments. Enforcing bans on access to football matches, protecting significant buildings, (instantly) tracing an offender, increasing border security – to name a few. The use of the software in these contexts are considered to be forms of non-cooperative facial recognition, which holds there is no explicit consent given to be subjected to the technology (van Rest et al. 2021, 7). In the United States, at least 26 states allow for police departments to use the technology for these sorts of applications (Garvie, Bedoya, and Frankle 2016), the South Wales Police has been using the software since 2017 to detect unwanted visitors at large events (South Wales Police n.d.), and since 2016, the Dutch national police have been using a system aptly called CATCH to identify suspects caught on security or bodycam footage (Houwing 2019).

However, even though facial recognition software holds a lot of potential for increasing security, the implementation of the technology has also received a lot of condemnation. Opponents maintain that it is in violation of fundamental rights like the right to privacy, freedom of expression, and the right to equal treatment (Houwing 2019). In the US, major tech companies Amazon, IBM, and Microsoft have already announced to refrain from doing business with police forces until legal protection of these human rights is established (Fung 2020). In this same vein, major cities like San Francisco, Boston and Portland have placed a ban on the implementation of facial recognition by their police departments altogether (Flynn 2020). In Europe, International advocacy group European Digital Rights (EDRi) launched a campaign to urge the European Commission to strictly regulate the use of the technology (Reclaim Your Face 2021). With provisional success: even though it was first ruled that individual European member states were to assess the technology for themselves (Fisher 2020), the draft for the new EU artificial intelligence (AI) act now holds that the use of real-time facial recognition systems by law enforcement in public space would be prohibited under this regulation (Madiega and Mildebrath 2021, 25).

In The Netherlands, the police force is currently only authorised to use software in which the identification process takes place after an event, the aforementioned CATCH system. According to Ferd Grapperhaus, Dutch minister of Justice and Security, a broad-ranging implementation of real-time FRT does not correspond to the country’s national societal values (Grapperhaus 2019). It is quite surprising then, that last year the ministry ordered the Dutch police to examine the legal frameworks and the potential use cases for the technology, leading to experiments with a specific type of real-time facial recognition software in an isolated setting (Krikken 2019, 7). The justification for conducting these experiments – despite the international move toward strict regulation – rests on the fact that the use of real-time FRT has already become normalised in society, which, according to them, will in turn result in pressure from citizens on Dutch authorities to start using the software as well (Krikken 2021, 7; Tijhaar 2021). In anticipation of this, the Dutch police wants to examine whether a more desirable form of the software can be developed.

This justification is particularly interesting. Not only does it offer an alternative to the often given argument that the use of real-time FRT is justified because it increases security, it also contains some specific assumptions about society's relation to (surveillance) technology and its effect on public opinion on government surveillance, which will be explicated below. Due to the technology's contested nature, it is paramount that the justification and underlying assumptions for experimenting with or implementing real-time FRT are valid. That is why, in this thesis, I aim to scrutinise the validity of the justification given by the Dutch national police by looking at the underlying assumptions within this justification. The corresponding research question reads as follows:

Is the normalisation of real-time FRT in society a valid justification for public authorities to experiment with or employ the technology?

In the remainder of this thesis, I will argue that this is not the case because this justification rests on two invalid assumptions. The first being that normalisation of a technology within society emerges independent from existing social structures; it thereby fails to acknowledge that governments are often (partly) responsible for the normalisation of surveillance technologies within society. If normalisation of surveillance technology is regarded as providing grounds for experiments with or the use of the technology by public authorities, it would indicate a dubious situation in which these authorities encourage the private use of surveillance technology (as I will show in section 3.1.) to later use the normalisation of said technology in society as a reason to employ the technology as well. The second assumption holds that public support can be inferred from private choices, which fails to recognise that people often take up a different frame of reference when it comes to decisions regarding society at large instead of their personal lives. Private use of real-time FRT might have become normalised, but this does not prima facie mean that people endorse the use of the technology by public authorities.

The focus of this thesis will limit itself to the situation in The Netherlands as including justifications given by public authorities in other countries would be too broad for the scope of this thesis. However, as the rise of the private use of (real-time) FRT is not bound to country borders, there is reason to suspect that public authorities in other parts of the world are also looking at societal developments in their quest to navigate threats to national security. Therefore, this thesis can be regarded as relevant for the Dutch as well as the international debate on the use of real-time FRT by law enforcement.

Before I delve into my argument, I will provide a more thorough overview of the current academic debate on (real-time) FRT and how this relates to Dutch law enforcement's justification for their experiments. Moreover, I will unfold the lens through which I will approach the topic at hand – the postphenomenological approach – and explain why and how this approach gives substance to my arguments.

In the succeeding chapters, I will argue for the position that the normalisation of the private use of real-time FRT does not provide grounds for experiments with or use of the technology by public authorities. In chapter 3, I will first bring into focus how governments can be seen as responsible for the normalisation of surveillance technologies in society. This is done by introducing the concept of 'lateral surveillance', which can be understood as the practice of monitoring one another (Andrejevic 2004, 481). This concept and corresponding theory allows me to illuminate how governments, and in this case the Dutch government in specific, play an encouraging role in the normalisation of the private use of surveillance technology through what is called 'the offloading of monitoring responsibilities onto citizens' (Andrejevic 2004, 487). I will show that in The Netherlands this is done through active and passive encouragement of the private use of surveillance technologies (which include real-time FRT). Subsequently, with the help of 'mediation theory', I will argue that this encouragement leads to a diminished sense of safety on a national level, as an increase in the private use of surveillance technology on a macro level mediates our perception of safety in that it brings potential risks in society into focus while de-emphasising the chances of falling victim. This has a reinforcing effect on the perceived need for surveillance technology, which normalises the use of these technologies even more. Taken together, these arguments allow me to conclude that *if* Dutch law enforcement is correct in their assumption that the normalisation of the private use of real-time FRT will lead to pressure on them to use it as well, this normalisation should not be regarded as providing grounds for their experiments with or employment of the technology, as the Dutch government was partly responsible for the normalisation of the technology in the first place.

However, my argument does not stop there; I also aim to discredit Dutch law enforcement's justification on another account. In chapter 4, I will argue that this justification is based on the false assumption that public choice can be inferred from private preference. With the help of literature on public environmental policy, I am able to argue that employment of real-time FRT by Dutch authorities would call for a vastly different consideration of ethical implications, values, and perspectives than when an individual uses it for private purposes. Therefore, it cannot be taken as a given that normalisation of the private use of real-time FRT in society will prima facie lead to pressure on Dutch authorities to use it as well.

Moreover, in chapter 5 I will examine whether a possible more nuanced reading of law enforcement's justification for their experiments holds up to scrutiny. A possible way for Dutch authorities to counter my argument is by saying that normalisation of real-time FRT in society *in itself* is not regarded as providing grounds for the experiments, but that future threats to national security, in addition to normalisation of the technology, would lead to societal pressure. By looking at empirical evidence concerning the societal endorsement for government surveillance, I am able to argue that this different reading of their justification is also invalid. This is because threats to national security would justify the exploration of ways to counter these threats, not experiments with real-time FRT in specific. If future threats to national security *do* lead to societal pressure to use real-time FRT, it is only because the Dutch police have presented the technology as being the most effective solution to counter these threats.

Lastly, to end on a more constructive note, I will provide a preliminary proposal for the Dutch police to consider before they continue their experiments with real-time FRT. The justification given for the experiments shows that public opinion has a major influence on Dutch law enforcement's direction. Instead of assuming that the normalisation of the private use of real-time FRT is a valid indicator for public opinion on government use of the technology, it would be more sensible for the Dutch police to engage in the practice of deliberative democracy. This method encourages active deliberation amongst citizens and helps to uncover what would be in the best interest of society as a whole. By doing so, the Dutch police would be able to obtain a more substantial grasp of what the public would actually prefer when it comes to decisions concerning national security, providing grounds for future decisions.

2. Theoretical framework

Before diving straight into the thick of the argumentation central to this thesis, it's important to further explore the theories fundamental to the aforementioned line of reasoning, as well as the academic debate this thesis will add to. I will start by further explaining how and why the

Dutch national police is conducting experiments with real-time FRT and will directly place this within the current debate concerning these technologies. Even though this thesis is focused on the validity of the justification given by the Dutch national police to experiment with the technology and thereby explicitly *not* concerned with the ethical implications of the technology itself, I believe situating their experiments within this debate is indispensable to fully grasp *why* a strong justification is needed on their part. Subsequently, I will provide a more extensive understanding of the theoretical approach within this thesis, namely the postphenomenological approach, and how this adds to my central argument.

2.1. Experiments with real-time FRT and the public/academic debate

2.1.1. 'Digitale Perimeter'

Exactly why and how, then, is the Dutch national police conducting the experiments with real-time FRT? In late 2019, a program called 'Digitale Perimeter' was developed by the municipality of Amsterdam, research institute TNO, football stadium Johan Cruijff ArenA, and the Dutch national police in order to experiment with and develop innovative technologies aimed at increasing local and/or national mobility and security. One of these innovative technologies is real-time FRT: the Dutch national police has joined hands with TNO to investigate how the technology works and how it could be adjusted in order to reduce associated privacy concerns. Their focus within these experiments is on acquiring an understanding of the use cases in which the technology could prove itself useful, under what conditions this could take place, and which measures should be implemented (Krikken 2021, 7). The space within the Johan Cruijff ArenA lends itself as a location in which (adjustments to) the technology can be tested in a controlled and isolated setting.

2.1.2. Benefits of the use of real-time FRT by Dutch authorities

Implementing real-time FRT could have several benefits for the police of The Netherlands, depending on its application. In a recently published policy framework, the World Economic Forum, the international Criminal Police Organisation (INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI), and the Dutch national police, have outlined specific domains in which FRT is or could be beneficial for the Dutch national police and/or INTERPOL.[1] Regarding *real-time* FRT, the authors outline a specific use case in which the technology could prove useful for the police of the Netherlands:

> “**Actively looking for a terrorist in public spaces**
>
> *Note: the following example is a potential use case and has not yet been used by the Netherlands police.*
>
> In the aftermath of a terrorist attack, where the terrorist remains at large, CCTV can be seized by law enforcement to collect a probe image of the fugitive terrorist. This probe image can then be distributed to all police patrols actively looking for the fugitive. In addition, the probe image can be compared in real time against other images of the suspect collected form separate CCTV footage or different image sources located in the terrorist’s assumed vicinity. This real-time comparison may generate a potential lead that can be sent to police patrols, which can conduct a stop-and-check based on this alert” (Louradour and Madzou 2021, 12).

However, terrorism is not the only domain in which real-time FRT could be beneficial for law enforcement. Even though the authors of the aforementioned policy framework only explicitly mention the use of real-time FRT in this specific case, they also describe three applications in which ‘normal’ FRT (not real-time) has already been implemented by Dutch authorities. These are 1) finding the identity of an ATM fraud criminal, 2) uncovering the identity of a rioter, and 3) looking for the identity of a museum thief (Louradour and Madzou 2021, 11-12). It is not hard to see how real-time FRT could, in the future, also be used to enhance security in these domains. Moreover, several other use cases for the technology were conceptualised in the report that was published by TNO for the experiments in the Digitale Perimeter. Commissioned by the Dutch police, TNO describes and explains nine possible uses of FRT and their associated privacy concerns. These described use cases are: 1) object and person protection; 2) immediately tracking a suspect after an incident; 3) tracing ‘most wanted’ or missing individuals; 4) protecting large crowds (so-called ‘soft targets’); 5) enforcement of bans to specific locations; 6) access control at events; 7) border security at international events; 8) ‘green lane’ at events, which means your face is your ticket; 9) monitoring online platforms (van Rest et al 2021, appendix E).

[1] As INTERPOL has a broader and international mandate, the potential use cases and therefore the benefits of using the technology differ (Louradour and Madzou 2021, 7).

2.1.3. Ethical concerns related to the use of real-time FRT by Dutch authorities

Taking only the benefits into account, one would probably find it hard to see why Dutch authorities need a justification for their experiments with real-time FRT at all. Unfortunately, as was already mentioned in the introduction, the use of FRT in general is not free from controversy. In recent years, human rights organisations have warned authorities about the several risks and ethical implications involved in implementing the software, albeit for private, corporate or public ends (Amnesty International 2021; Reclaim Your Face n.d.).

One of the most prominent ethical concerns voiced in the debate surrounding the use of FRT is that of its infringement of privacy. In their extensive report about the potential and limitations of FRT, Introna and Nissenbaum (2010, 44) argue that FRT undermines the right to privacy as it "disrupts the flow of information by connecting facial images with identity, in turn connecting this with whatever other information is held in a system's database". The software does not only allow its user to draw a connection between a face in an image or video and the identity of a specific person – it also enables users to connect this face to other (personal) information of this specific person, if this information is stored in the database. For instance, the software's database usually also contains logs of previous hits of a specific facial template, but also identity documents connected to an individual's template (van Rest et al 2021, 21). Moreover, the footage used to match with the database produces metadata which can also be regarded as personal information; e.g. specific clothing and jewellery, glasses, facial hair, and tattoos (van Rest et al 2021, 21). Specifically looking at real-time FRT, it means that at any given time, the software can instantly produce quite a lot of personal information about an individual in view of the camera. This concern is closely related to worries about security. Even though the software is often implemented in order to increase security, it can also pose a serious threat. This is because our face is "generally assumed to be a non-falsifiable anchor of identity" (Introna and Nissenbaum, 2010, 46). The rapid improvement of the technology paired with the fact that we only have one face makes it next to impossible to evade the software should it fall into the wrong hands. This recently happened in Afghanistan, where a biometric surveillance system containing data on Afghans that assisted the U.S. government was obtained by the Taliban (Klippenstein and Sirota 2021).

In their experiments with real-time FRT, the Dutch police and TNO are trying to mitigate these risks by focusing on a specific form of facial recognition software that lends itself to incorporate privacy preserving strategies, called ‘multi-party computation’ (MPC). How this works for FRT is that the parties involved in the implementation of the software each only have access to one specific domain of the technology. In practice, this means one party has exclusive access to the live camera footage, a second party is authorised to retrieve the encryption key for the database with registered facial templates, and a third party is licenced to decrypt the facial templates originating from the live video footage (van Rest et al. 2021, 38). In order for the comparison between the facial templates to take place, the data does not have to be decrypted and only the final list of identified matches is accessible to all involved parties (van Rest et al. 2021, 38). The benefit of this specific type of FRT is that it reduces some of the risks associated to the software (van Rest et al. 2021, 43-44). For instance, the fact that each domain is encrypted and only accessible to one party reduces the risk of unauthorised use (for example, through hacking). Moreover, it decreases the risk that the data collected for the implementation of real-time FRT is later also used for another application or paired with information in another database.[2]

The aforementioned strategies mitigate privacy concerns in terms of data protection. However, as is also acknowledged in the report published by TNO, these are not the only (privacy related) concerns associated with real-time FRT. The problem is that the other concerns are not as easily mitigated by technical solutions, as they seem to be inherent to the technology itself and/or the implementation of the technology. For instance, Smith and Miller (2021, 5-6) maintain a broader conception of privacy that could be compromised by FRT – also including the right to autonomy. This is undermined when people feel the need to adjust their behaviour or feel restricted in pursuing their plans because they know they might be watched – also known as the ‘chilling effect’. Citizens that know they might be watched, will adjust their behaviour “in such a manner that she does not ‘produce’ long-term accessible information that can backfire on her in the future. This is not only the case for deviant behaviour, but also stretches across other realms like self-expression” (Gorzemann and Korenhof 2017, 83). Citizens could, for instance, become hesitant to protest against a government policy when they know law enforcement might be able to identify them – undermining the freedom of expression, assembly, and association.

[2] These risks are also known as *mission* or *function creep;* when data or a technology are used for a different purpose than they were originally meant for (van Rest et al 2021, 52).

This last concern points to broader concerns surrounding FRT and privacy; the implications do not only pertain to individuals, but also to society as a whole (Smith and Miller 2021, 6; Introna and Nissenbaum 2010, 46). Smith and Miller (2021, 6) point to the power imbalance that arises when large scale violations of privacy and autonomy rights occur between the state and citizens, undermining liberal democracy. Furthermore, Introna and Nissenbaum (2010, 46) call into question "whether taking advantage of a central virtue of FRT, the capacity to identify covertly and at a distance, is acceptable for free societies whose political bedrock includes presumption of innocence and meaningful consent". This concern is especially significant for real-time FRT, as everyone within camera view is automatically subjected to the software – everyone is preliminarily investigated without probable cause (Introna and Nissenbaum 2010, 46).

Another concern associated with FRT is that of fairness. Research shows that marginalised groups disproportionately bear the risks of FRT, as misidentification occurs more often among ethnic minorities and women (Buolamwini and Gebru 2018, 12; Grother, Ngan, and Hanaoka 2019, 2-3). What this can lead to, is that people within these groups are more at risk of being accused of a crime they did not commit. For instance, last year, a black man was wrongfully arrested in front of his wife and children by Detroit police as FRT had produced a false positive by matching security recordings of a shoplifter to his photo (Porter 2020). Unfortunately, this is not something that is easily mitigated by technical adjustments. The algorithms used in facial recognition software are trained on datasets which are bound to contain human prejudice as some biases have become institutionalised within society (Caliskan, Bryson, and Narayanan 2017, 183). This is the general reason why algorithms contain the unfortunate characteristic of mirroring human prejudices, oftentimes even reinforcing them. Moreover, it is not only the software itself that can lead to the unfair distribution of risks – the *use* of FRT also bears the potential to become discriminatory. Research shows that a significantly higher percentage of Dutch citizens with a non-western background in the two largest cities in The Netherlands feel discriminated and/or racially profiled by Dutch police forces (Ferwerda and Kuppens 2019, 37). This could indicate that people that fall into this category are more likely to be arrested for minor crimes than people with a western background. What this would result in, is an overrepresentation of people with a non-western background in the database with facial templates, meaning that these groups are disproportionately more subjected to future surveillance.

2.1.4. The justification for the use of real-time FRT given by the Dutch police

Looking at the ethical concerns associated with (real-time) FRT combined with the fact that the experiments currently conducted by Dutch police will not diminish these concerns, a well-grounded justification for going ahead with the experiments is essential. As the Dutch police contends as well, by making improvements in terms of data protection, the technology becomes more desirable which makes eventual use of the technology by Dutch authorities more likely (Tijhaar 2021). So, as the benefits of using real-time FRT only pertain to increasing security, the Dutch police seems to realise that more is needed in order to justify why they are focusing on real-time FRT in specific. After all, they could also choose to reject the technology altogether based on the inherent associated ethical concerns and shift their attention to explore whether there are other, less contested, security enhancing methods. Instead of doing so, the Dutch police seems to sidestep the 'ethical concerns versus increased security debate' that often ensues when it comes to the implementation of (real-time) FRT, and justifies their experiments with the technology on the grounds that real-time FRT has already found its place in society:

> "Facial recognition technologies are already employed for several uses, also by organisations that do not necessarily have to comply with our laws as they are from other countries. So the technology is already coming at us. You could say: 'I am going to build a fence around my village and it will not happen here.' But that is not tenable. Sooner or later, there will be societal pressure, also on the Dutch police, to use this technology for serious cases. In preparation for that, I believe we should think about an application of facial recognition that fits our democratic constitutional state" (Tijhaar 2021).[3]

In short, the reasoning behind the justification given by the Dutch national police is that real-time FRT is already used by citizens and (international) organisations. For instance, we no longer only use the technology to unlock our phones, we increasingly mount video doorbells to our house that contain the technology as well (Smarthomeweb 2020). Moreover, more and

[3] This quote is translated from Dutch to English. The reason why I included the translation, is because I believe this quote serves as a perfect illustration of the reasoning behind the justification given by the Dutch police. The original quote is as follows: "Die gelaatsvergelijkingstechnologieën worden al in allerlei toepassingen gebruikt, ook door organisaties die zich niet naar onze wet hoeven te voegen omdat ze bijvoorbeeld uit andere landen komen. Dus de technologie komt al op ons af. Dan kun je zeggen: 'Ik zet een hek om mijn dorp heen en het gebeurt hier niet.' Maar dat houd je niet vol. Vroeg of laat komt er een maatschappelijke druk, ook op de politie, om die technologie te gebruiken voor heel serieuze gevallen. Daarop voorbereidend vind ik dat we moeten nadenken over een toepassing van gezichtsherkenning die bij onze democratische rechtsstaat past" (Tijhaar 2021).

more shop owners and football clubs are employing the technology to enforce bans (Houwing 2021). This normalisation of the use of real-time FRT in society, the Dutch police contends, will inevitably lead to societal pressure on them to start using this particular technology as well, for serious cases. In preparation for this, they want to explore a form of real-time FRT that fits our democratic institutional state. As most of the public and academic debate surrounding (real-time) FRT is focused on weighing the ethical concerns associated with the technology against its security gains, this line of reasoning could pose a new perspective. Should normalisation of real-time FRT in society and subsequent expected pressure from citizens be regarded as a valid justification for public authorities to experiment with or implement the technology?

Examining the validity of the justification given by the Dutch police is valuable on two accounts. Firstly, it will add to the academic as well as the public debate concerning whether and when the use of real-time FRT by pubic authorities should be justified. Secondly, this thesis serves as a means to hold Dutch authorities accountable for their ways of conduct. By resorting to the fact that the technology is already widely used in society and cannot be stopped, they seem to regard the debate as settled; people are already losing on values such as privacy, autonomy and fairness anyway, so why should Dutch authorities bother to try to protect those values? This conception allows them to sidestep the debate on whether the ethical concerns or increased security should put more weight on the table, thereby avoiding accountability regarding decisions on these matters.

As I will argue in the remainder of this thesis, I believe the justification should not be regarded as valid. This is because the line of reasoning provided by the Dutch police rests on two hidden assumptions, namely that:

1. normalisation of a technology within society emerges independent from existing social structures;
2. public support can be inferred from private choices;

By drawing on theories concerning lateral surveillance, mediation theory, and the distinction between public and private choice – all to be properly introduced later – I will show why these assumptions are invalid. The first assumption can be deduced from the fact that the Dutch police regards the technology as ‘already coming at us’ and that stopping it is impossible. However, as will become clear in chapter 3, the (private) use of real-time FRT does not just emerge in a vacuum; the assumption fails to acknowledge the influence of existing social structures such as the interplay between governments and citizens on the development, use and normalisation of technological devices within society. The second assumption becomes evident in the reasoning that the private use of real-time FRT will unavoidably lead to public endorsement for government use of the technology. However, as chapter 4 will illuminate, this assumption views the aggregate of the private preferences of individuals as indicative of future public endorsement for the use of real-time FRT by Dutch law enforcement. It thereby fails to acknowledge the distinction between private consumer preferences and public choice about what is in the best interest of society as a whole.

Nevertheless, the Dutch police might still be able to counter these arguments by adding a slight nuance to their justification. It could be that they do not mean normalisation of real-time FRT in society in itself to be the main justifying factor for their experiments, but that possible substantial threats to national security, in addition to the normalisation of the technology, will lead to societal pressure to employ the technology. However, as I will show in chapter 5, this line of reasoning fails to see that threats to national security do not necessarily lead to societal pressure to use real-time FRT, it leads to societal pressure to find ways to counter threats to national security. Real-time FRT is just presented and therefore regarded to be the most effective solution at hand.

2.2. The postphenomenological lens

Even though my arguments will be focused on the aforementioned theories, the broader perspective that serves as a framework for this thesis is situated in the postphenomenological tradition. Within this tradition, technology is approached as affecting and shaping human beings' relation with the real life world (Rosenberger and Verbeek 2015, 11). From this perspective, the subjectivity of human beings and the objectivity of the world are formed through interactions between human beings and technology (Verbeek 2006, 363). This perspective is preferable when it comes to analysing the relation between human beings and technology, as it poses an alternative to the social constructionist view that cultural values and societal tendencies are the main actant in shaping technology, as well as the determinist position that technology determines these cultural values and societal tendencies. The one should not be seen as solely shaping the other; their relationship should be regarded as mutually constituting. As I pointed toward in the previous section, and will explicate further in the remainder of this thesis, the justification given by Dutch law enforcement seems to be situated in the determinist camp. It is maintained that the emergence of real-time FRT in society cannot be stopped and will lead to pressure on the Dutch police to use it as well. This would indicate that the technology in itself alters societal values (less weight on privacy, more weight on security) and will inevitably influence societal tendencies. However, as stated before, an increase in private use of real-time FRT (or other surveillance technologies) does not just occur in a vacuum. By looking at the circumstances through a postphenomenological lens, the mutually constituting relationship between surveillance technology and societal structures such as the interplay between the Dutch government and citizens can be uncovered. This, as the following sections show, will undermine the assumptions underlying Dutch law enforcement's justification.

3. The normalisation of FRT in Dutch society

The interplay between the Dutch government and citizens is an important factor to look into when it comes to the normalisation of the private use of real-time FRT in Dutch society. As I mentioned before, the reasoning behind the justification given by the Dutch police contains the assumption that normalisation of surveillance technology in society emerges independent from existing social structures; they contend that the technology is already here and controlling it is not tenable. This implies that the technology in itself is regarded as a leading factor in how our society takes shape, which, as I mentioned before, is deterministic and fails to acknowledge how societal structures influence technology and its role in society. As Mark Andrejevic argues in his work on lateral surveillance, governments play an important role in the emergence and normalisation of surveillance technologies for private use in society (Andrejevic, 2004, 2006). In sections 3.1. and 3.2. I will explicate Andrejevic' theory and use it to illuminate how the Dutch government actively and passively promotes the private use of surveillance technologies. Furthermore, by applying mediation theory to the case at hand in section 3.3., I am able to argue that surveillance technology has a negative effect on the overall perception of safety within society due to its mediating effect. This would in turn increase the perceived need for even more invasive surveillance technology. Lastly, in section 3.4. I will show how, taken together, these findings undermine the assumption that normalisation of surveillance technology like real-time FRT emerges independent from existing social structures, as it shows that the Dutch government was partly responsible for this normalisation in the first place.

3.1. Lateral surveillance and the offloading of monitoring responsibility

In his article ‘The Work of Watching One Another: Lateral Surveillance, Risk, and Governance”, Andrejevic defines lateral surveillance as the monitoring of one another, as opposed to the top-down monitoring of employees by employers or citizens by the state (Andrejevic 2004, 481). Even though, in a sense, all our interactions with others contain some form of mutual monitoring, the practice of lateral surveillance is distinctive as the domestic use of surveillance technologies allows us to gather information in an asymmetrical, non-transparent manner, similar to state surveillance practices (Andrejevic 2006, 398). That lateral surveillance mimics state surveillance is not surprising, as the surveillance tools used in these private settings were often originally developed for public authorities but over time found their way into the private sphere (Andrejevic 2006, 398). For instance, the first dashboard camera (also known as ‘dash cams’) was used by Texas police in the 1980s – domestic use only became popular internationally after the Russian government allowed its citizens to get them installed in 2009 and footage was widely shared online (Young n.d.). Additionally, and more related to the current case, the foundational research into the FRT we know and use today was funded by the CIA back in the 1960s (Leon 2020). The reason why these surveillance technologies have a way of creeping into our personal lives is because we depend on public authorities to identify, target and communicate certain risks within society, which means they also set the benchmark for how to mitigate these risks in our individual lives. As Andrejevic puts it: “lateral monitoring takes place with an eye to the monitoring gaze of authorities who set the guidelines for subjects responsible for their own security – a responsibility that includes keeping an eye on those around them” (Andrejevic 2006, 396-397). To illustrate this: governments started protecting important buildings with surveillance cameras – it’s not surprising that a lot of citizens are following suit to protect the most important building in *their* lives; their house.

What is more, is that public authorities actually benefit from lateral surveillance as well: if citizens keep each other in check, there is less work to be done for law enforcement. Governments of several western countries have launched campaigns that promote watchfulness among citizens (Chan 2008, 225-226), a phenomenon described by Andrejevic as ‘the offloading of government monitoring responsibilities onto citizens’ (Andrejevic 2004, 487). Most of them pertain to increasing watchfulness with regard to possible terrorist attacks; for instance, the government of the United Kingdom launched a campaign called ‘Action Counters Terrorism (ACT)’, calling citizens to look out for and report suspicious activity

(HM Government n.d.). In the US, the national ‘If You See Something, Say Something’ campaign has been running since 2010 – the government even designated September 25th as the yearly National Awareness Day (Homeland Security n.d.). From this perspective, it can be argued that public authorities play an important role in the normalisation process of lateral surveillance and the private use of surveillance technologies. This process is further amplified by commercial parties playing into this by marketing technologies to the public that were originally developed for law enforcement.

3.2. The Dutch government and lateral surveillance

The aforementioned theory is useful for unveiling how the Dutch government has played a role in the normalisation of the domestic use of real-time FRT in Dutch society. As I will illustrate in the next paragraphs, by indulging in the practice of offloading monitoring responsibilities onto citizens, lateral surveillance – including the use of invasive surveillance technologies like real-time FRT – is actively and passively encouraged by the Dutch government. This undermines the assumption that the arrival of the technology itself should be seen as leading to the normalisation of the private use of these technologies; the Dutch government should be regarded as playing an important role.

3.2.1. Active encouragement of lateral surveillance

Over the last two decades, several examples of the active encouragement of lateral surveillance by the Dutch government can be found. For instance, in a similar vein as the previously given examples, a campaign called ‘Nederland tegen terrorisme’ (The Netherlands against terrorism) was launched back in 2006, which involved TV commercials and the spread of posters and flyers in several municipalities (NU.nl 2006). Today, citizens are still reminded to report suspicious behaviour and packages in public spaces like train stations and festivals (Rijksoverheid n.d.). Moreover, lateral surveillance is also actively promoted with regard to other domains than terrorism. A recent example is the pilot called ‘Digitale Deurbel’ (Digital Doorbell), which was launched in 2019 by the Ministry of Justice and Security, the Dutch national police, several municipalities, and the Centre of Crime Prevention and Security (Hofmans 2019). In this pilot, video doorbells were handed out in specific neighbourhoods of municipalities in order to monitor whether these doorbells would prevent crime and increase a feeling of safety. Interestingly enough, the results were inconclusive: even though the doorbells were not found to have a significant influence on crime figures, the majority of participants did indicate that they felt safer (Hofmans 2019). Despite this, the legal basis for the pilot is questionable. Video doorbells are generally installed next to the front door, which often means the camera will be filming sidewalks or roads. According to the General Data Protection Regulation (GDPR), one is only allowed to film public spaces when it is proportional and unavoidable in terms of safety threats (Autoriteit Persoonsgegevens n.d.). Whether a pilot project in a neighbourhood should be regarded as proportional and unavoidable is contentious at best – even more so when you take into account that several types of video doorbells contain the option to include real-time FRT (Smarthomeweb 2020).

Nevertheless, the distributed video doorbells were automatically added to 'Camera in Beeld' (Camera in View), a system utilised by the Dutch police in which citizens can register their private cameras so local police can request footage if needed (Politie n.d.). From a legal perspective, this is basically a database of private cameras unlawfully filming public spaces. In early 2020, Camera in Beeld was filled with 230.000 cameras, of which 87,6% filmed public roads (Houwing 2020). The Dutch police needs specific authorisation from the mayor to add cameras to public space within a municipality (Houwing 2020) – by offloading the monitoring responsibilities onto citizens, Dutch law enforcement is able to sidestep this regulation while still obtaining the benefit of having access to camera footage when it's deemed useful. The previous examples show that the Dutch government actively promotes the use of surveillance technology, among which real-time FRT, and inexplicitly even normalises unlawful use of these technologies.

3.2.2. Passive encouragement of lateral surveillance

The fact that the police is encouraging citizens to register their unlawfully placed private cameras in the Camera in Beeld database and that the violation of the GDPR does not lead to repercussions can also be regarded as examples of how lateral surveillance is *passively* fostered by the Dutch government. For several years now, the Dutch privacy watchdog Autoriteit Persoonsgegevens has voiced its discontent about not being able to enforce the GDPR due to being structurally underfunded by the government (Autoriteit Persoonsgegevens 2021). As a result of this, illegitimate use of domestic surveillance technologies is rising, while the majority of citizens is unaware of being in violation of privacy laws as the government seems to be actively promoting it for their own benefit. Moreover, this passive form of offloading monitoring responsibilities does not only pertain to citizens – it extends to commercial organisations as well. When it comes to the use of (real-time) FRT, organisations are legally only permitted to employ the software if they have obtained explicit informed consent from those subjected to it, or when it serves a weighty societal interest (Autoriteit Persoonsgegevens 2020). Nevertheless, in recent years, there have been numerous instances of stores, casinos, football stadiums, festival organisations, and businesses using the technology without any legal consequences (Houwing 2021). An example of this, is FC Den Bosch; the football club has installed 24 cameras in order to identify unwelcome visitors. Their justification for the use of real-time FRT is reminiscent of the justification given by the Dutch police: others do it too (van Dijck 2019). However, the reason why others 'are doing it too', is because the GDPR is not sufficiently enforced and the use of these technologies is actively promoted by the government.

Dutch law enforcement's assumption that once a technology is 'there', it cannot be stopped, can therefore be undermined. As the previous paragraphs have illustrated, Dutch authorities have the means to cease the normalisation of real-time FRT in society through enforcement of the GDPR. However, not only did they refrain from doing so, they also actively encouraged the private use of real-time FRT by promoting lateral surveillance. This shows that the emergence and normalisation of a technology like real-time FRT in society does not occur independent from social influences, thereby disproving the deterministic view underpinning Dutch law enforcement's justification.

3.3. Mediation theory

However, even though I have shown that the technology in itself should not be regarded as leading to normalisation of its use, it would be a mistake to not ascribe any influence on society to technology. As the following sections will confirm, the relationship between (surveillance) technology on one hand, and social structures such as the interplay between a government and citizens on the other should be regarded as mutually constituting. By bringing this relationship to the forefront, the possible danger of Dutch law enforcement's invalid reasoning can be unveiled. Setting the benchmark for and encouraging the private use of surveillance technologies, either actively or passively, can be argued to have an even more profound impact on the normalisation of these technologies within society when the mediating effect of the technology itself is taken into account. At the end of the line, this could lead to a self-reinforcing loop in which more and more invasive surveillance technologies become normalised in society. Following Dutch law enforcement's reasoning, this would subsequently lead to more and more endorsement for invasive government surveillance.

A specific theoretical approach developed to illuminate the mediating effect of technology, is philosopher Peter-Paul Verbeek's mediation theory, situated within the postphenomenological tradition. In his article 'Materializing Morality: Design Ethics and Technological Mediation', Verbeek distinguishes two ways in which human subjectivity is mediated through interaction with technology: through 'mediation of perception' and through 'mediation of action'. Mediation of perception is aimed at analysing how technology co-shapes how a human being perceives the world (Verbeek 2006, 366). In order to unveil how this transpires, Verbeek builds on philosopher Don Ihde's theory (1990) that technologies alter our perception by way of amplification and reduction. When interacting with technology, certain aspects of reality are amplified, while others are reduced (Verbeek 2006, 365). This happens on both a micro and a macro level. For instance, when you look at blood through a microscope, certain aspects of the substance – like its colour and density – get lost, while other details – like the blood cells – become amplified. This change in micro perception has in turn fundamentally altered our macro perception: we now believe our blood is better to be assessed on the basis of the quality of our blood cells than just its colour and density. This change in macro perception can also be regarded as a form of mediation of action. In his explanation of mediation of action, Verbeek draws from the work of sociologists Bruno Latour and Madeleine Akrich: objects influence human action because they contain a certain 'script' (Verbeek 2006, 366). This script prescribes how we are to interact with the object, as it invites and inhibits specific behaviour (Verbeek 2006, 367). The microscope, to return to the previous example, invites a person to look through the lens and focus on the details of the blood, whereas it inhibits this person to just observe the blood as it is. By doing so, it mediates our actions.

3.3.1. Lateral surveillance and the mediation of perception

Even though both mediation of perception and mediation of action are present when it comes to surveillance technology, I will mainly develop my argument with the use of its mediation of perception. This is because mediation of action mostly pertains to individual actions, while the alterations on a larger scale hold the most relevancy for the argument I am trying to make.

In order to illustrate how mediation theory comes into effect in surveillance technology, let us return to the video doorbells that were handed out by the Dutch government. As I mentioned before, the results of the pilot showed no significant influence on crime figures. However, people did *perceive* the doorbells to have an influence, as participants indicated that they felt safer. This is because, on a micro level, it brings other people's behaviour within proximity of the camera into focus, while reducing what actually takes place outside the camera's view. The chances of falling victim to a residential burglary in The Netherlands are generally quite low, so it is safe to assume that in the majority of cases other people's behaviour within the field of vision is favourable. However, due to the technology's mediation of perception, people are now more likely to attribute this favourable behaviour to the presence of the camera, instead of the trustworthiness of others or the fact that the number of residential burglaries in The Netherlands has been consistently dropping for years (CBS 2021). Alternatively, if something unpleasant does happen, chances are that people will resort to adding more surveillance technology to their house (mediation of action) – after all, it is what makes them feel safer. In both cases, the addition of a video doorbell to their house is likely to mediate people's perception in that it strengthens the view that camera surveillance is needed.

Nevertheless, the previous example only pertains to mediation of perception on a micro level; people feel that their house is safer. On a macro level, an increasing amount of (lateral) surveillance can actually be argued to reduce people's sense of safety. For instance, when the majority of residents in an area have a video doorbell installed to their house, it is likely to give off a signal that cameras are needed in that neighbourhood because it is unsafe. This is because the presence of surveillance technology reminds us of possible risks through amplification, while leaving the probability of these risks becoming reality out of the picture. This does not just stop at video doorbells; it pertains to all sorts of (lateral) surveillance strategies. When an increasing amount of football clubs or festival organisations use real-time FRT at the entrance, it might make us feel safe at a particular event, but on a macro level it serves as a continuous reminder of the threat of a dangerous individual gaining access, while the probability of this actually happening is left out of focus. This altered perception of risks in society is reinforced by disproportional media coverage of crimes: the mundane fact that most of the time nothing happens does not make it to the eight o'clock news.

What is problematic about this mediation of perception on a macro level, is that it contributes to what is called the 'reassurance gap' (Millie and Herrington 2005, 41). This gap points to the discrepancy between a population's general feeling of safety and the country's actual crime rates – people tend to perceive crime figures to be higher than they really are, leading to a need for more safety measures in order to feel safe and reassured. This could lead to a downward spiral; the skewed perception of safety reinforces the perception that more surveillance technology is needed, but the addition of surveillance technology actually decreases the overall sense of safety even more. The offloading of monitoring responsibilities onto citizens and organisations by a government can therefore be argued to reinforce this. By encouraging lateral surveillance, they highlight the possibility of falling victim to crime, while underemphasising the actual chances of it happening. As Chan argues in her article “The New Lateral Surveillance and a Culture of Suspicion”, this government induced focus on what *could* happen, leads to a state of preparedness among citizens (Chan 2008, 228). We are to imagine the worst and prepare for it. As a result, she argues, endorsement for the use of more invasive surveillance technologies – by ourselves, organisations, or the government – increases, which further normalises and increases its use.

3.4. The normalisation of real-time FRT and Dutch authorities

So far, I have argued that Dutch authorities have played an active part in fostering the normalisation of the private use of real-time FRT, and that the mediating effect of the technology itself further accelerates and reinforces this process. When linked to the justification given by the Dutch police, this has allowed me to show how one of the assumptions underlying their line of reasoning can be undermined. Namely that:

1. normalisation of a technology within society emerges independent from existing social structures;

The Dutch police contends that real-time FRT is coming at us and cannot be stopped, but as became clear, this view is determinist in nature and fails to acknowledge how existing social structures play a part in the normalisation of the use of a technology in society. By approaching this assumption from the postphenomenological position, I have been able to illuminate how the Dutch government has contributed to the normalisation process of real-time FRT by actively and passively encouraging lateral surveillance. Citizens are constantly reminded to be vigilant for possible security threats, video doorbells were handed out in several neighbourhoods, and violation of the GDPR through unlawful placement of surveillance technologies like real-time FRT does not only stay without consequences but is actually used to Dutch law enforcement’s benefit. These examples serve to illustrate that real-time FRT is in fact not coming at us out of nowhere and unstoppable; its emergence and spread in society are partly the result of policy decisions made by the Dutch government. In turn, the mediating effect of surveillance technology reinforces this spread, as the technology alters our perception of safety on a macro level.

However, this perspective does not only undermine the assumption underlying the justification given by the Dutch police, it also points to a possibly precarious interplay between citizens and Dutch authorities regarding surveillance technology. Dutch authorities contribute to the normalisation of the private use of a controversial surveillance tool, and this normalisation later serves as justification for Dutch authorities to use it as well. Failing to acknowledge this is problematic, as it could lead into a reinforcing loop. As I have illustrated, governments play a leading role in communicating risks to society; not only by promoting lateral surveillance, but also by adopting more invasive surveillance technologies themselves. Both practices influence people's perspective on the need for private surveillance technology, further normalising its use. When public authorities keep promoting lateral surveillance and use the ensuing normalisation as a justification for an increase in government surveillance, the cycle would start again – resulting in the normalisation of more and more invasive government and private surveillance.

4. Normalisation of real-time FRT: a private or public choice?

Nevertheless, an important question still remains unanswered: is it really that self-evident that normalisation of private use of real-time FRT in society will lead to pressure on the Dutch police to employ the technology as well? In their justification for the experiments, Dutch law enforcement seems to assume that public support for the use of real-time FRT by Dutch authorities can be inferred from the fact that Dutch citizens use it as well. As I will show in the following section, this is not the case. What an individual does in their private lives might actually not be the most accurate indicator for how they prefer their government to act. The assumption fails to acknowledge the distinction between private and public choice – it merely takes an aggregate of the private preferences of individuals into account.

4.1. Private versus public choice

This distinction between private and public choice has been very well explicated in literature on public environmental policy. In his article 'Environmental valuation, deliberative democracy and public decision-making institutions', economist and political theorist Michael Jacobs invokes this distinction to argue that alternative decision-aiding conventions are needed when it comes to environmental policy-making (Jacobs 1997, 211). All too often, he argues, environmental policy-decisions are made based on the aggregate of private preference-based choices (Jacobs 1997, 215). However, by only taking private preferences into account, one fails to see that individuals often take up a different frame of reference when it comes to decisions regarding public goods. Choices regarding public goods are different from private choices because public goods differ from private goods in three respects: 1) they may have negative externalities (e.g. hurt other people); 2) are the object of ethical concern (invoke debate about right and wrong); and 3) are part of what we consider to be ‘the common good’, holding societal value beyond the value it brings to individuals (Jacobs 1997, 214). When it comes to choices about public goods, the majority of people will not only take their own personal interests into account, but will also consider other people’s perspectives, relevant ethical considerations and values, and what is in the best interest of society as a whole (Jacobs 1997, 214). To illustrate how this materialises in practice, Jacobs provides an example of a rare wetland habitat (1997, 214). Even though building a road through this wetland might reduce his travel time by twenty minutes, other considerations can just as well outweigh his private interest. For instance, the proposed route might lead to the demolition of houses which causes harm to the people living there (externality argument), or he might view biodiversity as having intrinsic value and therefore building a road through the wetland would be wrong in itself (ethical consideration), or he could believe it to be bad for our society if we give up on rare habitats (common good argument) (Jacobs 1997, 214). So even though the road brings personal value to him and the rare wetland habitat does not, he might just as well place more value on this wetland because of these other considerations.

Philosopher Mark Sagoff makes a similar claim in his book *The Economy of the Earth: Philosophy, Law, and the Environment* (2008, 51); he argues that expressions of what an individual prefers for themselves are often confused with beliefs about the choices we should make for the community. This distinction between how a person acts with regard to their personal preference and what they would choose in respect of society as a whole is what he describes as the distinction between an individual as ‘consumer’ and ‘citizen’ (Sagoff 2008, 47-49). For instance, someone who buys and smokes cigarettes regularly might still vote in favour of placing a ban on smoking in public spaces. Or more personally, I still use apps that have suboptimal privacy policies; yet, I vote for political parties that promise strict privacy regulations and enforcement. This shows that the choices people make in their consumer behaviour can differ significantly – and even conflict with – choices they would make regarding society at large. Moreover, it illustrates that companies playing into this consumer behaviour by selling certain goods cannot be regarded as reflective of public choices either; they unsurprisingly only reflect an aggregate of consumer choices.

Both of the aforementioned theories illustrate that there are things in life that we value regardless of whether it brings value to us personally. It is therefore paramount that public authorities acknowledge this as well when making decisions. When only the aggregate of private/consumer choices is taken into account, the things we value besides or despite our personal preferences might end up getting lost in the decision-making process because the appropriate considerations and the question of whether we, as citizens, regard something to be right or wrong for society as a whole are left out of the equation.

4.2. Public choice and real-time FRT

The same point can be made for decisions regarding whether or not the Dutch police should experiment with and eventually use real-time FRT. As I have stated before, their justification is based on the fact that the technology is already normalised in society; people have made the private choice to buy the technology and use it in their personal lives. Dutch authorities therefore seem to infer this private choice means that people place more weight on security than the values undermined by the implementation of the technology (privacy, fairness, and autonomy).

However, as we have seen in the previous section, this private choice does not necessarily correlate with decisions concerning public goods. People might regard security to be of greater importance than these other values when it comes to their personal lives, but that does not prima facie mean they would do the same when it affects society as a whole. To illustrate this, consider the following case. When I consider to install a video doorbell with real-time FRT to my house, I expect it to increase my private security, which would be in my private interest. As the effect of my individual video doorbell on society at large will presumably be insignificant, I will only take the benefits of the technology for me personally into account. Now, an increase in national security through the use of real-time FRT by the Dutch police would also be in my private interest; it is expected to increase my private security as well. However, in this situation, the use of the technology *will* have an impact beyond my personal life. Therefore, I will most likely also consider other people's perspectives, relevant ethical considerations and values, and what is in the best interest of society as a whole. In this case, I might conclude that these other considerations outweigh my private interest of enjoying increased security. Remember the ethical concerns set out in section 2.1.3.? The fact that marginalised groups will be targeted disproportionately could be a dealbreaker to me (externality argument); or I could view privacy, fairness, and/or autonomy as having intrinsic value and would therefore believe the use of real-time FRT by the Dutch police to be wrong in itself as it undermines these values (ethical argument); lastly, I could be of the opinion that it would be bad for our society if the Dutch police starts to employ a technology that creates a power imbalance between state an citizens, compromising liberal democracy (common good argument). Regardless of whether I end up being in favour or against the use of real-time FRT by the Dutch police, this shows that it is not self-evident that the choices I have made in my private life correspond with what I would choose when it pertains society at large.

Therefore, it cannot be taken as a given that the private use of real-time FRT will eventually lead to societal pressure on the Dutch police to use it as well. When it concerns use of the technology on a larger scale, people will most likely make different considerations than they would if it only concerned their private interest. This shows that the second assumption underlying Dutch law enforcement's line of reasoning is invalid. Namely that:

2. Public support can be inferred from private choices

The fact that Dutch authorities fail to acknowledge this and take it as a given that private use of real-time FRT will lead to societal pressure on them to employ the technology as well can be regarded as yet another expression of their determinist view on society's relation to technology. They seem to assume that the private use of the technology will prima facie alter our societal values to such an extent that public values such as autonomy, privacy, and fairness, and fundamental rights such as the freedom of expression, assembly, and association become regarded as less weighty than security. This assumption allows them to sidestep the 'ethical concerns versus increased security debate' associated with the implementation of (real-time) FRT by public authorities. The Dutch police regards the debate as already being settled; people are using it in their private lives, so they must place more value on security. However, as the previous paragraphs show, the debate re-emerges when people start to consider whether the implementation of real-time FRT on a national scale would be desirable. This shows that sidestepping this debate by pointing to normalisation of real-time FRT in society is fallacious; if the Dutch police wants to provide a valid justification for their experiments with real-time FRT, they will need to address this debate first (see chapter 6 for a possible way forward).

5. Real-time FRT and substantial threats to national security

In the previous chapters, I have shown that the Dutch government was partly responsible for the normalisation of real-time FRT in society and that this normalisation will not prima facie lead to societal pressure on Dutch authorities to start using the technology as well. This would lead to the conclusion that the justification given by the Dutch police for their experiments with real-time FRT is invalid. Nevertheless, the Dutch police could try to counter this conclusion by adding a slight nuance to their justification. Maybe normalisation of real-time FRT in society in itself is not regarded as the main justifying factor for their experiments. It could very well be that possible substantial threats to national security, in addition to the normalisation of the technology, will lead to alterations in societal values, resulting in societal pressure on Dutch law enforcement to employ the technology. Would this mean the justification given by the Dutch police still holds, despite the two errors in their reasoning as illuminated in the previous chapters? After all, conducting experiments in preparation for expected societal pressure might lead to the implementation of a more favourable form of real-time FRT, should worse come to worst.

In the following paragraphs, I will argue why on this account the justification given by the Dutch police still does not hold. The prospect of an increase in threats to national security does not justify experiments with real-time FRT, it justifies the examination of ways to combat possible future terrorist attacks. Real-time FRT is just presented and therefore regarded as the most effective solution, even though this is not necessarily the case.

5.1. Support for state surveillance

An empirical study examining public support for state surveillance in four European countries shows that in all four countries the pertinence of terrorist attacks is a strong indicator for higher levels of support for surveillance (Ziller and Helbling 2021, 999). It seems safe to assume that this will not be any different in The Netherlands. According to a terrorist threat assessment conducted by the NCTV, the national coordinator for counterterrorism and security, the current threat level of terrorism in The Netherlands is significant (NCTV 2021). This means that the chance of a terrorist attack happening in the near future is conceivable, due to jihadist, Salafist, and extremist right-wing movements, and social unrest resulting from the COVID-19 pandemic (NCTV 2021). Taken together, it seems reasonable that the Dutch police expects societal pressure to employ real-time FRT. As I have illustrated in section 2.1.2., one of the main benefits of the technology is that it proves effective in identifying and tracking (possible) terrorists.

5.1.1. Support for real-time FRT

However, it is important to emphasise that an increase of terrorist threats does not necessarily lead to higher levels of support for real-time FRT *in specific*, it leads to higher levels of support for state surveillance. A salient detail in the previously mentioned study is that public support for state surveillance is higher when the measures are targeted at criminals only, instead of subjecting all citizens to the surveillance (Ziller and Helbling 2021, 1003). As this is inherently impossible when it comes to the use of real-time FRT, it can be inferred that citizens would actually prefer other less intrusive measures to be explored or taken if possible. An increase in the threat of terrorism therefore does not necessarily lead to societal pressure to use real-time FRT, it leads to societal pressure to find ways to combat possible future terrorist threats. Nevertheless, by focusing on experiments with real-time FRT instead of investing time and resources in exploring other (possibly less intrusive) options, real-time FRT is presented as being the most effective solution at hand. By doing so, the expected pressure on Dutch authorities to employ real-time FRT might become a self-fulfilling prophecy; not only will the technology be regarded as one of the few available options to counter terrorism, the adjustments made to the software during the experiments also make the technology look more appealing to the public.

From this perspective, it can be argued that even with the added nuance, the justification given by the Dutch police does not hold. The reason why substantial threats to national security would lead to societal pressure on the Dutch police to employ real-time FRT is because the police themselves have created a focus on this particular solution, thereby presenting it as the most viable solution. This should not come as a surprise, as it coincides with Andrejevic's theory on lateral surveillance, introduced in chapter 3 of this thesis: we depend on public authorities to identify and communicate risks in society, and how to mitigate these risks. In this sense, the experiments with real-time FRT in itself could lead to societal pressure to employ the technology; by creating a focus on this particular solution, other possible options to counter threats to national security are left out of focus and stay underexplored.

5.2. Technological solutionism

What is more, is that the way in which real-time FRT is treated can actually be regarded as an example of technological solutionism. This notion was first coined by technology critic Evgeny Morozov in his book *To Save Everything, Click Here* (2008, 5) and refers to the way in which new technologies have led human beings to adopt new strategies of problem-solving. All too often, the fact that a technological solution is available leads us to resort to this solution without properly considering alternative options. What is problematic about this according to Morozov, is that using technological developments to address complex societal issues frequently recasts these issues as "neatly defined problems with definite, computable solutions or as transparent and self-evident processes that can be easily optimized" (Morozov 2013, 5). The result of this, is that these technological solutions often only treat the symptoms of these complex issues, instead of addressing the issues themselves. As an example, Morozov points to the way in which self-tracking apps are marketed as solutions to reduce health problems, but at the same time fail to address underlying causes for a decline in national health (Tucker 2013).

Looking at the experiments conducted by the Dutch police, a similar case can be made. By resorting to real-time FRT in their experiments to enhance national security, Dutch authorities do not sufficiently acknowledge and communicate the complex societal issues underlying the increase in terrorist threats and how to deal with these. The result of this is that possibly more effective, non-technological, alternatives are left underemphasised and stay unrecognised within society. For instance, research shows that enhancing social welfare of citizens by improving social security, reducing unemployment rates, and providing better healthcare and education reduces the risk of terrorist attacks happening in that country (Burgoon 2006, 177).
If Dutch authorities would place more emphasis on these non-technological alternatives to counter terrorist threats, societal pressure on the Dutch police to use real-time FRT might become less likely to materialise.

6. Possible way forward

In the previous chapters, we have seen that the justification given by the Dutch police for their experiments with real-time FRT does not hold on several accounts. However, after deconstructing this justification, it is time to become a bit more constructive. Could there be a way in which these experiments with the technology would be justified? The answer is: yes, under the condition that the right questions are answered *before* the experiments are conducted (or in this case: continued). In their justification, the Dutch police assumes that societal pressure to start using the technology is inevitable and starts with the question how we can shape an application of facial recognition that fits our democratic constitutional state. Now that we know that societal pressure is, in fact, not inevitable, a different question can form the starting point: do and (more importantly) should we, as a society, want public authorities to use real-time FRT at all?

Finding a decisive answer to this question is not an easy task and the proposal provided in the following sections is by no means meant to provide a definite solution; doing so would be outside the scope of this thesis. However, I do aim to point in the direction of a possible way forward for the Dutch police. This way forward takes shape in the form of engaging in macro deliberative democracy, further explicated below. By following this route, Dutch authorities could enable themselves to acquire a more well-informed understanding of what we, as citizens, believe to be in the best interest of society when it comes to enhancing national security.

6.1. Deliberative democracy

Despite the fact that the Dutch police in their justification wrongly assumes that public choice can be inferred from the aggregate of private preferences, this line of reasoning does indicate that public opinion is a leading factor in steering Dutch law enforcement's direction. After all, it was the expected societal pressure that instigated the experiments with real-time FRT. To get a more substantial grasp of what the public would actually choose when it comes to issues concerning society at large, deliberative democracy could pose a helping hand. This theory holds that active deliberation amongst citizens is a necessary precondition in order to uncover what should be done in the best interest of society as a whole (Jacobs 1997, 221). This deliberation often takes place in a forum setting, such as a citizen assembly or parliament, where citizens meet to exchange and debate views on a particular societal topic (Mendonça, Ercan, and Asenbaum 2020, 2). One of the benefits of this method as opposed to procedures like voting or sending out a survey is that it is a public instead of a private endeavour. Not only does it require engagement with other people and their interests and values, it also demands an individual to test and substantiate their own views and beliefs (Jacobs 1997, 219). The result of this is that "people's positions can alter, as new arguments are heard and perspectives appreciated" (Jacobs 1997, 221), bringing people's views closer together.

Reaching complete consensus is not required, and rather impossible in diversified societies; however, it does lead to more considerate decisions (albeit compromises) on what would be in the best interest of society at large (Jacobs 1997, 221).

Now, it should be mentioned that the Dutch police have (to some extent) already tried to encourage active deliberation on the use of real-time FRT. Within the Digitale Perimeter program that the experiments with real-time FRT form a part of, the public research university of Amsterdam (VU Amsterdam) and research communication institute NEMO Kennislink have organised several sessions to enable citizens to voice their opinions on how technologies should be integrated in society (Krikken 2021, 10). However, these sessions were merely targeted at residents of Amsterdam and the majority of participants consisted of direct stakeholders like representatives of local organisations and civil servants (Krikken 2021, 11). As the use of real-time FRT by public authorities concerns society at large, these sessions can hardly be argued to result in a representative and well-informed understanding of the public opinion on this matter.

6.1.1. Macro deliberative democracy

A more fruitful alternative for the Dutch police would be to engage in the deliberative process on a macro level; also taking the debate transpiring in the broader public sphere into account. This means that weight is not only given to the outcomes of the deliberation of small-group assemblies (micro deliberation), but also to the debate ensuing among, for example, activists, civil society organisations, and the media (Mendonça, Ercan, and Asenbaum 2020, 2). One of the shortcomings of micro deliberative democracy is that the prevalence of existing power structures within this method are insufficiently acknowledged (Sanders 1997, 370). This means that within citizen assemblies or parliaments, social standing still influences whose voices are given more weight, which could result in the reinforcement of dominant views. By engaging with the deliberation process on a macro level, the Dutch police would not only be able to incorporate a fuller range of perspectives, it also allows them to duly include the voices of marginalised groups. As was shown in section 2.1.3., one of the ethical concerns associated with the use of real-time FRT by public authorities is that these groups are unfairly subjected to and affected by the technology. It is therefore paramount that the experiences and perspectives of these groups are given proportional weight.

So, macro deliberative democracy can be helpful for Dutch authorities to acquire an understanding of the public opinion on whether or not the utilisation of real-time FRT is desirable. This as opposed to the assumption that public support can be inferred from private preferences. However, as I have shown in the preceding chapters, Dutch authorities also run into other issues when it comes to taking public opinion as a guiding factor regarding whether or not to use real-time FRT. The first problem concerns the fact that Dutch authorities have encouraged normalisation and support for the technology. It can be argued that the encouraged support will also trickle through into the deliberative process. When people are being primed to respond to security risks by resorting to an increase in surveillance, it is likely that these convictions will resonate in the debate on real-time FRT as well. However, as we have seen, the majority of the encouragement was based on the amplification of the risk of falling victim to crime, while the actual chances of falling victim were de-emphasised. The deliberative process can counter this imbalance by bringing factual crime figures back into focus, which could lead to a more well-informed and reasoned debate on whether the use of real-time FRT by Dutch authorities is proportional. A similar case can be made for the issue that public support for real-time FRT is influenced by the fact that the technology is presented as the most effective solution. The deliberative process creates room for the deliberation of alternative (non-technological) ways to counter threats to national security and thereby alleviates the risk of forming a tunnel vision on real-time FRT.

7. **Conclusion**

In this thesis, I have argued that normalisation of real-time FRT in society is not a valid justification for public authorities to experiment with or employ the technology. By deconstructing the justification given by the Dutch police from a post-phenomenological perspective, I have been able to show that this justification rests on two invalid assumptions, namely that 1) normalisation of a technology within society emerges independent from existing social structures, and 2) that public support can be inferred from private choices.

With regard to the first assumption, I have illuminated how governments bear a responsibility when it comes to normalisation of surveillance technologies in society. I have done so by drawing from literature on lateral surveillance which has allowed me to uncover how public authorities encourage the private use of surveillance technologies, resulting in normalisation of this practice. Dutch authorities do so through active and passive encouragement; they actively promote the private use of surveillance tools (including real-time FRT) by encouraging watchfulness among citizens and handing out video doorbells. Passive encouragement of the private use of surveillance technologies is done by not providing enough financial resources to the Dutch privacy watchdog to enforce the GDPR. Moreover, I have argued that this encouragement leads to a diminished sense of safety by introducing mediation theory. Our perception of safety is mediated by surveillance technology as it places an emphasis on security risks in society, while it leaves the actual chances of falling victim out of focus. This further normalises the private use of surveillance technologies, as it has a reinforcing effect on the perceived need for surveillance technology. Taken together, I have been able to conclude that on this account, normalisation of real-time FRT in society does not provide grounds for experiments with or use of real-time FRT by Dutch authorities, as they were originally responsible for this normalisation. Furthermore, it illuminates a illuminates a questionable situation in which authorities encourage normalisation of surveillance technologies among citizens and later use this normalisation as a justification to scale up state surveillance.

The second assumption, that public choice can be inferred from private preference, is shown to be fallacious by drawing from literature on public environmental policy. This has allowed me to illuminate that the choices we make in our personal lives often do not correspond with the choices we make regarding society at large. The use of real-time FRT by public authorities would affect society as a whole, which means we are likely to take up a different frame of reference and consider other ethical implications, values, and perspectives than when it would only concern our own interest. Taking it as a given that the private use of real-time FRT will lead to societal pressure on authorities to use it as well therefore fails to acknowledge that there are things in life we value besides or despite our personal preferences. On this account, I have shown that normalisation of real-time FRT in society can yet again not be regarded as a valid justification for experiments with real-time FRT by public authorities as it will not prima facie lead to the expected public pressure on Dutch authorities to use it as well.

In order to provide a comprehensive dissection of whether normalisation of real-time FRT in society provides grounds for experiments with or use of the technology, I have also considered whether a slight nuance in the justification holds up to scrutiny. This nuance maintained that Dutch authorities might not regard normalisation of real-time FRT in itself as providing grounds, but that possible threats to national security in addition to this normalisation should be regarded as the main justifying factor. With the help of empirical evidence concerning the societal endorsement for government surveillance, I have been able to argue that threats to national security would only justify the exploration of ways to counter these threats, not experiments with real-time FRT in specific. The expected societal pressure to use real-time FRT would only materialise because Dutch authorities have presented the technology as being the most effective option to combat security threats. Therefore, I can conclude that even with the added nuance the justification would still be invalid.

Taken together, these claims have allowed me to conclude that normalisation of real-time FRT in society is not a valid justification for experiments with or use of the technology by public authorities. By doing so, I hope to have made a valuable contribution to the public as well as the academic debate on whether and when the use of real-time FRT by authorities is justified. Moreover, by suggesting macro deliberative democracy as a possible way forward, I have tried to aid the Dutch police in obtaining a more well-informed understanding of society's view on the use of real-time FRT by police forces. However, more research is necessary to further develop this preliminary proposal.

8. References

Amnesty International. 2021. “Ban dangerous facial recognition technology that amplifies racist policing.” January 26, 2021. https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist policing/.

Autoriteit Persoonsgegevens. 2020. “AP: Pas op met camera’s met gezichtsherkenning.” October 29, 2020. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-pas-op-met-camera%E2%80%99s-met-gezichtsherkenning.

Autoriteit Persoonsgegevens. 2021. “Miljoenennota: geen verhoging budget AP.” September 21, 2021. https://autoriteitpersoonsgegevens.nl/nl/nieuws/miljoenennota-geen-verhoging-budget-ap.

Autoriteit Persoonsgegevens. N.d. “Camera’s bij huis en bij de buren.” Accessed November 17, 2020. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameras bij-huis-en-bij-de-buren#mag-ik-een-camera-ophangen-bij-mijn-huis-6124.

Burgoon, Brian. 2006. “On welfare and terror: Social welfare policies and political-economic roots of terrorism.” *Journal of Conflict Resolution* 50, no. 2 (April): 176-203. https://doi.org/10.1177/0022002705284829.

Caliskan, Aylin, Joanna J. Bryson, and Arvind Narayanan. 2017. “Semantics derived automatically From language corpora contain human-like biases.” *Science* 356 no. 6334 (April): 183-186. https://doi.org/10.1126/science.aal4230.

CBS. 2021. “Veiligheid.” 20 oktober, 2021. https://www.cbs.nl/nl-nl/visualisaties/welvaart-in-coronatijd/veiligheid.

Ferwerda, Henk, and Jos Kuppens. 2019. “Professioneel politieoptreden: in gesprek met burgers.” *Tijdschrift voor de Politie* 6/7. https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/96415.pdf.

Fisher, Christine. 2020. “EU backs away from proposed five-year facial recognition ban.” *Engadget,* November 2, 2020. https://www.engadget.com/2020-02-11-european-commission-facial-recognition-guidelines.html?guccounter=1.

Flynn. Shannon. 2020. “13 Cities were police are banned from using facial recognition tech.” *Innovation & Tech Today,* November 18, 2020. https://innotehtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/.

Fung, Brian. 2020. “Microsoft says it won’t sell facial recognition technology to US police departments.” *CNN Business,* June 11, 2020. https://edition.cnn.com/2020/06/11/tech/microsoft-facial-recognition-police/index.html.

Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. 2016. “Unregulated police face recognition in America.” *Georgetown Law, Center on Privacy & Technology,* October 2016. https://www.perpetuallineup.org/.

Gorzeman, Ludo, and Paulan Korenhof. 2017. "Escaping the panopticon over time." *Philosophy & Technology* 30, no. 1 (October): 73-92. https://doi.org/10.1007/s13347-016-0238-y.

Grapperhaus, F. B. J. 2019. "Waarborgen en kaders bij gebruik gezichtsherkenningstechnologie." *Tweede Kamer Der Staten-Generaal,* November 20, 2019.

HM Government. N.d. "Report suspicious activity." Counter terrorism policing. Accessed November 25, 2021. https://act.campaign.gov.uk/.

Hofmans, Tijs. 2019. "Gratis deurbellen tegen criminaliteit. Het twijfelachtige effect en de privacyzorgen." *Tweakers,* December 11, 2019. https://tweakers.net/reviews/7524.all/digitale-deurbellen-het-twijfelachtige-effect-en-de-privacyzorgen.html.

Homeland Security. N.d. "About the campaign." If You See Something, Say Something. Accessed November 25, 2021. https://www.dhs.gov/see-something-say-something/about-campaign.

Houwing, Lotte. 2019. "Minister komt met zorgwekkende antwoorden op kamervragen over CATCH." *Bits of Freedom,* September 11, 2019. https://www.bitsoffreedom.nl/2019/09/11/minister-komt-met-zorgwekkende-antwoorden-op-kamervragen-over-catch/.

Houwing, Lotte. 2019. "Volg San Francisco: verbied gezichtsherkenningssoftware in de publieke ruimte." *Bits of Freedom,* July 1, 2019. https://www.bitsoffreedom.nl/2019/07/01/volg-san-francisco-verbied-gezichtsherkennings-software-in-de-publieke-ruimte/.

Houwing, Lotte. 2020. "Hoe de politie haar buitenwettelijke surveillancenetwerk uitbreidt." *Bits of Freedom,* February 5, 2020. https://www.bitsoffreedom.nl/2020/02/05/hoe-de-politie-haar-buitenwettelijke-surveillancenetwerk-uitbreidt/.

Houwing, Lotte. 2021. "Biometrische surveillance in Nederland: Het mag niet, maar gebeurt toch." *Bits of Freedom,* July 7, 2021. https://www.bitsoffreedom.nl/2021/07/07/biometrische-surveillance-in-nederland-het -mag-niet-maar-gebeurt-toch/.

Introna, Lucas, and Helen Nissenbaum. 2010. "Facial recognition technology : A survey of policy and implementation issues." *The Department of Organisation, Work and Technology, Lancaster University* (July). https://eprints.lancs.ac.uk/id/eprint/49012.

Jacobs, Michael. 1997. "Environmental valuation, deliberative democracy and public decision-making institutions." In *Valuing Nature: Economics, ethics and environment.* Edited by John Foster, 211-231. London: Routledge.

Klippenstein, Ken, and Sara Sirota. 2021. "The Taliban have seized U.S. military biometrics devices." *The Intercept,* August 18, 2021. https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

Krikken, Eva. 2021. "Op waarden geschat: Living lab Digitale Perimeter." *Bits of Freedom,* 29 april, 2021. https://www.bitsoffreedom.nl/wp-content/uploads/2021/05/2021rapport-digitale-perimeter-bof.pdf.

Leon, Harmon. 2020. “How LSD, nuclear weapons led to the development of facial recognition.” *Observer,* January 29, 2020. https://observer.com/2020/01/facial-recognition-development-history-woody-bledsoe-cia/.

Louradour, Sebastien, and Lofred Madzou. 2021. “A policy framework for responsible limits on facial recognition, Use case: Law enforcement investigations.” *World Economic Forum* October 1, 2021.

Madiega, Tambiama, and Hendrik Mildebrath. 2021. “Regulating facial recognition in the EU.” *European Parliamentary Research Service,* September 2021.

Morozov, Evgeny. 2014. *To Save Everything, Click Here: Technology, Solutionism and the Urge to Fix Problems That Don’t Exist.* London: Penguin Books Ltd. 2014.

Mendonça, Ricardo Fabrino, Selen A Ercan, and Hans Asenbaum. 2020. “More than words: A multidimensional approach to deliberative democracy.” *Political Studies* 70, no. 1 (July): 153-172. https://doi.org/10.1177/0032321720950561.

NCTV. 2021. “Terrorist threat assessment for The Netherlands 54.” Ministry of Justice and Security, April 2021.

NU.nl. 2006. “Campagne ‘Nederland Tegen Terrorisme’ gelanceerd.” *NU.nl,* 18 september, 2006. https://www.nu.nl/algemeen/828129/campagne-nederland-tegen-terrorisme-gelanceerd.html.

Politie. N.d. “Camera in Beeld.” Accessed November 17, 2021. https://www.politie.nl/onderwerpen/camera-in-beeld.html.

Smith, Marcus, and Seumas Miller. 2021. “The ethical application of biometric facial recognition technology.” *AI & Society* (April). https://doi.org/10.1007/s00146-021-01199-9.

Tucker, Ian. 2013. “Evgeny Morozov: ‘We are abandoning all the checks and balances’.” *The Observer: Technology.* March 9, 2013. https://www.theguardian.com/technology /2013/mar/09/evgeny-morozov-technology-solutionism-interview.

Reclaim Your Face. N.d. “Civil society initiative for a ban on biometric mass surveillance practices.” Accessed October 7, 2021. https://reclaimyourface.eu/.

Rijksoverheid. N.d. “Hoe kan ik helpen om een terroristische aanslag te voorkomen.” Terrorismebestrijding: vraag en antwoord. Accessed November 25, 2021. https://www.rijksoverheid.nl/onderwerpen/terrorismebestrijding/vraag-en-antwoord/hoe-kan-ik-helpen-om-een-terroristische-aanslag-te-voorkomen.

Rosenberger, Robert, and Peter-Paul Verbeek. 2015. “A field guide to postphenomenology.” In *Postphenomenological Investigations: Essays on Human-Technology Relations.* Edited by Robert Rosenberger and Peter-Paul Verbeek, 9-42. London: Lexington Books.

Sagoff, Mark. 2008. *The Economy of the Earth: Philosophy, Law, and the Environment.* Cambridge: Cambridge University Press.

Sanders, Lynn M. 1997. “Against deliberation.” *Political Theory* 25, no. 3 (June): 347-376. https://www.jstor.org/stable/191984.

Smarthomeweb. 2020. “Ring slimme deurbel met gezichtsherkenning.” October 21, 2020. https://www.smarthomeweb.nl/binnenkort-ook-ring-slimme-deurbel-met-gezichtsherkenning/.

South Wales Police. 2021. “Deployments.” Smarter Recognition Safer Community. Accessed October 7, 2021. https://afr.south-wales.police.uk/.

Van Dijck, José. 2019, “Wildgroei van gezichtsherkenning regelt zich niet vanzelf.” *Financieel Dagblad,* September 4, 2019. https://fd.nl/opinie/1315377/wildgroei-in-gebruik-van-gezichts-herkenning-regelt-zich-niet-vanzelf.

Van Rest, J.H.C., T. Attema, T. Timan, R.J.M. den Hollander, en G.P. van Voorthuisen. 2021. *Privacy bescherming bij niet-coörporatieve gezichtsherkennng.* Den Haag: TNO, 2021.

Verbeek, Peter-Paul. 2006. “Materializing morality: Design ethics and technological mediation.” *Science, Technology & Human Values* 31, no. 3 (2006): 361-380. https://www.jstor.org/stable/29733944.

Young, Travis. N.d. “The evolution & history of dash cams.” *WiredSmart.* Accessed December 27, 2021. https://wiredsmart.io/dash-cams/evolution-and-history/.

Ziller, Conrad, and Marc Helbling. 2021. “Public support for state surveillance.” *European Journal of Political Research* 60, no. 4 (November): 994-1006. https://doi.org/10.1111/1475-6765.12424.