Rathenau Instituut

Citizens and sensors

Eight rules for using sensors to promote security and quality of life

Report

Authors

Dhoya Snijders, Marijn Biesiot, Geert Munnichs, Rinie van Est, met medewerking van Stef van Ool en Ruben Akse

Illustrations
Rikkers Infographics

Photo cover
David Rozing / Hollandse Hoogte

Preferred citation:
Snijders, D., M. Biesiot, G. Munnichs, R. van Est (2020). *Citizens and sensors – Eight rules for using sensors to promote security and quality of life. The Hague: Rathenau Instituut*

Foreword by Melanie Peters

All around us, we see a growing number of sensors being used to promote security and quality of life. Smart cameras read our number plates, body cams record what police officers encounter on the street, and there are even experiments with lampposts that measure sound levels to detect quarrels. Some of these sensors are used by law enforcement, but the majority belong to private citizens and businesses. For example, I am part of a neighbourhood crime watch group on WhatsApp, and smart cameras at Schiphol Airport monitor and analyse my behaviour.

Technological advances increasingly offer opportunities for surveillance, which puts law enforcement in a complex position. Dutch Police Commissioner Erik Akerboom noted in our *Decent Digitisation* blog-series that on the one hand people are worried that 'their freedom will be severely restricted if historical data determine how they are perceived today and for the rest of their lives'. On the other hand, it is 'socially unacceptable for the police not to make use of technology that can improve public safety'. The key to managing this tension is to find the right balance between the two.

At the request of the Dutch national police force, we investigated how the public thinks about the use of sensors to promote quality of life and security. The findings are presented in this report. In our research, we organised focus groups in which we talked to private citizens about sensors that are becoming smarter, more mobile and more ubiquitous and elaborate. These conversations show that people expect law enforcement to consult with the public and strike a healthy balance between a range of disparate public values. In addition to physical safety and privacy, these values include democratic rights, efficient and effective business operations, innovativeness, transparency, quality of life, personal freedom and human contact. Based on the outcomes of our study, we propose eight rules that can help to achieve a healthy balance between the disparate values.

Digital technologies are changing the way teachers teach, how doctors and patients talk to each other, what politicians debate, and how people share news. They are also changing the way we observe and monitor one another. The Dutch government has expressed its support for a digital future in which everyone can participate. We hope that the eight rules set out in this report will help to achieve this.

Dr. ir. Melanie Peters
Director Rathenau Instituut

Foreword by Ido Nap

Sensors have become commonplace. They make our lives easier, both at home and elsewhere. On the streets, citizens encounter them everywhere. There are cameras in nightlife areas (some of which react to noise, shouts or screams), traffic lights with sensors that initiate ‘green waves’ for cyclists, lampposts that light up when it’s foggy or dark, ‘connected cars’ that analyse overall driver behaviour, and so on. Car parks store your vehicle registration information when you enter or leave, and Google knows exactly when you’re at home. These data are collected fora reason: they form the basis for many other applications, both wanted and unwanted.

What do people think of this changing world, and do they find it acceptable? How would they feel if detectives investigating a serious crime had access to a car manufacturer’s data on driver behaviour? Would they also find it acceptable if data on speeding were used ‘only’ to prosecute speeding violations, or drunk driving? And what if vehicle sensor data show a car manufacturer or an insurer that a certain driver regularly breaks the speed limit or drives recklessly – do we expect *them* to intervene?

Society must be able to count on government to deal professionally with sensor applications in public places. In particular, when quality of life issues overlap with security issues, government – and law enforcement in particular – should know how to use sensors to benefit society and should understand the legal and social frameworks within which their use is acceptable. But that knowledge cannot be assumed. As a society – and that society includes law enforcement agencies – we are still in search of relevant legal and social frameworks for new digital possibilities. We must also be aware that what is acceptable is not always sensible.

It is in this context that the Programme Director for Digitalisation and Cybercrime of the Dutch national police force asked the Rathenau Instituut to examine what people think of a world with a growing number of private and public sensors in which the police also plays a role. This study has given us a better idea of what is important to the public when the police, local authorities, businesses and private citizens themselves use sensor data, and which rules should govern such use.

This new awareness will help us to use sensing applications in a socially responsible manner. The study has also shown us that the public expects us, as law enforcement officials, to learn how best to apply new technologies in our work.

We will actively take these rules into account when developing new sensor applications.

The rules and conceptual framework set out in this report can also help the police force and other organisations to be more responsive to the public's questions, opinions and criticisms of sensor use. The findings therefore also furnish tools for engaging in dialogue with the public, businesses, executive boards and other professionals, and for generating support for using and evaluating sensing applications to promote security and quality of life.

I would like to thank the researchers at the Rathenau Instituut for this report and for the many hours that we have spent pinpointing lessons learned and how we should interpret the findings. I would also like to thank the advisory committee for its constructive criticism. Its input has made this study even more valuable.

Ido Nap
Sensing Programme Manager

Summary

The Dutch national police force wants to know what using sensors means for law enforcement as a profession and for the societal legitimacy of policing. The Programme Director for Digitalisation and Cybercrime therefore asked the Rathenau Instituut to investigate what the public thinks about using sensors to promote quality of life and security. We looked not only at police deployment of sensors but also at the growing use of sensors across society. Based on the results of a literature review and focus group research, this report presents a conceptual framework of factors that influence the public's perception and eight rules governing the use of sensors for purposes of security and quality of life.

Sensors to promote security and quality of life
Sensors, such as cameras or Wi-Fi trackers that monitor and record movement, are increasingly being used in the Netherlands to improve quality of life and security. Private citizens and businesses, for example, own approximately 1.5 million security cameras, local authorities operate more than 3,000 surveillance cameras and the police have approximately 500 to 1,000. With new technology making such sensors smaller, cheaper and more mobile, they are becoming easier to integrate into other devices, such as cameras in smartphones. Also, it is getting easier to collect and process data, for example with smart algorithms in apps. All these advances have resulted in an elaborate network of sensors that generates huge quantities of data. This network not only consists of new sensors but has also drawn in new actors and is shaping new types of surveillance. That is to say, not only government and businesses monitor people (surveillance), but people also monitor one another (horizontal surveillance) and people monitor government and businesses (sousveillance).

This report outlines various trends that show how surveillance is changing. For example, we see that 1) the police force is making more and more use of sensors and sensor data, 2) smart sensor technology is being used to automate core police activities, such as investigating and law enforcement, 3) private citizens, businesses and local government are allcollecting more and more sensor data, 4) new forms of cooperation are emerging between the police and other actors in society involving the use of sensors to promote quality of life and security, and 5) private parties are themselves using sensors to investigate and enforce law.

Which factors determine what the public thinks about sensors?
To understand what the public thinks about using sensors to promote security and quality of life, we developed a conceptual framework (see Figure 1). We

differentiate between three dimensions of private citizens (left-hand column, bold) and three dimensions of sensor applications (right-hand column, bold) that influence what people think about the use of sensors to promote quality of life and security.

Important factors for citizens

The literature shows that personal traits, general attitudes and the immediate social environment play a role in informing the public's opinions. For example, older people are more likely than younger people to accept sensor technologies. It also appears that men are more likely to consider the party using the sensor (such as the police or a private security firm) important, whereas for women it is the purpose of the investigation. Finally, having a positive attitude towards technology in general tends to boost a person's confidence in sensors.

We also differentiate between three dimensions of sensor applications that influence the public's opinion of sensors. To begin with, there is the technology itself, i.e. the type of sensor and the extent to which it incorporates privacy-by-design principles. The next dimension is social practice and actors, referring to the context in which the technology is being used and the people or organisations involved. Finally, there is the societal and institutional context, for example legal regulations concerning camera surveillance or the level of public trust in the authorities. To find out more about what the Dutch public thinks of sensor technology, we organised various focus groups.

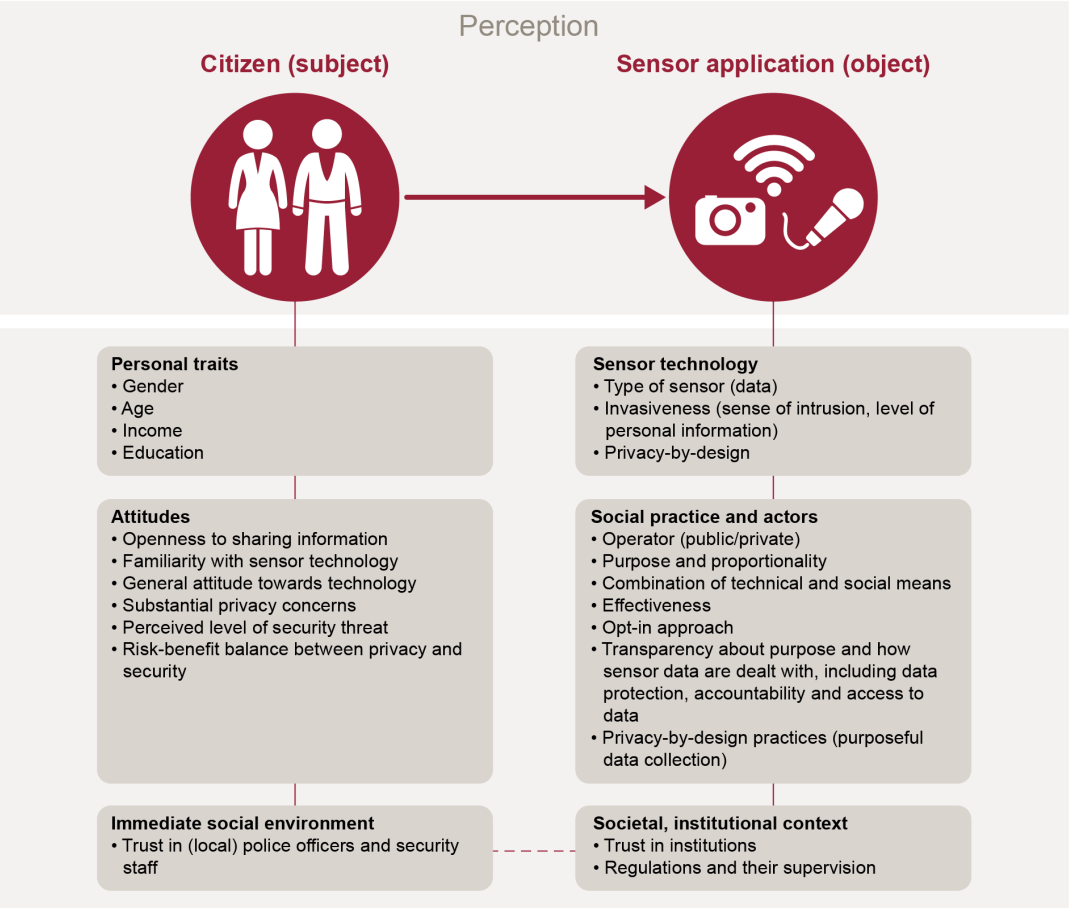
What does the Dutch public think about using sensors?

The picture that emerges from the focus groups is nuanced. It is impossible to talk about the acceptance of certain sensors or technologies without considering the context. People are neither for or against certain technologies, such as body cams or Wi-Fi trackers. Their opinion depends on:

- the features of the technology itself
- the purpose for which it is being used
- the effectiveness of the technology
- the type of crime for which the technology is employed, and
- the context in which it is applied (where, when, how, by whom).

The focus group discussions revealed that two factors are particularly important: the setting in which sensor technology is used, and how safe people feel in that setting (see Figure 2). We see that acceptance of sensors depends on the perceived level of safety: the more risk people perceive in a situation, the more they tolerate the use of sensors to improve security and quality of life. Acceptance also depends on the setting: the use of sensors in private settings is less acceptable than their use in public places, especially in crowded situations.

Figure 1 How people think about using sensors – a conceptual framework

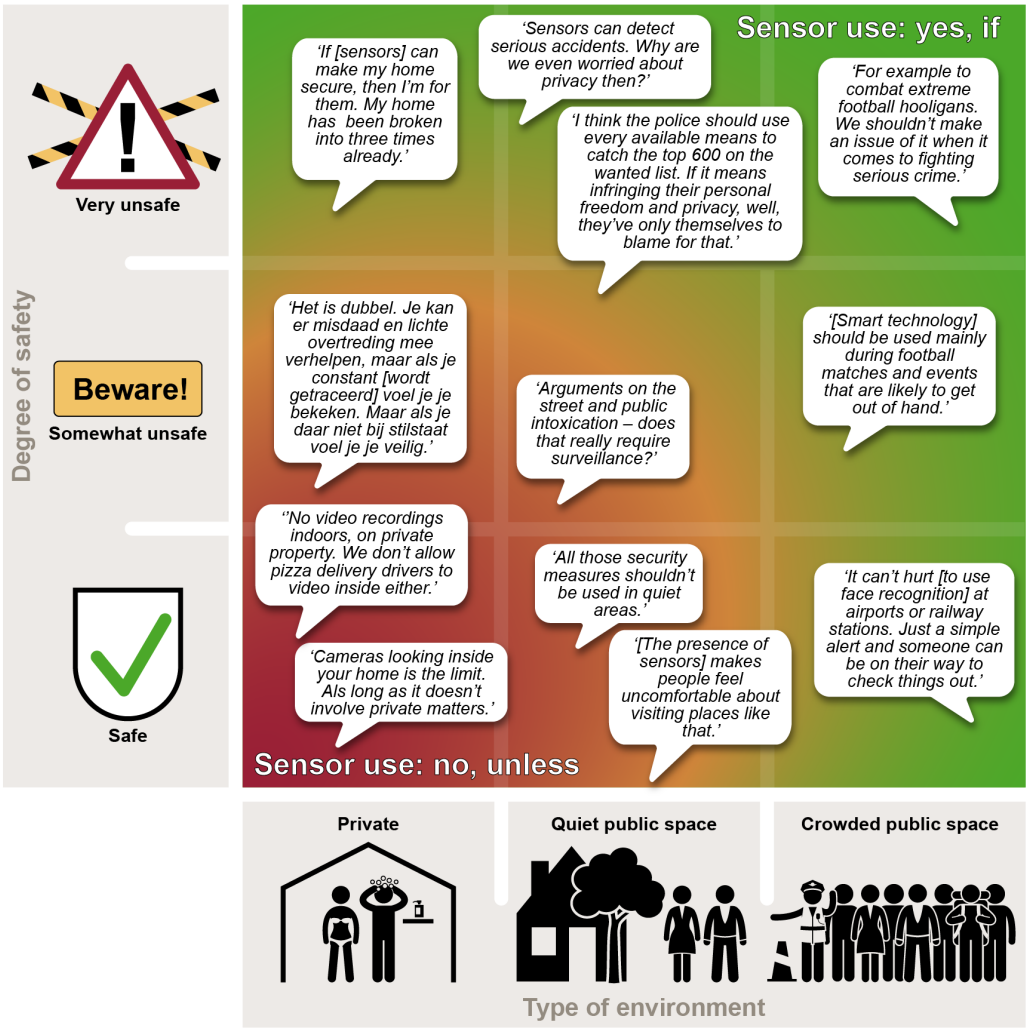


Source: Rathenau Instituut

On the one hand, then, people do approve of the use of sensors in very unsafe circumstances and crowded public places, but only if doing so meets a number of important criteria. On the other hand, people do not approve of using sensors in private homes or in quiet public places that feel safe or only slightly unsafe, unless doing so clearly improves security and quality of life and meets a number of important criteria, for example relating to privacy and personal freedom.

The focus groups revealed that values also guide people's opinions. For example, the discussion about sensor technology use was often framed as a trade-off between security and privacy. At the same time, people clearly feel that a broader range of values should be considered when using sensors. In addition to security and privacy, these values include democratic rights, efficiency, effectiveness, innovativeness, transparency, quality of life and human contact.

Figure 2 Influence of perceived safety and setting on public acceptance of using sensors to improve quality of life and security



Source: Rathenau Instituut

Eight rules for using sensors

The police are expected to consider and in fact uphold the aforementioned public values when deploying sensors and sensor data. In reality, however, such values can be at odds with one another and the public therefore expects law enforcement to strike a healthy balance between disparate values, in consultation with the public. We have taken the results of our literature review and focus group research to come up with a set of rules governing the interpretation of these values in real-life situations. The rules are aimed specifically at law enforcement, but our study shows that the public would like other branches of government, businesses and fellow citizens to play by these rules as well.

1. **The police should use sensors in a way that inspires public trust.**

2. **Provide the public with straightforward, transparent information about the use of sensors.**
3. **Apply privacy-by-design principles.**
4. **Citizens do not want the employment of sensors to lead to a reduced amount of presence of and contact with police officers.**
5. **Citizens want the police to be both innovative and effective in the employment of sensors.**
6. **The use of sensors may not lead to discrimination.**
7. **Ensure personal freedom by restricting the use of sensors for security purposes to unsafe situations and crowded public places.**
8. **The foregoing rules equally apply to cooperation between the police and other parties.**

Contents

Introduction

1.1 The sensor society

Some years ago law enforcement agencies predict that by 2020, 90% of the automated data streams available to them will come from private and public sensors.[1] Such sensors make it possible to collect, analyse and use data automatically, in the fight against transport crime, for example. Smart cameras set up along motorways and in car parks have helped the police to reduce lorry and cargo theft in recent years. Examples include remote-controlled 'dome cameras', infrared cameras and automatic number plate recognition (ANPR) cameras, used to detect cargo theft. Between 2009 and 2011, the number of heists from lorries traveling on the A67 motorway from the Port of Rotterdam to Germany fell from 74 to 4.[2] The police did not undertake this campaign on their own but collaborated with private security firms, local authorities and businesses.

Sensors are becoming increasingly important for government, businesses and the public, and this means that not only the police force but also other actors are taking on such tasks as investigation, surveillance and enforcement. For example, motorists who take out motoring club ANWB's Safe Driving insurance policy are given an in-car sensor system that collects data every time they drive and keeps track of their driving style. Safe driving habits may earn users a discount on their insurance,[3] but ANWB can also terminate the policy if a user takes too many risks. The service works with colour codes. If an insured motorist receives six red alerts or one black alert for speeding in a year's time, ANWB is entitled to cancel the insurance under the terms and conditions.[4]

Our cars, phones, laptops, GPS sensors, cameras and other devices capture the many data traces that users leave behind in their everyday lives. Businesses welcome these sensor-generated data as valuable resources – indeed, some have even referred to them as the 'new oil'. It is important to understand that the

1 'Beleidsvisie sensing'. Appendix to Parliamentary Proceedings TK 2015-2016, 29628, no. 594.
2 G. Homburg, A. Schrijenberg, J. van den Tillaart, Y. Bleeker (2016). *ANPR: toepassingen en ontwikkelingen*. WODC, Den Haag.
3 Speerstra, R-J. 'ANWB-apparaatje ontmaskert parkeerfraudes bij Schiphol, Friezen spleen hoofdrol'. Leeuwarder Courant, 23 October 2018. Retrieved from https://www.lc.nl/friesland/ANWB-apparaatje-ontmaskert-parkeerfraudes-bij-Schiphol-Friezen-spelen-hoofdrol-23693008.html
4 Terms and conditions of ANWB Safe Driving Insurance. ANWB, November 2016 version, Articles 8.10 and 33. Retrieved from https://www.anwb.nl/binaries/content/assets/anwb/pdf/verzekeringen/polisvoorwaarden/voorwaarden-veilig-rijden-autoverzekering.pdf

discussion about sensor technology is not only about sensors themselves, but about new data-ecosystems.

The rise of 'big data', the fascination with the 'data scientist', and the development of new forms of data analytics and interconnectivity between data systems are all interlinked in this respect. Andrejevic and Burdon have coined the term 'sensor society' as a useful way of approaching these interconnections and exploring their societal significance.[5] The defining attributes of the sensor society are:
1) the increasing deployment of interactive, networked devices as sensors; 2) an explosion in the volume of sensor-generated data; 3) the development and application of predictive analytics to handle the huge amounts of data; 4) the ongoing development of data collection, data storage and data-analysis infrastructures devoted to making sense of sensor data.

The emergence of the sensor society has implications for the way in which we collect and store data, but it also generates new views on relationships between different groups of people and concepts such as security, quality of life, privacy and surveillance.

1.2 Quality of life and security

With sensor technologies and applications varying so widely, we have been forced to focus on specific contexts in this study. We have defined the boundaries of our research by choosing to concentrate on quality of life and security. We have chosen these domains because they highlight an interesting dichotomy. On the one hand, the public, businesses and law enforcement appear to have considerable confidence in the role that technology and digitalisation can play in tackling major societal issues related to security and quality of life. On the other hand, there is a growing awareness that the deployment of technology impacts numerous public values and mutual social relationships, from privacy and safety to equal treatment and power imbalances.

We realise that quality of life and security are ambiguous concepts that cannot easily be captured in a single definition. For example, there are various types of 'security'[6], such as economic, environmental, military, physical, emotional or digital

5 Andrejevic, M. & Burdon, M. (2015). 'Defining the Sensor Society.' *Television & New Media* Vol. 16(1) 19–36.
6 The Dutch word *veiligheid* encompasses both 'safety' and 'security'. This article in fact addresses issues of security *and* personal and public safety, but for simplicity's sake we use the word 'security' here to cover both concepts.

security.[7] Security can be defined *subjectively* as a feeling shaped by personal experiences, but it can also be defined *objectively* through quantifiable factors such as the number of crimes reported to the police within a given domain.[8] Our research does not concern itself with the varying interpretations of security. We interpret security and quality of life as compliance with laws and regulations, with the concepts positioned on a sliding scale: quality of life relates to minor infractions, such as littering, while security relates to more serious offences.

1.3 Research question

At the request of the Dutch national police force, the Rathenau Instituut has examined how private citizens perceive the use of sensor data to promote quality of life and security. To legitimise its actions, the police must have the public's trust when using sensor technology. That is why the police force would like to understand the factors influencing public opinion about the way in which different actors use sensors and sensor data. It wants to know what the public considers to be possible, acceptable and desirable.

Having a better understanding of public opinion will help the police to engage in dialogue, to formulate policies going forward, and to use technology in a socially responsible manner. The main research question is:

Which factors play a role in how the public perceives the use of sensors and sensor data by law enforcement, businesses, local government or private citizens for purposes of quality of life and security?

We answer this question by addressing four sub-questions:

1. What is the state of affairs in the Netherlands with regard to the use of sensors and sensor data for purposes of security and quality of life?
2. What has previous research revealed about the factors that underlie the public's perception of sensors and sensor data used for purposes of security and quality of life?
3. What relevant socio-technical scenarios can be proposed to the public?
4. How does the public perceive the deployment of sensors and sensor data for purposes of security and quality of life, and what factors underpin this perception?

7 Baldwin, D. (1997) 'The concept of security'. *Review of International Studies*, *23*, 5-26; Kool, L. et al. (2017). *Urgent Upgrade: Protect public values in our digitized society*. The Hague: Rathenau Instituut.

8 Stol, W., Tielenburg, C., Rodenhuis, W., Kolthoff, E., van Duin, M. & Veenstra, S. (2016). *Basisboek integrale veiligheid*. Den Haag: Boom Criminologie.

1.3.1 Explanation of sub-questions

We zullen hieronder per deelvraag toelichten wat we met de belangrijkste begrippen bedoelen en hoe we deze vragen proberen te beantwoorden.

Sub-question 1: What is the state of affairs in the Netherlands with regard to the use of sensors and sensor data for purposes of security and quality of life?

We identify:

a. the types of sensors used in the Netherlands in relation to security and quality of life;
b. the actors that own these sensors;
c. the actors that use sensor data for purposes of security and quality of life.

The sensor owner and the user of sensor data are not necessarily one and the same actor. For example, businesses can sell consumer product data to law enforcement agencies. Here, the consumer owns the sensor but multiple parties use and act with the data that the sensor generates. A private citizen may own a car, but a built-in speed delimiter uses sensor data to automatically adjust the speed without the owner having any control over it. We define the term ‘use’ broadly, in other words.

Sub-question 2: What has previous research revealed about the factors that underlie the public’s perception of sensors and sensor data used for purposes of security and quality of life?

This sub-question addresses what we already know about the public’s perception of the use of sensors and the sharing of sensor data for purposes of security and quality of life. We examine both Dutch and international academic literature.

Sub-question 3: What relevant socio-technical scenarios can be proposed to the public?

To facilitate discussion of the use of sensors to promote security and quality of life, we devised scenarios that acknowledge the versatility of sensor technology and public values. We refer to them as socio-technical scenarios because they reveal the interdependence between sensor technologies and the social context or contexts in which they are used. We discussed these scenarios with the focus groups to examine what private citizens regard as important when it comes to using sensors and sensor data.

Sub-question 4: How does the public perceive the deployment of sensors and sensor data for purposes of security and quality of life, and what factors underpin this perception?

Based on the socio-technical scenarios identified in the previous question, we used this sub-question to deepen our understanding of public perceptions of the use of sensors and sensor data. We did this by organising focus groups in which we discussed the deployment of sensors with private citizens and examined their feelings, rationales and considerations. Our findings can help the police to engage in a meaningful dialogue with the public about how best to integrate sensor technology into policing in a socially responsible manner.

1.3.2 Publications

This study is meant to encourage public discussion of the responsible use of sensor data for quality of life and security purposes. In addition to publishing our overall findings in the course of our research, we have therefore also published two articles dealing with the first two sub-questions of the study.[9] To give readers a better understanding of the practice of sensor deployment, we also conducted interviews with people who are involved with sensors, most of them in a professional capacity. The interviews can be found between the chapters of this report in six 'intermezzos'. They were published online in Dutch during the research trajectory.

1.3.3 Advisory committee

For quality control purposes, we established an advisory committee of experts in the field who provided feedback on our research methods and findings (see Appendix 3). The committee members are active in a variety of different domains (local government, the business community, civil society, science, and law enforcement).

1.4 Reader's guide

After the introduction, we look in detail at our methodology in **Chapter 2**. We describe our approach to the literature study, the interviews and the focus groups (that were based on the socio-technical scenarios we developed).

Chapter 3 answers the first sub-question and discusses the current state of affairs in the Netherlands with regard to sensor deployment. We analyse the sensor data value chain and reveal current trends in sensor applications in the Netherlands, and

9 See: Biesiot, M., Jacquemard, T., Van Est, R. (2019) and Biesiot, M., de Bakker, E., Jacquemard, T., and Van Est, R. (2019).

discuss how surveillance and the actors involved in surveillance are evolving into a ‘sensor society’.

Chapter 4 discusses the second sub-question, based on a literature review outlining what other scientific researchers have concluded about public perceptions of sensors and sensor data. We introduce a conceptual framework that helps us dig deeper into public perceptions of sensor deployment in our own research.

Chapter 5 looks at the focus groups. We report the actual discussions as accurately as possible by sticking to the structure of the focus group sessions and by quoting literally from the conversations.

Chapter 6 describes our analysis of the focus groups and answers the final sub-question: ‘How does the public perceive the deployment of sensors and sensor data for purposes of security and quality of life, and what factors underpin this perception?’. We do this by structuring our analysis around the conceptual framework presented in Chapter 4 and by comparing our own data with those of other researchers covered in our international literature review.

Chapter 7 is the concluding chapter. We look back on the main question and its sub-questions and, based on our conclusions, present a set of rules for a socially responsible approach to sensor deployment.

Intermezzo: crowd management

Amsterdam's authorities are trying to make the city safer by using sensors to better regulate pedestrian traffic. Decisions are taken based on camera and Wi-Fi tracker data during major events and in congested areas (such as the Red Light District and Kalverstraat). This approach is known as 'crowd management' and it involves new forms of cooperation between local authorities and the police.

Source: Sergey Galyonkin / Flickr

Daniël van Motman, who works for Amsterdam's traffic management unit, talks about the technology involved and the future of sensors in the city.

Crowd management and crowd control
According to Van Motman, the principle of crowd management is fairly straightforward. The influx of pedestrians must be managed so that the network of streets won't be overcrowded during peak times. It is the same principle used to manage vehicle traffic. Crowd management involves analysing the situation, providing information, and devising and implementing measures. It is only in critical circumstances that the police are called in to exercise crowd *control*, for example by closing a street.

The local authority's aim is to avoid crowd control and to divert the flow of people as much as possible using 'smart' methods. Van Motman notes that this is nothing new; even before sensors became available, city officials would forecast the number of visitors and feed the result into a simulation model (of Dam Square, for example), pinpointing potential problem areas in advance.

More recently, 'smart crowd management' based on sensor technology is helping to speed up and improve the city's response in real time. 'We've been testing Wi-Fi tracking and people-counting cameras since SAIL Amsterdam 2015 {ed. a large 5-yearly maritime event). We've given it a lot of thought: where do you set up the sensors and cameras, and what's the best way to count?' Wi-Fi tracking uses the MAC address – a unique identifier assigned to a mobile device – whereas cameras count the number of people and detect body types. Data from both sources are then used to analyse the situation on the street, with pedestrians being represented by dots on a digital map simulation.

After a successful trial run during SAIL Amsterdam 2015, the city installed sensors and cameras in Kalverstraat and the Red Light District, the aim of the project being to build expertise in both the technology and traffic conditions over the longer term. 'The thinking was that an event lasts only three to five days, but we wanted ongoing, long-term surveillance. Events often have a peak period, but the Red Light District is more or less at peak capacity all the time.' Initial analysis showed that overcrowding in the narrow, winding streets of the Red Light District had resulted in hazardous logjams, especially at night and in the weekend.

Technology *and* people are the solution

Data on the number of pedestrians and their estimated route were fed into in the simulation model in real time. The model considers all property and infrastructure in the area and calculates crowd density. Because crowd density was too high in the Red Light District, the city decided to deploy 'hosts' there, i.e. officials who manage the crowds along the narrow streets. 'We don't want to close off streets immediately. We're looking for "soft" measures. The hosts keep bidirectional pedestrian traffic flowing and they tell people to move along.'

Van Motman emphasises that technological and human intervention converge in this case; the metrics complement the work of civil servants and help them decide how and where to deploy the hosts most effectively.

The collected data can also lead to action being taken at other levels. For example, police duty rosters can be adjusted in busier or quieter times, or the burden on the city's infrastructure might become clearer. 'When a quay and a bridge in the Red Light District needed replacing, the city wanted to remove them and then replace

them later. Based on the data, we concluded that we really needed to install a temporary bridge, otherwise there would be problems.'

Data processing and privacy
The project is generating vast sensor data streams. All these data now end up on a platform managed by a commercial enterprise. 'We're trying to get the city of Amsterdam to host the platform. We want to control the data so that we can share them with municipal partners and develop useful applications with them.'

Van Motman says that the general public must be absolutely convinced that there are no commercial motives involved, e.g. that crowd metrics are not meant to tempt visitors to walk past certain shops or products, as is the case with commercial parties such as shopping malls. 'Businesses always take commercial factors into account when it comes to pedestrian routes and crowds. Our entire focus is on convenience and public safety.' Van Motman also stresses that municipal researchers never track individuals. 'We're not interested in individual people – that's not crowd management.' Amsterdam's Personal Data Committee has also screened the project against privacy criteria.

A website was developed to ensure transparent communication with the public, and signs have been posted at sensor and camera locations. So far, the local council and businesses in the Red Light District have responded favourably to the project. One interesting side effect is that pub owners in the Red Light District have noticed fewer drug dealers on the streets because there are always hosts walking about.

Future and cooperation
Going forward, Van Motman foresees many different ways of using data in Amsterdam. 'Infrastructure is often rigid, but a smart city would be flexible. If we saw a peak in cyclists in the morning, then we could open extra bicycle lanes. Later in the day, we could free up two lanes for lorries. And in the afternoon, we could turn it into one big pedestrian walkway.'

In the long term, it should be possible to map out the entire mobility chain from Schiphol Airport to Amsterdam. That would allow the city to anticipate the arrival of charter flights at Schiphol Airport, for example. But such solutions are still a long way off. For the time being, work is under way to develop a public dashboard with traffic volume data that can help visitors decide whether to go to a specified destination. 'If you make the reasons clear and explain how people will benefit, then I truly believe that the public will be willing to cooperate.'

2 Approach and methods

2.1 Introduction

We answer the main research question of this report by examining four sub-questions. This chapter describes the study's methodological considerations and summarises the steps taken to answer each sub-question. The chapter also describes the conceptual and practical choices that played a role (see Table 1).

Table 1 Overview sub-questions and methods

Research question	Method
Sub-question 1 What is the state of affairs in the Netherlands with regard to the use of sensors and sensor data for purposes of security and quality of life?	Literature review
Sub-question 2 What has previous research revealed about the factors that underlie the public's perception of sensors and sensor data used for purposes of security and quality of life?	Literature review Interviews
Sub-question 3 What relevant socio-technical scenarios can be proposed to the public?	Scenario-development
Sub-question 4 How does the public perceive the deployment of sensors and sensor data for purposes of security and quality of life, and what factors underpin this perception?	Focus groups

The way in which we have structured the research informs the structure of the present chapter. For example, we devote separate sections to our literature review (2.2), interviews and intermezzos (2.3), the socio-technical scenarios (2.4) and the focus groups (2.5). In each case, we discuss our reasons for using the relevant method, what this method entails and how we have applied the method. Because focus groups are at the heart of our study, we discuss this method in more detail.

2.2 Literature review

Our literature review is designed to give us a better understanding of the research questions and to serve as input for two other research methods, i.e. the socio-technical scenarios and the focus groups. We conducted the review in two phases.

We began by performing desk research and a literature review regarding the current use of sensors and sensor data in the Netherlands for purposes of security and quality of life. This research allowed us to identify the types of sensors used in the Netherlands for these purposes and the relevant societal actors.

In the second phase, we reviewed what the literature says about the factors that influence public perceptions of sensors deployed within the context of security and quality of life. This review focused on answering sub-question 2 and indicated which factors the public regards as important when sensors are deployed. Examples include the purpose of their deployment, the relevant actor, the degree of transparency in data collection and proportionality.

To encourage a broad discussion, members of the research team wrote and published online articles during both phases of the literature review.

2.3 Interviews and intermezzos

We supplemented our findings from the first research phase with expert interviews. We spoke to two experts who are involved on a daily basis in the development and implementation of sensors in the Netherlands. Discussions with the advisory committee gave rise to the idea of arranging individual interviews with ‘actors in the field’ that would illuminate the context of certain statements and examine the use of sensors in greater depth. We interviewed six people whose professional activities routinely involve the use of sensors, choosing respondents who represent the business community, law enforcement, local government and the public. Another selection criterion was the type of technology (see Table 2). The interviews are presented in the form of ‘intermezzos’, between the chapters.

Table 2 Interviews and intermezzos

Naam	Functie	Technologie	Locatie	Sector
Jaime van Gastel	Vlogger	Video-camera, social media	Amsterdam	Citizen
Daniël van Motman	Traffic management expert, City of Amsterdam	Crowd management: wifi-trackers and cameras	Municipal Offices, Amsterdam	Local government
Tinus Kanters	Project manager for Stratumseind Living Lab, City of Eindhoven	Data analysis and predicting behaviour	Stratumseind, Eindhoven	Local government
Erwin Binneveld	Founder Spar University	Smart shop	Spar Winkel De Uithof, Utrecht	Business community
Arjen Wollers	Senior Constable, police force	Bodycam	Police station Amersfoort	Law enforcement
Juliette Anker	Intelligence Specialist, Limburg police unit	ANPR-camera and predicting behaviour	Police station Roermond	Law enforcement

2.4 Socio-technical scenarios

The scenario method is widely used to foster ‘strategic conversations’ by and between government, businesses and other civil society organisations. By exploring the array of future possibilities, an organisation can develop a vision of its environs and devise a strategy on that basis.[10] In this study, we opted to use scenarios to spark focus group discussions about using sensor applications to promote security and quality of life. We developed socio-technical scenarios, which are meant to

10 Est, R. van (2004). *Dictaat: Toekomstverkenningen en socio-technische scenario’s*. Eindhoven: Technische Universiteit Eindhoven.

address the interconnection between technological advances and social embeddedness.[11] Developing the scenarios was not a goal in itself, however, but merely a means to give the focus groups a clear idea of how sensors are or may be used in practice to promote security and quality of life and to open up this subject for discussion.

Three scenarios

We developed a total of three scenarios to spur discussion of important aspects of sensor applications, such as the technology used, common practices and the wider context (see section 4.3). We first drew up a long list of sensor applications representing the widest possible range of technologies, contexts, relevant actors, and sensitivities. We presented this list to the advisory committee (see Appendix 2) and, based on their feedback, narrowed it down to a shortlist.

Drawing from this preliminary study, we prepared three scenarios illustrating three technological trends: 'more mobile', 'smarter' and 'more elaborate'. We decided to focus on sensor applications that are already in use in some form but show enough potential to fuel a discussion of further advances within the next five years. In designing each scenario, we also considered the different forms of monitoring that we had noted in the literature review (see section 3.4). After consulting with the client and the advisory committee, we opted to focus on two forms of monitoring, i.e. 'surveillance' and 'horizontal surveillance'. We also incorporated the factors identified in our conceptual framework (see Chapter 4) into the scenarios. For example, each scenario examines the practical effects of a technology, the context in which it is applied and the broader social aspects. Below is a brief description of the three scenarios.

'More mobile' scenario

The first scenario envisions the transition from stationary to mobile camera surveillance by various parties. It addresses cooperation between the police, businesses and the public regarding sensor deployment, cameras (body-worn video cameras and others) and smartphones that private citizens use as mobile cameras.

'Smarter' scenario

This scenario addresses 'smarter' sensors. The emphasis here is on the software that actually makes a sensor application 'smart'. We have opted for automatic facial and behavioural recognition. What is most important in this context is that sensors not only collect information but also automatically analyse it and undertake action, for example opening access gates at airports or automatically detecting pickpockets by their irregular behaviour.

---

[11] Idem.

‘More elaborate’ scenario

The third scenario envisions how a broad array of sensors operated by multiple parties can converge in a specific context. We have opted to discuss the ‘smart shop’ and the ‘smart city’, one as an example of a controlled environment involving commercial interests and the other of an uncontrolled environment involving public (and commercial) interests.

In a smart shop, people take products from shelves, put them in their bags and walk out. There are no cashiers and no queues. This is only possible because of the many sensors constantly monitoring the shoppers. The smart city takes this one step further: there, the local authority and other parties collect data using all kinds of sensors in a bid to promote security and quality of life.

The number of scenarios (three) was appropriate for this study because it allowed us to a) give the participants a broad array of applications to discuss and b) compare results, since each scenario was discussed by at least two focus groups. In the case of ‘more mobile’ and ‘smarter’, we opted for simpler scenarios that revolve around one specific sensor application. In the case of ‘more elaborate’, we describe a more complex scenario involving several types of sensors. The two simpler scenarios were discussed in alternating focus groups and the complex one in all the groups, allowing us to compare focus group outcomes during the analysis phase.

Procedure

We operationalised the scenarios by drawing up a procedure for the focus groups. The procedure structured the discussion, identified the questions, provided the texts and established how much time would be needed for each item (see Appendix 1).

For each scenario, we began with a general question to assess the participants’ knowledge at the start (baseline assessment) and concluded the discussion with specific questions. Each scenario consisted of a number of ‘scenes’, short texts fleshing out the scenario. The participants reviewed the scenes and discussed them during the focus groups.

Kantar Public research agency assisted in drafting the procedure and organising the focus groups. The procedure, and therefore the various scenarios and scenes, was written in easily comprehensible language (B2 language level). We tested readability in several internal and external pilot sessions, as well as with the client and Kantar Public, and made the final text emendations based on the feedback.

2.5 Focus groups

Focus groups shed light on the feelings, rationales and arguments that underlie the public's perceptions of sensor applications. That is why we chose this method to answer our main research question. Focus groups are ideally suited to observing how people express their views and opinions in conversation with others. Although the participants' personal backgrounds play less of a role than in individual interviews, focus groups do provide a good impression of how people talk to one another about a subject. Their responses help to clarify what they think of something, as is the case in everyday life. Focus groups are ideally suited for examining a variety of arguments, viewpoints and perceptions relating to relatively unexplored issues, such as sensors (and how they will be implemented in the future). Focus groups can also be used to explain the differences between perspectives.

Purpose and organization
We organised a total of six focus groups and a pilot focus group. The results of the pilot have not been included in our final analysis. Each focus group lasted two hours and had eight private citizens participating. Kantar Public helped to recruit participants, facilitate the meetings and moderate the discussions. The participants were not aware of the subject of the focus groups in advance and came to the meetings unprepared. At the end of each focus group, Kantar Public drafted the report on the session. Researchers from the Rathenau Instituut attended each focus group as co-moderators and jotted down notes and observations.

The first challenge in organising the focus groups was to establish selection criteria for the participants. We based our criteria on personal traits regarded as relevant for forming an opinion on the subject, i.e. the use of sensors in the context of security and quality of life. To begin with, we made a distinction between people who have attended primary or secondary education and those who have a tertiary education (higher professional and above). We assigned these two categories to different focus groups because our own experience and Kantar Public's recommendations suggest that their conversational dynamics often differ. People with a higher level of education are more likely to speak in more abstract terms, whereas those with a lower and intermediate level of education are more likely to talk about specific and personal examples. To ensure the right atmosphere for an open-hearted discussion in which everyone felt comfortable speaking their minds, we divided these categories into separate focus groups.

Two other relevant background traits were whether the participant 1) lived in a city or a village and 2) in an affluent or less affluent neighbourhood. We identified these

traits in consultation with the police. Our shared assumption was that sensors have a much higher visibility in cities and that urban-dwellers are more aware of them than people living in a (small) village. The size of the community (which in villages is much smaller) may also influence people's perceptions of sensor deployment. Another assumption was that people living in less affluent neighbourhoods might have a different view of sensors than people living in more affluent ones. For one, the latter group usually has the means to purchase sensors themselves. For another, the two groups may have different attitudes towards the authorities, possibly influencing how they perceive the use of sensors and sensor data.

In selecting the participants, we took care to recruit a broad cross-section of the population based on age, gender and immigrant origin so that a variety of different perspectives would be put forward in the discussion. Given the small number of participants, however, the composition of the focus groups should not be taken as a reflection of the Dutch population, nor should it be assumed that the focus groups have yielded representative results. For example, we cannot claim that elderly people in the Netherlands are more critical than young people about the use of biometric cameras. It is not the purpose of this study to make such assertions, but we did make a conscious decision to collect a variety of opinions that would give us a better idea of the feelings, rationales and arguments of private citizens regarding sensor applications. Our purpose was not to achieve consensus or joint decision-making in the focus groups; rather, the setup was meant to encourage participants to express their ideas in an open and frank discussion.[12]

12 Krueger, R. & M. A. Casey (2000). *Focus groups: A practical guide for applied research*. California: Sage.

Intermezzo: a body cam as an extra pair of eyes

Sensors are becoming increasingly mobile, with the police officer's body cam being a concrete example. Senior Constable Arjen Wollens, who does his daily rounds wearing a body cam, talks about his experiences from the police officer's point of view.[13]

Source: Hollandse Hoogte

The idea behind the body-worn video camera

When Arjen Wollens stands up, one cannot help noticing just how many aids and technical devices he's kitted out with. He has a bulletproof vest, a baton, a walkie-talkie, handcuffs, a strap for carrying his riot control helmet, a cartridge holder, a firearm, a pocket knife, a pager in its holder, latex gloves for first aid, a torch, pepper spray, a taser, a body cam, and a notebook and pen. Most of these are suspended from a belt around his waist, but he wears the body cam on a chest strap. 'It all makes for a heavy load, and I'm also wearing a heavy pair of shoes. It's hard for me to keep up with a fleeing suspect on trainers.'

13 The officer's real name has been changed to protect his identity.

As a senior constable, Wollens' main job is surveillance on the streets. He also deals with incidents and reports made by the public, for example a reported break-in, traffic accident, shoplifting incident or physical violence. Wollens's team has been using the body cam for about eight years now, initially in pubs and nightclubs. 'Serious incidents are not uncommon when people go out for the evening, and it can get chaotic.' If it becomes impossible to de-escalate a situation, then officers can decide to switch on the body cam and record audio and images.

Officers may have several reasons for doing so. 'Drunk people often don't remember what they said later on. It's nice for officers to have evidence showing that they acted appropriately even when someone was rude to them.' The recordings can be presented to suspects later and provide evidence that they insulted an officer in uniform or committed a violent act. 'Sometimes the courts question the accuracy of reports that we type up later. Video recordings are ideal for removing their doubts.'

Using the body cam

The body cam starts recording as soon as the officer switches the camera to stand-by manually. To save the recording, the officer presses a specific camera button twice. The camera also saves the previous thirty seconds of recording.

The officer can view the recording on a smartphone app and then save it on an external hard drive. The officer can also decide to delete the recording. The focus group discussions (see Chapter 5) revealed that some people are unhappy about police officers deciding for themselves when to video. Wollens points out that they work according to strict protocols and that they are not there 'to bully people'.

He also points out that police officers are entitled to privacy. 'We talk about private matters at the station and while we're on duty, for example. It would infringe our privacy if all that were recorded.'

Connected to taser

The body cam is updated regularly. The latest version has fewer wires and the camera is now connected to the taser to record its use. When an officer switches on their taser, the body cam turns on automatically, provided it is already on stand-by. It also records the previous two minutes, rather than only thirty seconds.

Wollens says that the body cam makes him feel less vulnerable on the street. If he is being subjected to abuse and can record the incident, he feels more confident about taking action. Police officers can also use the body cam to reflect on their own behaviour. 'Things sometimes go wrong. We're human, after all. I want to learn

from my mistakes.' By viewing a recording later, officers can reconsider their response.

The body cam and how people react to it

A frequent argument in favour of body cams is that they have a preventive effect. One claim is that suspects who realise they are being videoed tend to exhibit less violence towards officers. Wollens confirms that this is true. 'A suspect who's dragged out of anonymity has good reason to behave themselves because we have hard evidence.' But he also says that people get angry when they see the camera.

How do the body cam recordings compare with the officer's own judgement? 'There can be discrepancies between my own interpretation of events and what the camera actually records. In a fast-moving situation, you might mix up the sequence of events. A body cam is a good way to refresh your memory.'

Despite all this, the body cam does not always produce conclusive evidence. For example, it occasionally comes loose. 'If I climb a fence while I'm chasing someone, the camera can fall right off and then I have to go search for it later.' And the images captured when an officer is wrestling with a suspect may be useless. The camera also has to be on stand-by before it starts recording, and officers sometimes forget to switch it on in rapidly evolving situations.

Fighting discrimination?

Chapter 1, Article 1 of the Constitution of the Kingdom of the Netherlands is displayed in large letters at the police station: 'All persons in the Netherlands shall be treated equally, in equal circumstances. Discrimination on the grounds of religion, belief, political opinion, race or sex or on any other grounds whatsoever shall not be permitted.' Wollens recounts a case in which he himself was accused of racial profiling. The person in question was enraged and attacked him verbally. However, because the body cam was switched on, Wollens was able to prove that he had conducted himself properly and, after viewing the recording, his superior was inclined to support his version of the incident. Even so, Wollens does not believe that body cams can resolve every issue. 'A camera has no insight into my reasons for questioning certain people. That's a matter of interpretation, and that's in your head, not in the camera.'

Our interview makes clear that Wollens wants to use the body cam as a tool to furnish transparency about his policing methods. He has faith in his methods and 'I want them on record'. He thinks it would be a good idea for every officer to wear a bodycam, although each one has to feel comfortable using it in their own way.

3 Sensors in the Netherlands

3.1 Introduction

This chapter discusses the current state of play in sensor technology in the Netherlands. It is based on the article 'Eyes and ears everywhere. Using sensor data for safety and quality of life', published by the Rathenau Instituut in the context of this study.[14]

In this chapter, we look at five trends in the Netherlands regarding the use of sensors and sensor related cooperation. We then analyse the concept of 'monitoring' and arrive at a model that shows how forms of monitoring are shifting between different actors in the sensor society. Finally, we show how not only the number of sensors is changing, but also their features. We differentiate between different strands of sensor technology related to quality of life and security.

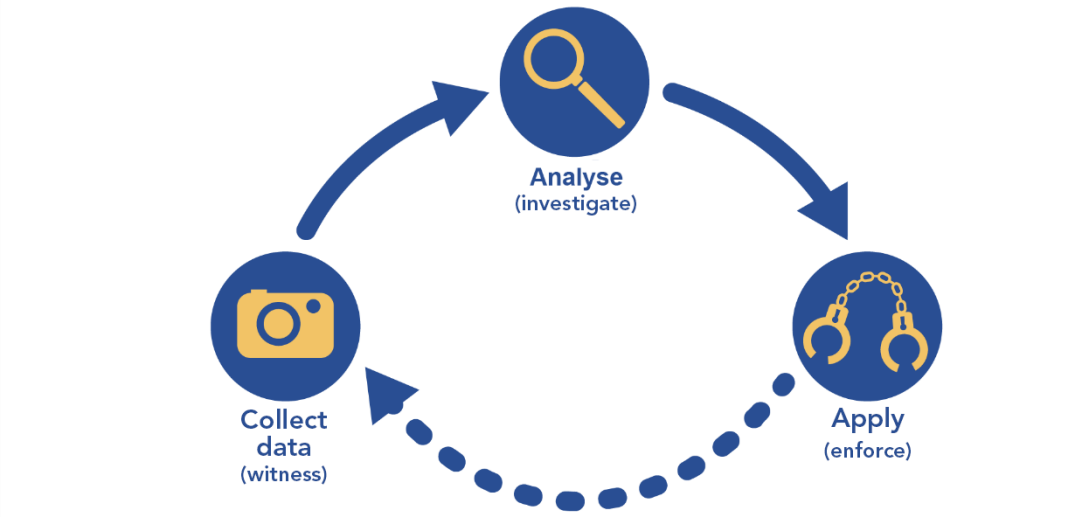
3.2 The sensor data value chain

Sensors that are meant to promote security and quality of life are digital technologies that process data and also intervene in the physical world (see Figure 3). The 'cybernetic loop' helps us to understand how this works. It visualises the entire value chain of digital sensor data and consists of three stages: collecting data, analysing data and applying data.[15] These three stages correspond broadly to three core policing activities: to witness, investigate and enforce.

14 Biesiot, M., Jacquemard, T., Van Est, R. (2019). *Using sensor data for safety and quality of life*. The Hague: Rathenau Instituut.

15 Kool, L. et al. (2017). *Urgent Upgrade: Protect public values in our digitized society*. The Hague: Rathenau Instituut.

Figure 2 Cybernetic loop: the sensor data value chain



Source: Rathenau Instituut

Collect data: witness
Sensors can serve as digital witnesses in situations in which quality of life or security is under threat. The information provided by the sensors supports and enhances observations by the police. Individuals, businesses, and local authorities collect a great deal of sensor data that can help to improve public safety. The police must obtain their consent before accessing that data, however. In addition to sensor data, the police collect information from public sources (such as YouTube and Twitter) and restricted sources (such as court data and banking systems). They also ask the participants of Dutch digital platforms like Burgernet[16] and Amber Alert[17] to provide information about missing persons or suspicious individuals.

Analyse: investigate
Investigating involves searching the data for patterns and outcomes. The police analyse sensor data that has been collected and perhaps combine it with data from other sources. The process can be undertaken by police analysts, and software and artificial intelligence can also play a role.

Apply: enforce
Enforcement involves applying the data, with the police intervening based on their analysis. Enforcement can also involve crime prevention. The automated application of sensor data can, for example, help officers decide which behaviour is irregular but innocent and which is in fact suspicious.

16 'Hoe werkt Burgernet'. Burgernet, 22 October 2018. Retrieved from https://www.burgernet.nl
17 'AMBER Alert Nederland'. AMBER Alert Nederland, 22 October 2018. Retrieved from https://www.amberalert.nl

The cybernetic loop makes clear how sensor data is used in various core policing activities such aswitnessing, investigainge and enforcement. The same model can also be applied to other parties that use sensor data to improve security and quality of life however, such as businesses, local authorities, and private citizens. Sensors make it possible for them to monitor their surroundings and not only collect data but also analyse these data themselves and then take action.

3.3 Trends

Based on the cybernetic loop, we identified five notable trends in the way sensors are used to improve security and quality of life in the Netherlands.

Trend 1: There are more and more police sensors producing a growing amount of sensor data

The Dutch police work increasingly with sensors. The police force was already using sensors in the 1970s, such as cameras to photograph crime scenes and surveillance cameras on the streets. The number and types of digital sensors at their disposal have increased enormously, however. Officers on the street have backup from digital sensor technology and that is affecting their role. They take decisions in part based on sensor information. In that sense, the action that they take is informed by data. It is conceivable that sensor data will play a more decisive role in the near future. In that case, is it still the police officer who is taking the decision?

Trend 2: The police are automating some of their core activities using smart sensor technology

A smart sensor, or automated robot system, can perform core policing activities. The definition of a robot we use here is ‘a machine that can observe, think and act’.[18]

In the case of a robot, the three stages of the cybernetic loop are automated. An ANPR camera can collect images continuously (see section 3.5), but it is still a police officer who decides what action is required based on an analysis of these images. Fully automated intervention is also conceivable, however. For example, the Central Judicial Collection Agency (CJIB) could have ANPR cameras that track motorists and automatically issue fines. The ANPR camera system would then collect the data, analyse it, and take action without human intervention.

18 Van Est, R., D. Bunders & I. Korthagen (2017). ‘Rise of robot city politics: The state of affairs in the Netherlands.’ Essay presented at URBAN AUTOMATION, an international workshop in Sheffield, UK, on 4-6 September 2017.

Trend 3: Private citizens, businesses and local government are collecting growing volumes of sensor data

Digital sensors have become commonplace over the past twenty years. In the Netherlands private citizens and businesses own a thousand times more security cameras than the police, not counting all the smartphones and other sensors. In practical terms, that means that the police have a very large number of digital witnesses to support them in their work.

Trend 4: The police are seeking new forms of cooperation that will allow them to use sensor data collected by the public to improve security and quality of life

We see various examples in the Netherlands of how the police force is cooperating with private citizens, businesses and local government to use sensor data to improve security and quality of life. In Roermond, the police are working with the local authority, Eindhoven University of Technology and the Public Prosecution Service in the public domain. The police also work with private parties, i.e. private citizens and businesses. They are looking for new ways to access the sensor data collected by private parties, for example in the 'Camera in Beeld' project, a form of public-private partnership with private citizens and businesses.

Another example is the police encouraging people to do policing tasks by developing new digital platforms that help private citizens conduct their own investigations. The SamenZoeken (Search Together) app helps people conduct smart searches for missing family members, friends or neighbours. The police officer who devised the app explains: 'It's a fundamentally different way of looking at public participation. We're not asking people to help the police with an investigation but instead helping them with their own searches.'[19] If the police take over the case at a certain point, people can easily share the information they have already collected. Another example is Automon, which will be launched in 2019.[20] It's a variation on Pokémon Go for stolen cars and works as follows:[21] ANPR cameras on the streets recognise the number plates of stolen cars and automatically send an alert to nearby Automon players, who then start looking for the car. The first person to find it receives a reward. An other app – called Sherlock – has been announced to give people tips on how to investigate petty crime, such as vandalism or burglary.

19 'Burgerpanel test meezoek-app'. Dutch national police force, 12 January 2018. Retrieved from https://www.politie.nl/nieuws/2018/januari/12/00-burgerpanel-test-meezoekapp.html

20 Hoorweg, E. et al. (2018). *Vertrouwen en wantrouwen in de digitale samenleving. Trends in veiligheid 2018*. Utrecht: Capgemini.

21 'How these new apps are helping citizens solve their own crimes'. The Next Web, 9 July 2018. Retrieved from https://thenextweb.com/the-next-police/2018/07/09/new-police-apps-citizens-solve-crimes

Trend 5: Private parties are undertaking investigation and enforcement themselves using sensor data

A Ford executive at a major consumer electronics trade fair in Las Vegas raised eyebrows when he announced that, thanks to embedded sensors in Ford's cars, the company knows what drivers are up to. 'We know everyone who breaks the law; we know when you're doing it…We have GPS in your car, so we know what you're doing,' he claimed.[22] Although he later assured his listeners that Ford sought the customer's 'approval or consent', this example shows how sensor applications are generating new types of surveillance. Besides law enforcement and local government, private parties (individuals and businesses) are also using sensors and sensor data to make their own environment safer and more liveable. Not only do they collect sensor data to share with the police (witness), but they also analyse it themselves (investigate), and take action (enforce). They undertake 'do-it-yourself policing' at their own initiative.[23] It is becoming commonplace in the business community, but also among private citizens. 'Jaime the Villain-Spotter', for example, has been tracking pickpockets and shoplifters in Amsterdam as a hobby for years now.[24] He films his adventures and uploads the clips to his own YouTube channel, which has more than sixty thousand subscribers (see the Intermezzo 'Spotting villains').[25]

3.4 Forms of monitoring in the sensor society

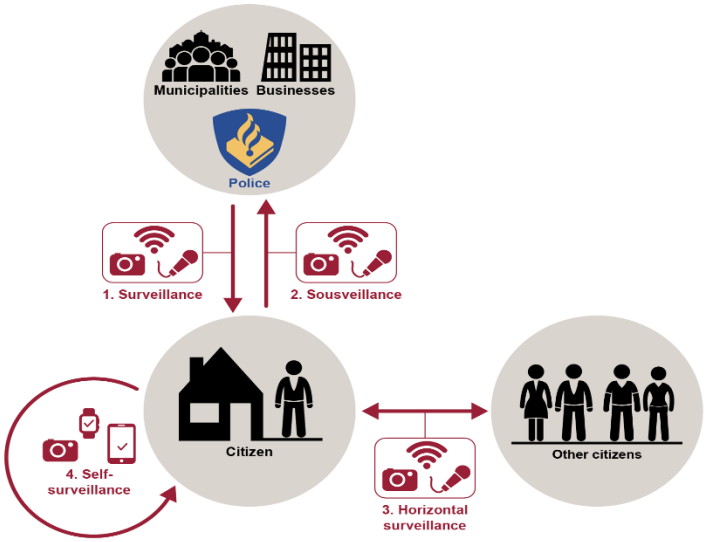
The trends described above reveal a complex network related to 'sensor surveillance'. Private citizens are not only monitored by the police and other bodies (*surveillance*), but also use cameras themselves in various ways (*sousveillance*, *horizontal surveillance*, and *self-surveillance*).

Both public and private parties can collect and analyse sensor data and then take action, but these processes can also take place automatically (at least in part). In addition to the police, private citizens, businesses, and local government are also using sensors to improve security and quality of life. The police have about 500 to 1,000 cameras and local governments have over 3,000 surveillance cameras on

22 Edwards (2014) in Andrejevic, M. & Burdon, M. (2015). 'Defining the Sensor Society'. *Television & New Media* Vol. 16(1) 19-36.
23 Westerink, J. 'Waarom je wel/niet zelf op boeven moet jagen'. NOS, 9 June 2017. Retrieved from https://nos.nl/artikel/2177406-waarom-je-wel-niet-zelf-op-boeven-moet-jagen.html
24 Thole, H., 'Deze 44-jarige manager van een kledingzaak jaagt al 16 jaar op zakkenrollers in Amsterdam… als hobby'. *Business Insider Nederland*, 4 January 2017. Retrieved from https://www.businessinsider.nl/jaime-van-gastel-zakkenroller-jager-amsterdam-youtube
25 'Boevenspotter'. YouTube, 14 August 2018. Retrieved from https://www.youtube.com/channel/UCQOOK3MJ0wNeMeyv7yKdETQ

the streets. By comparison, private citizens and businesses own some 1.5 million security cameras.[26] When necessary, the police want to make use of the data from those sensors, which is why they ask private citizens and businesses to register their security cameras. The idea behind the aforementioned 'Camera in Beeld' project is to provide the police with a list of all such cameras so that, in the event of a crime, they can quickly retrieve all the data from the cameras nearest to the crime scene.[27] Some 200,000 cameras have already been signed up for the project.[28] It is a form of public-private partnership aimed at making society safer. It also shows that people are not only monitored by the authorities but also regularly operate cameras themselves.[29] From the perspective of the private citizen, there are four types of sensor surveillance (see Figure 4).

Figure 3 Four types of sensor surveillance



Source: Rathenau Instituut

1. Surveillance

With surveillance we mean monitoring 'from the top-down', with organisations and authorities monitoring private citizens and property. Camera surveillance on the streets is a familiar example. In our study, we consider surveillance by law enforcement, local government and businesses. Like the police force, local government and businesses also use other types of digital sensors to improve

26 Leenaers, H. (red.) (2016). *De Bosatlas van de veiligheid*. Groningen: Noordhoff Uitgevers, p. 31.
27 'Camera in Beeld'. Dutch national police website, 5 December 2018. Retrieved from https://www.politie.nl/themas/camera-in-beeld.html?sid=8d2bd8fd-17e2-4add-afbf-7873ebb30d70
28 'Politiebonden willen verplicht register voor bewakingscamera's'. *Nu.nl*, 27 June 2018. Retrieved from https://www.nu.nl/gadgets/5334143/politiebonden-willen-verplicht-register-bewakingscameras.html?redirect=1
29 Van 't Hof, C., R. van Est & F. Daemen (red.) (2011). *Check In / Check Uit. De digitalisering van de openbare ruimte*. Rotterdam/Den Haag: NAi Uitgevers / Rathenau Instituut, pp. 75-133.

security in the neighbourhood. More and more local authorities are experimenting with sensors in the context of 'smart city projects',[30] for example for crowd control purposes. In 2017, the City of Amsterdam began using Wi-Fi sensors and smart camera surveillance to determine crowd density on the streets. The aim was to manage the holiday shopping crowds.[31] The City of Eindhoven is working with the police, businesses, and knowledge institutions to reduce disturbances and incidents in the Stratumseind nightlife district. They are experimenting there with noise-sensing cameras that not only measure volume but also warn officers on duty if they detect aggression.[32] Local authorities that undertake 'smart city projects' collect data about private citizens in public places. Amsterdam and Eindhoven have formulated principles for the careful handling of this kind of sensor data.[33] Geonovum (a government foundation) has also proposed a set of rules for using sensors in public places.[34]

Businesses do not limit camera surveillance to office buildings and parking spaces. ProRail, which manages the country's rail infrastructure, has installed smart cameras along tracks to detect copper thieves or trespassers.[35] All seven hundred staff members of the Dutch Railways Safety & Service divison will soon be wearing a body cam, which they can turn on in the event of a high-risk situation.[36] Another form of sensor technology can be found in the security scanners at Schiphol Airport, which use millimetre wave technology to check whether travellers are concealing prohibited items under their clothing.[37]

---

30 Many 'smart city' projects focus on improving quality of life and the living environment in some cases using digital sensors. Projects can also involve improving security, but that is not absolutely necessary, for example in the case of smart signs that guide drivers to a car park with available parking spaces or waste bins that show when they are full. The definition of 'quality of life/living environment' applied in smart city projects is therefore broader than the one used in the present study. See also the website of the Association of Netherlands Municipalities (VNG) on the implementation of the NL Smart City Strategy: https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/smart-society/nieuws/vng-en-g5-gaan-samenwerken-aan-smart-society

31 'Amsterdam zet camera's en wifi-sensoren in voor bijsturen kerstdrukte'. *Nu.nl*, 19 December 2017. Retrieved from https://www.nu.nl amsterdam/5056442/amsterdam-zet-cameras-en-wifi-sensoren-in-bijsturen-kerstdrukte.html

32 Hoekstra, D. 'Netwerk van hypermoderne camera's op Stratumseind in Eindhoven gaat politie helpen'. *Eindhovens Dagblad,* 11 December 2017. Retrieved from https://www.ed.nl/eindhoven/netwerk-van-hypermoderne-camera-s-op-stratumseind-in-eindhoven-gaat-politie-helpen~a1e8acee/

33 Executive Councillors Ollongren and Depla, 20 February 2017. 'Brief Digitale Stad'. Retrieved from https://vng.nl/files/vng/20171204-brief-digitale-stad-wethouders-ollongren-depla.pdf

34 'Spelregels voor sensoren in de publieke ruimte'. Rathenau Instituut, 10 August 2018. Retrieved from https://www.rathenau.nl/nl/digitale-samenleving/waardevol-digitaliseren/spelregels-voor-sensoren-de-publieke-ruimte

35 'Slimme mobiele camera's tegen overlast op het spoor'. ProRail, 22 November 2017. Retrieved from https://www.prorail.nl/nieuws/slimme-mobiele-cameras-tegen-overlast-op-het-spoor

36 'NS introduceert bodycam voor Veiligheid & Service-medewerkers'. NS, 4 July 2018. Retrieved from https://nieuws.ns.nl/ns-introduceert-bodycam-voor-veiligheid--service-medewerkers/

37 'Security check'. Schiphol Airport, 4 October 2018. Retrieved from https://www.schiphol.nl/nl/security-check

Some companies are monitoring their employees with digital sensors.[38] The BestDriver app developed by DHL Express, the City of Rotterdam and CGI (an IT company), for example, utilises sensors and serious gaming to encourage drivers to drive more sustainably and safely.[39]

2. Sousveillance

In the case of sousveillance, it is private citizens who keep an eye on the authorities. The term refers to surveillance 'from the bottom up', for example when a member of the public uses their phone to film the police in action. 'Arrest films' are common on YouTube. They can play an important role in criminal cases, one example being the investigation into the death of Mitch Henriquez after the police used force to arrest him in The Hague in 2015.[40] Bystanders filmed the arrest while Henriquez was on the ground, and his family released photos taken at the hospital. His death led to demonstrations in the Schilderswijk district of The Hague against police brutality.[41] The video images and photos taken by bystanders were used in court to show exactly what had happened.[42]

3. Horizontal surveillance

People who 'spy on' one another, for example by peeking in on their neighbours with a drone,[43] are engaging in horizontal surveillance. They are sometimes referred to as 'little Big Brothers'.[44] In TV programmes such as the Dutch show 'Idiots on the road' screen footage from digital cameras mounted on the dashboard of cars is shown. In the Netherlands, there are already some 250,000 cars with a 'dash cam'.[45] In addition to security cameras inside their house and at the front door, people are also installing sensors that can detect movement and attempted

38 Van Noort, W. 'Zo gluurt de baas digitaal met je mee'. *NRC Handelsblad*, 15 March 2016. Retrieved from https://www.nrc.nl/nieuws/2016/03/15/hoe-de-baas-digitaal-met-je-mee-kan-gluren-1599289-a526307

39 'DHL Express, gemeente Rotterdam en CGI behalen top 3 tijdens NL ICT Milieu Award 2016 met BestDriver-app'. CGI Nederland, September 2016. Retrieved from https://www.cginederland.nl/artikelen/dhl-express-en-cgi-behalen-top-3-tijdens-nl-ict-milieu-award-2016-met-bestdriver-app

40 Bahara, H. 'De smartphone op je hielen. De politie in beeld'. *De Groene Amsterdammer*, 22 July 2015. Retrieved from https://www.groene.nl/ artikel/de-smartphone-op-je-hielen; Naafs, S. 'De muren hebben sensoren'. *De Groene Amsterdammer*, 6 December 2017. Retrieved from https://www.groene.nl/artikel/de-muren-hebben-sensoren; Thijssen, W. 'Nieuwe beelden opgedoken van politiearrestatie van Mitch Henriquez'. *De Volkskrant*, 13 November 2017. Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/nieuwe-beelden-opgedoken-van- politiearrestatie-van-mitch-henriquez~bbf8640f/

41 Visser, J. 'Wat ging er mis in het Zuiderpark?'. *De Volkskrant*, 29 June 2015. Retrieved from https://www.volkskrant.nl/nieuws-achtergrond/wat-ging-er-mis-in-het-zuiderpark-~b9a223d0/

42 For more information about this case, see 'De zaak Mitch Henriquez'. *De Rechtspraak*, 14 August 2018. Retrieved from https://www.rechtspraak.nl/Uitspraken-en-nieuws/Bekende-rechtszaken/mitch-henriquez

43 Witteman, J. 'Wanneer schendt een drone uw privacy?'. *De Volkskrant*, 7 June 2017. Retrieved from https://www.volkskrant.nl/cultuur-media/wanneer-schendt-een-drone-uw-privacy-~b91d9c53/

44 'Little big brothers are watching you'. Rathenau Instituut, 10 October 2017. Retrieved from https://www.rathenau.nl/nl/digitale-samenleving/little-big-brothers-are-watching-you

45 Boere, R. 'Wegpiraten steeds vaker gepakt dankzij dashcam weggebruiker'. *Algemeen Dagblad*, 3 April 2017. Retrieved from https://www.ad.nl/binnenland/wegpiraten-steeds-vaker-gepakt-dankzij-dashcam-weggebruiker~a7aeef60/

break-ins. The ‘HomeWatch’ system available from Interpolis insurance company, for example, consists of a sensor system with a smart camera and door and window sensors. When the occupants are not at home and the sensor detects a movement at the door, it automatically transmits an alert to their mobile phone. If the movement turns out to be the postman or the wind blowing, then no action is required. But if the camera reveals a potential intruder, the occupant can use an app to ask friends or neighbours or a professional security firm for help.[46] A WhatsApp neighbourhood crime watch group allows local residents to alert one another to irregularities in the neighbourhood, for example by sharing photos of suspicious persons.[47]

4. Self-surveillance
People can also use devices and applications with digital sensors that help them follow the rules meant to ensure security and quality of life, for example the ANWB motoring organisation’s ‘Fair Insurance’ and ‘Safe Driving’ apps. Sensors keep track of the insured’s driving behaviour and those who drive safely are given a discount on their car insurance. The idea is that this will improve road safety.

While this particular sensor technology system lets users decide what to do with the feedback, other applications apply filters to improve safety. Examples include ASR’s ‘Drive Safe’ or KPN’s Safe Lock, both apps that block WhatsApp and other message systems while the user is cycling or driving.

3.5 Sensor technology

Not only are the number and type of sensors changing, but their users are changing as well. In the late 1990s, sensor data consisted mainly of video images from surveillance cameras on the streets.[48] Today, the police are experimenting with face-recognition cameras and anti-jamming sensors. Only specialist police teams are using these innovative technologies at the moment, but they are nevertheless developing in three different ways: they are becoming more elaborate, more mobile and smarter.

46 ‘Abonnement Interpolis ThuisWacht’. Interpolis, 4 October 2018. Retrieved from https://www.interpolis.nl/verzekeren/slimme-oplossingen/thuiswacht/productbeschrijving
47 ‘Wat is WABP?’. WhatsApp Buurt Preventie, 6 December 2018. Retrieved from https://wabp.nl/nl/wat-wabp
48 We described the evolution of camera surveillance from the 1990s to 2011 in Van ‘t Hof, C., R. Van Est & F. Daemen (red.) (2011). *Check In / Check Uit. De digitalisering van de openbare ruimte*. Rotterdam / Den Haag: NAi Uitgevers / Rathenau Instituut, pp. 75-133.

More elaborate

Traditional imaging cameras and microphones can ‘see’ and ‘hear’ but digital sensors are more elaborate and have in fact digitised all our senses in that they can also ‘smell’, ‘taste’ and ‘feel’. Digital sensors can often perceive more than people can, for example detect the presence of metal and read DNA for forensic analysis.[49] The police are also studying the use of digital sensors that can track smartphones through Wi-Fi signals (‘Wi-Fi sniffing’).[50]

More mobile

The Dutch national police force installed cameras in police cars for the first time in 1975.[51] Since then, digital sensors have shrunk in size. These days, there are even nanosensors, such as the ‘e-noses’ used in the Port of Rotterdam to detect unhealthy air and hazardous gases.[52] As a result, digital sensors have become more mobile. They are found in smartphones, they can be worn on the body (for example smartwatches and smartglasses), and they can be controlled remotely. Body-worn video cameras or ‘body cams’ are attached to the police officer’s uniform, giving the officer a second pair of eyes and ears in the incident room. The first police body cams in the Netherlands were used by Maastricht’s local police force in 2008.[53] Hundreds are now in use, albeit still experimentally.[54] The police also use helicopters and drones equipped with various sensors, such as thermal-imaging cameras to identify cannabis plantations and high-definition cameras that can take ultra-sharp images of large areas of land.[55]

Smarter

An example of a ‘smart’ camera is one that can recognise faces. It not only records video images but, for example, can potentially recognise the faces of football hooligans in those images.[56] Another example is automatic number plate recognition or ANPR. The software in this camera can read car number plates and

---

49 See for example: Kamerstukken II 2015/2016, 29 628, no. 594 and appendices ‘Visie op sensing’ and ‘Beleidsvisie sensing’; Engberts, B. & F. Copini (2016). ‘Sensing door de politie en publiek-private samenwerking: operationele noodzaak’. *Het Tijdschrift voor de Politie* 78, no. 7/16, pp. 18-22. Retrieved from https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2015Z22421&did=2015D45494

50 Idem.

51 Flight, S. (2016). ‘Politie en beeldtechnologie: gebruik, opbrengsten en uitdagingen’. *Justitiele verkenningen* 42, no.3, pp. 68-94.

52 ‘Verkenning van toepassingsmogelijkheden’. Twente: Universiteit Twente. Retrieved from https://www.utwente.nl/en/bms/steps/staff/nanotechnologie-in-dienst-van-veiligheid-en-justitie-2016.pdf

53 Flight, S. (2016). ‘Politie en beeldtechnologie: gebruik, opbrengsten en uitdagingen’. *Justitiele verkenningen* 42, no.3, pp. 68-94.

54 De Leeuw, P. & I. Nap (2018). ‘Programma Sensing. Concept programmaplan 2018-2019’. Draft, version 2.0, 19 February 2018.

55 Wide Area Motion Imagery (WAMI) is explained on pp. 75-77 of Politieacademie (2018). *Kennis voor de politie van morgen. Een conferentie over onderzoek bij, naar en voor de politie.* Den Haag: Sdu uitgevers.

56 Van Gelder, H., ‘Politie gaat hooligans pakken met slimme bril’. *Algemeen Dagblad*, 3 September 2015. Retrieved from https://www.gelderlander.nl/binnenland/politie-gaat-hooligans-pakken-met-slimme-bril~a180de4d

compare them with those in a database. The police are also currently testing smart video cameras that can detect motorists who are making phone calls or using an app while driving.[57]

3.6 Conclusion

In this chapter, we described the sensor data value chain and identified five trends in the use of sensors to improve security and quality of life:

1. There are more and more police sensors producing a growing amount of sensor data.
2. The police are automating some of their core activities (witness, investigate and enforce) using smart sensor technology.
3. Private citizens, businesses and local government are collecting growing volumes of sensor data.
4. The police are seeking new forms of cooperation that will allow them to use sensor data collected by the public to improve security and quality of life.
5. Private citizens and other private parties are undertaking investigation and enforcement themselves using sensor data.

Sensor data are used by public parties (the police and local government), private parties (private citizens and businesses), and in public-private partnerships. Individuals are not only monitored by the police and other bodies (surveillance), but they also use cameras themselves in various ways (sousveillance, horizontal surveillance and self-surveillance). Both public and private parties can collect and analyse sensor data and then take action, but these processes can also take place automatically (at least in part). In the following chapter, we look more closely at the form that these various practices take.

57 'ANPR'. Dutch national police force, 5 December 2018. Retrieved from https://www.politie.nl/themas/anpr.html; 'Politie test camera die appende automobilist filmt'. Nu.nl, 13 March 2018. Retrieved from https://www.nu.nl/binnenland/5175332/politie-test-camera- appende-automobilist-filmt.html?redirect=1

Intermezzo: roving bandits

In the southern Dutch town of Roermond, knowledge institutions, businesses and local government are cooperating with police to crack down on roving bands of criminals. There, sensors and big data analysis are leading to smarter policing here. Juliette Anker, police intelligence specialist, talks about the experiment.[58]

Figure 4 Automatic Number Plate Recognition.

An ANPR system photographs a number plate, normalises it for brightness and contrast, and segments the characters to prepare them for OCR.
Source: https://commons.wikimedia.org/w/index.php?curid=565899

Designer Outlet Roermond

The town of Roermond's main attraction is the Designer Outlet, which opened in 2001. The outdoor shopping mall attracts more than ten million visitors a year. 'That's good news for the town,' says Juliette. Tourists and day trippers come from

58 The officer's real name has been changed to protect her identity.

all over. But in addition to the well-intentioned shoppers, the Outlet also appeals to the less well-intentioned, such as shoplifters and pickpockets.

The police analysed which groups of visitors are most often associated with pickpocketing and shoplifting. ‘A simple analysis of crime report patterns reveals where they come from. We see perpetrators from the Netherlands, of course, but a striking number come from Bulgaria, Poland and Romania. Many of them have no fixed abode, and so we can categorise this type of crime as “mobile banditry”.’ The police then coordinated with Roermond’s local government to set up a ‘sensing’ programme that uses smart technology to cut down on such crime.

Tracking with sensors and adding up points

Based on a review of the literature examining mobile banditry in Europe, the police’s operational findings on the street, and other data, analysts compiled a profile of potential perpetrators. The profile answers such questions as:

- Who are they?
- How old are they?
- What cars do they tend to drive?
- What is their country of origin?
- What times of the day are they active?

The profile consists of a set of more than ten knowledge rules describing the perpetrators’ attributes. The rules are used to programme the sensors so that they match on-street observations with the profile. In this phase, the most-used sensor is the ANPR sensor, which can identify whether a passing car’s number plate is Lithuanian, Bulgarian, German or Dutch. The number plates observed by the ANPR sensors are then fed into the database of the Netherlands Vehicle Authority (Road Transport Unit) to retrieve additional information about the vehicle.

Ultimately, the purpose of the system is to identify suspicious circumstances on the streets. Every knowledge rule is assigned a point based on a sensor match. The points are added up to produce a score. Beyond a certain score, the circumstances are considered suspicious.

Follow-up on the streets

In the event of suspicious circumstances, the programme sends an automatic alert to the Operational Centre, which instructs the officers on duty. ‘The OC then orders the Roermond policing team to check whether their real-time observations match what the technology has reported.’ The officers then attempt to intercept the car and question the passengers. Those with malicious intentions often cut their losses after speaking to police officers and immediately leave Roermond. ‘And that’s just what we want,’ Anker says. ‘A potential crime has been prevented and that’s what this living lab is all about.’ At the time of this interview (spring 2019), the system

was still being trialled. ‘We’ll soon be going operational, with operational instructions being issued to officers on the streets. We’ve been testing the system for three months now, and there were between eight and fifteen alerts a day.’

Data analysis makes it possible to examine whether the metadata show any irregular patterns. For example, a pattern showing a car travelling at a certain time and in a certain direction may be indicative of a mobile bandit. Observed patterns of movements and behaviours can help to finetune the perpetrator profile. Throughout the trial period, the basic idea was that the system had to be dynamic, not rigid. ‘If it turns out that you aren’t stopping the right people, you have to figure out why and make adjustments, for example by editing or deleting certain knowledge rules. What we don’t want is to pull people over who aren’t in our target group. We have to keep that to an absolute minimum.’

No gut feeling

One of the risks associated with such a project is the stigmatisation of certain groups. Anker, however, argues that the system eliminates going on a ‘gut feeling’ and that the analysts always look at the data with an open mind. ‘We compare our observations on site and in the Outlet to the demographics. Certain groups originating in the countries I mentioned simply stick out.’

Anker wants as few false positives as possible. The system must be reliable and effective. ‘We want to prevent theft, and we want to see hard evidence that we’re doing just that. We have an objective measure, and that’s the number of shoplifting and pickpocketing cases in Roermond’s shopping district.’

Cooperation

The police force cooperated closely in this project with researchers at Eindhoven University of Technology and at the Brightlands Smart Service Campus in Heerlen, where universities, government and private parties (e.g. businesses and start-ups) work together on digitisation, technology and data science. ‘It took a little time to get used to it at first, because we were operating outside our comfort zone as police officers. It’s all fine and well to have an interesting research proposition, but we can’t just share all our operational data.’ The system is attracting attention abroad as well. The German police force, for example, is very interested and Anker says they are amazed at what the Netherlands allows in this regard. ‘German privacy law is a lot stricter.’

Transparancy

Transparent algorithms and knowledge rules are points of concern for the police. They cannot always be transparent about them and their research because any information about how an algorithm functions can, in fact, help criminals to

circumvent sensor surveillance systems. Generally speaking, the police work with protocols and rules, for example to account for the use of force. However, this experiment involves a dynamic system that is undergoing continuous development. The initial knowledge rules emerging from the analysis do not offer any absolute guarantee. ‘It’s not guesswork when we introduce a knowledge rule, but if the rule turns out to be flawed in everyday practice, then it has to be edited.’

4 What do people think of sensors? A conceptual framework

4.1 Introduction

When full-body security scanners were introduced at Schiphol Airport ten years ago, a fuss ensued about 'scanners that show you naked'. Journalists and opinion-makers raised questions. Was it not going too far to ask passengers to 'expose' themselves in the scanner? Could they trust security staff to handle the image data with due care? Could they be absolutely certain that the scanners were not harmful to health? Were scanners even the right weapon in the fight against terrorism?

These questions highlight factors – for example personal data protection and impact on health – that may influence whether or not the public regards the use of sensors as acceptable. In this chapter, we examine these factors based on our literature review. We introduce a conceptual framework for this purpose that organises the factors logically and helps us to assemble our focus groups.[59]

Our basic premise is: someone (a subject) has an opinion about something (an object). In other words, a private citizen finds a sensor application acceptable or unacceptable. The subject and the object of that opinion is the first level of our conceptual framework.

4.2 Survey of factors identified in research

There have been few (recent) empirical studies in the Netherlands addressing the public's wishes, concerns and attitudes concerning the use of sensor data to improve security and quality of life. Research by Koops and Vedder (2001) and Dinev et al. (2005) shows that people are more inclined to tolerate privacy-sensitive interventions to solve serious crimes as opposed to petty offences. The public also looks more favourably on retrieving camera footage than on wiretapping phones or conducting a search of someone's house.[60] People find it important to know how

59 Much of this chapter is based on two articles published within the context of this study, Biesiot et al. (2018) and Biesiot et al. (2019). They provide a more detailed description of the conceptual framework and can be found at www.rathenau.nl.

60 Koops, E.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. Den Haag: Sdu Uitgevers; Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government

and for what purpose their information is being used. They see the police as more trustworthy than private security firms.[61]

The studies show that, as the public grows more open-minded about information-sharing, it is also increasingly accepting of the use of sensors for surveillance purposes.[62] One study also reveals that gender can influence perceptions: men are more likely to consider the party that is using the sensor (such as the police or a private security firm) important, whereas for women it is the purpose of the investigation.[63] Whether the sensor application is effective is scarcely relevant.[64] People are concerned about the amount of personal information being collected and the purpose for which sensor data are used, but they are seemingly less worried about whether the technology actually does what it is supposed to do.

Every year, Capgemini investigates Dutch attitudes towards trends in the security domain. Figures from its publication *Trends in veiligheid 2018* (Trends in security 2018) show that 58% of the Dutch feel safe or very safe and comfortable with the growing number of cameras in public spaces, while 9% say they feel the opposite.[65] Capgemini also asks people how they feel about the use of sensors to increase safety. Seventy-eight percent of the respondents have a positive or very positive opinion of police body cams and 6% have a negative or very negative opinion.[66] The survey does not examine the arguments and reasons behind the respondents' views.

Unlike the Netherlands, other countries offer multiple recent examples of studies examining public attitudes towards sensor applications.[67] Their relevance to our research is limited by their emphasis on privacy and, in many cases, by their American context. However, the European SurPRISE study is of particular interest

---

Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

61 Schildmeijer, R., C. Samson & H. Koot (2005). *Burgers en hun privacy: opinie onder burgers.* Amsterdam: TNS NIPO Consult.

62 Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

63 Koops, E.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. Den Haag: Sdu Uitgevers.

64 Idem.

65 Hoorweg, E. et al. (2018). *Vertrouwen en wantrouwen in de digitale samenleving. Trends in veiligheid 2018*. Utrecht: Capgemini, p. 4. Retrieved from https://www.capgemini.com/nl-nl/bronnen/visierapport-trends-in-veiligheid-2018/

66 Idem, p. 38.

67 See for example Potoglou, D. et al. (2017). 'Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study'. *Computers in Human Behaviour* 75, pp. 811-825; Rainie, L. M. Duggan. (2016). 'Privacy and information sharing'. Pew Research Center. Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/; Madden, M. L. Rainie. 'Americans' Attitudes About Privacy, Security and Surveillance'. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance

to the question we are investigating. This study surveys factors that may play a role in whether or not the public deems a sensor application acceptable.

SurPRISE is a large-scale research project that examined public acceptance of 'Surveillance-Orientated Security Technologies' (SOSTs).[68] The study was carried out in nine European countries. Between 2012 and 2015, researchers conducted a quantitative and qualitative study of public acceptance of SOSTs in Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom. Among other technologies, the study covered (smart) CCTV, biometric identification systems, drones, smartphone location tracking and deep packet inspection (far-reaching analysis of electronic data transmission). Two thousand people (approximately 200 per country) were interviewed and attended the related participatory events ('Citizen Summits'). Based on an in-depth literature review, the SurPRISE researchers identified thirty factors thought to affect public acceptance of SOSTs, which they then tested empirically.[69]

The SurPRISE study identified seven factors that have a significant impact on people's attitudes towards sensor technologies used for surveillance purposes:

- **General attitude towards surveillance-orientated security technologies:** The more people approve of technology to improve security, the more likely they are to find sensor technologies acceptable. Conversely, the less they approve, the less likely they are to accept sensor technologies.
- **Institutional trustworthiness:** Perceiving institutions as trustworthy makes people more likely to find sensor technologies acceptable. Using more acceptable technologies also helps institutions appear more trustworthy.
- **Social proximity:** The more people perceive sensor technologies to be targeted at specific others (such as suspects and criminals), the more acceptable they find them compared with blanket surveillance technologies.
- **Perceived intrusiveness:** The more people perceive technologies as intruding into their personal or everyday life, the less likely they are to find them acceptable.
- **Perceived effectiveness:** The more people perceive sensor technologies to be effective, the more likely they are to find them acceptable.

68 Pavone, V., E. Santiago & S. Degli-Esposti (2015). SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe. Retrieved from http://surprise-project.eu/wp- content/uploads/2015/02/SurPRISE-D24-Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs-c.pdf

69 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*, p. 77.

- **Substantial privacy concerns:** The more people are concerned about their personal data and physical integrity, the less likely they are to find sensor technologies acceptable.
- **Age:** Older people are more likely than younger people to accept sensor technologies.

Note that people do not necessarily always realise that these factors are influencing their opinions, feelings and attitudes.[70] Nuances aside, the study further identifies seven other factors that have only a minor or indirect influence on public acceptance of sensor technologies.[71] The factors 'Perceived level of security threat' and 'Familiarity with SOSTs' were found to have no significant influence. The same was true of 'Income', 'Education', 'Spatial proximity', 'Temporal proximity' and 'Trade-off between privacy and security'.

SurPRISE also revealed which conditions or 'rules' the public wants to see implemented to make the use of sensors more acceptable. These rules indicate what people consider important in sensor surveillance. During the Citizen Summits organised by the SurPRISE researchers, the participants recommended criteria and put forward arguments underpinning their opinions and feelings about sensor technologies. People find the SOSTs covered by the SurPRISE study more acceptable if:

- they are operated within a European regulatory framework and under the control of a European regulatory body;
- they are operated in a context where there is transparency about the procedures in connection with data protection and accountability;
- they are operated only by public authorities and only for public benefit; any participation by private parties must be strictly regulated;
- their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives;
- their operation can be regulated through an opt-in approach;
- they allow monitored individuals to access, modify and delete data about themselves;
- they overwhelmingly target non-personal data and public places, in line with criteria and purposes known to the public;
- they do not operate blanket surveillance but address specific targets, at specific times, in specific places, and for specific purposes;
- they incorporate privacy-by-design protocols and mechanisms;

70 Idem, p. 80

71 Pavone, V., E. Santiago & S. Degli-Esposti (2015). *SurPRISE. Surveillance, Privacy and Security: Final publishable summary report*, p. 6.

- they work and are operated in combination with non-technological measures and social strategies addressing the social and economic causes of unsafe circumstances.

These rules mainly concern practices and actors, i.e. the way in which sensors are applied in real-life situations, by whom and for what purposes. Nevertheless, the public also makes demands on the technology itself and the institutional context. People want sensor technology to be designed in a way that excludes privacy issues from the outset, for example by minimising data storage, anonymising personal data and encrypting all information. Privacy-by-design principles can also be incorporated into the procedures for using sensor technology, for example agreeing to minimise the number of people who have access to data. The public also finds the broader institutional context important: the technology must comply with the overarching framework of European rules and regulatory mechanisms. This implies that the public has faith in those rules and trusts that they are monitored properly.

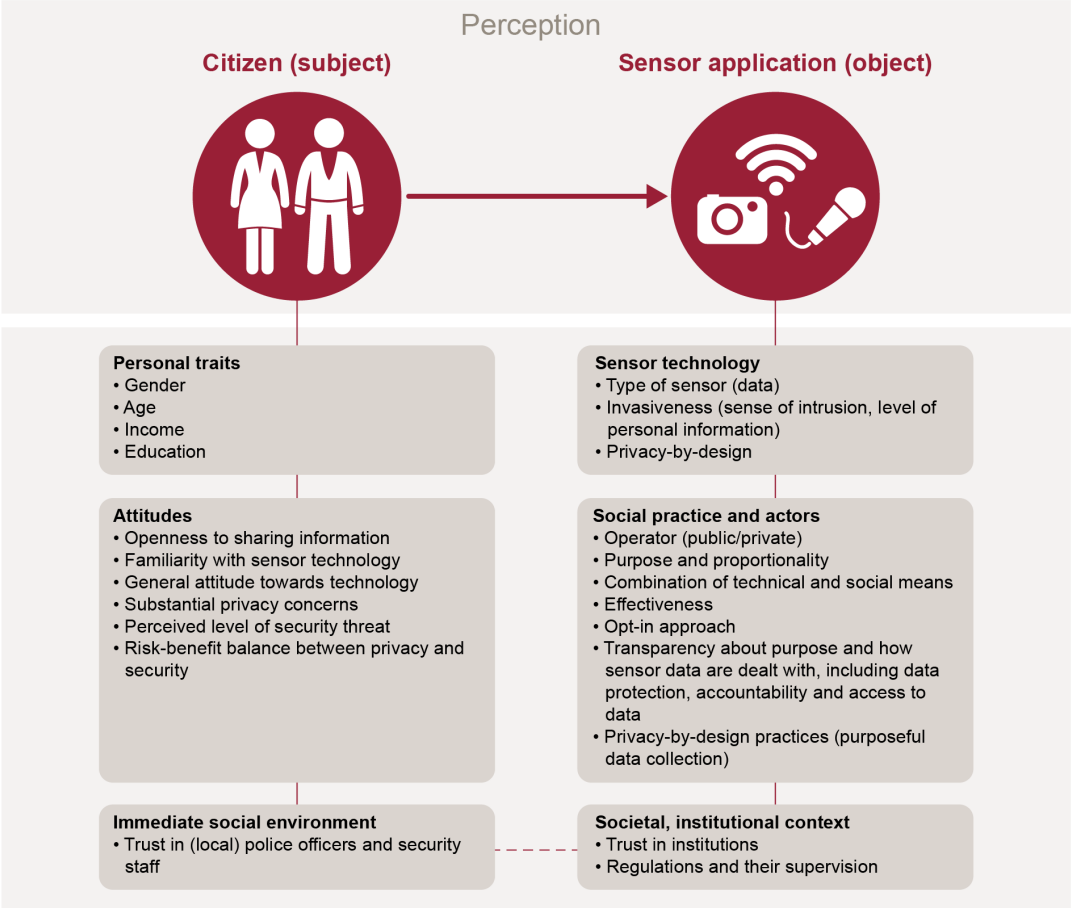
4.3 Conceptual framework

We have sorted the factors from Dutch research and the European SurPRISE study into a conceptual framework. Figure 7 reviews factors taken from research that may affect public perceptions of surveillance using sensors.

Our basic premise is: someone (a subject) has an opinion about something (an object). In other words, a private citizen finds a sensor application acceptable or unacceptable. The subject and the object of that opinion are the first level of our conceptual framework. At the second level, we differentiate between three dimensions on either side. Whether or not people find a sensor application acceptable may depend on their own, individual traits (is someone open to sharing information?) and on the features of the relevant sensor application (what sort of information is it collecting?).

The private citizen: three dimensions
Personal dimensions influence the way in which a private citizen (the subject) perceives a sensor application. Our literature review shows that personal traits (such as gender) and attitudes (such as being open to sharing information) play a role in how people perceive sensor applications. Their immediate social environment also influences their perceptions, such as the neighbourhood in which they live.

Figure 5 Conceptual framework of factors that may affect public perception



Source: Rathenau Instituut

Sensor applications: three dimensions

We also identify three dimensions of sensor applications (the object) that influence perceptions of sensors:

1. Sensor technology: How the sensor technology functions.
2. Social practice and actors: The context in which the technology is applied and the actors involved.
3. Societal and institutional context: The broader societal, cultural and institutional context in which the sensor is being used.

Public perceptions may hinge on any and all of these dimensions.

The first dimension (how the technology functions) concerns the design of the technology and what repercussions this may have, for example for public health or privacy.

The word ‘actors’ in the second dimension refers to all the parties involved in the sensor application. They include the person or organisation collecting the sensor data or the analyst who links and analyses the data. Another actor is the police officer on the street or security officer in the shop who take action. In addition, sensor data can be collected about different people or groups of people, for example everyone walking down the high street or driving past an ANPR camera.

In the third dimension, the societal, cultural and institutional context plays a role in various ways. This dimension may concern laws governing camera surveillance and the extent to which the public generally trusts or mistrusts the authorities.

In real-life situations, the three dimensions are interrelated. The extent to which a sensor application infringes people’s private lives may, for example, be related to the design of the technology itself, but also to the procedures of the specific social practice in which the technology is used.

4.4 Conclusion

By studying and deconstructing the concept of surveillance, we developed a conceptual framework in this chapter that helps us examine the way in which private citizens perceive the use of sensors. Based on real-life examples and research on public perceptions, we identified factors that may play a role in what people think of sensor surveillance. We differentiate between three personal dimensions and three dimensions of sensor applications; all these dimensions can affect people’s attitudes.

1. Sensor technology. How the sensor technology functions
2. Social practice and actors. The social practice in which the technology is applied and the actors involved.
3. Societal and institutional context. The broader societal, cultural and institutional context in which the sensor is being used.

We have used these dimensions in our study both to assemble our focus groups and to analyse the outcomes of their discussions. In the next chapter, we report in detail on the focus groups and, with the help of quotes, discuss the opinions, considerations, concerns, wishes and feelings of private citizens concerning sensor technology. In Chapter 6 we analyse the focus groups, once again turning to the conceptual framework for support.

Intermezzo: spotting villains

Jaime van Gastel scans high streets looking for people who are acting suspiciously. ‘When I scan the public, I can immediately spot things that don’t look quite right. And then I start following the person in question.’ In the event of criminal behaviour, he calls the police pickpocketing team and waits for them to arrest the suspects. He videos the crime and the arrest and uploads it to his YouTube channel. We accompanied Jaime on one of his outings. ‘For me, this is active relaxation – like jogging or going to a club. It gives me a kick.’

Source: Rathenau Instituut

The use of cameras and sensors to improve quality of life and security is not confined to government and the business community. Private citizens use them too, to keep an eye on one another. In fact, more and more people are using their smartphones to investigate crime and, in some cases, even enforce the law. This is referred to as ‘horizontal surveillance’. Jaime van Gastel (46) has made horizontal surveillance into a hobby. He has his own YouTube channel, under the name ‘Boevenspotter’ (‘Villain-Spotter’).

In his spare time, he travels to places where pickpockets are known to be active. He scans the streets for people behaving suspiciously, follows them, calls the Amsterdam police's pickpocketing team and waits for officers to make an arrest. He videos the entire escapade and uploads the results to his YouTube channel. 'My point is to make people aware of how pickpockets operate so that they can avoid becoming victims.'

More than 60,000 people subscribe to Van Gastel's channel and some of his videos have had more than a million views. By his own estimate, he has caught about 1,200 pickpockets. We accompanied him one afternoon around Amsterdam, his favourite 'villain-spotting' location. His tactics resemble those of a hunting dog: he watches, weaves back and forth constantly, or stands on a bench looking out for potential criminals.

Talent discovered in a clothing shop

Van Gastel hit upon the idea of spotting villains 24 years ago when he worked in a clothing shop. 'I was given a police phone number and asked to report suspicious behaviour. I started keeping an eye out in the shop and after a month I could spot shoplifters and pickpockets as soon as they came in the door. The police said to me, "That's a gift, you should make use of it".'

From that time forward, Van Gastel has made a hobby out of spotting pickpockets in Amsterdam. He goes to pickpocket 'hotspots' in the city once or twice a week. 'For me, this is active relaxation – like jogging or going to a club. It gives me a kick because my mind is so focused.'

Watch behaviour, not appearance or clothing

Van Gastel relies on his gut instincts to spot pickpockets on the streets. 'In a crowd, there's no time to think about someone's appearance or what they're wearing. When I scan the public, I can immediately spot things that don't look quite right. And then I start following the person in question. I notice certain behaviour, like they're looking around nervously, walking faster than other people in the street, or they suddenly pivot and walk into a shop.'

Van Gastel says that inexperienced spotters look only at appearance, and do so unconsciously. He looks at behaviour. 'I don't look at whether they're male or female, or at their appearance. I'm only interested in their behaviour. These days, pickpockets can be just as trendy and fashionable as anyone else. They blend in better that way.' When Van Gastel notices a suspicious person, he immediately calls the police pickpocketing team, follows the suspect and starts videoing. 'I have to be close enough to catch them steal something. Once they've actually broken the

law, then plainclothes police officers can move in and make the arrest.' Occasionally, he catches pickpockets red-handed.

Vlogging and obscuring subjects

Van Gastel has been videoing his 'villain-spotting' adventures for the past two years. He says that the people who feature in his vlogs are '100% guilty', otherwise he would not upload the video. He puts the video clips online to show viewers how pickpockets operate so that they can avoid becoming victims themselves.

He earns a few hundred euros in advertising from his vlogs. It seems like a nice sum of money, but he spends half of the proceeds on having his videos edited professionally. Using filters to make people unidentifiable is quite expensive. Van Gastel says that the cost factors into whether or not he obscures a suspect's identity.

When he uploaded his first clip online, there were no blurred faces. The police immediately asked him to obscure the plainclothes police officers. They also advised him to obscure the faces of the suspects, since putting videos of them online could result in a reduction in their sentence. Although obscuring the faces of perpetrators is not currently required by law, Van Gastel says that it may become necessary in the future due to EU copyright legislation. It's something he would rather not do. 'I deliberately want to make people aware of how pickpockets operate. The videos show that they signal to each other, and observe other people for minutes at a time. I know that these are professionals.' Another factor is that the videos with obscured faces get fewer views on YouTube.

Van Gastel says that if a suspect were to ask him to take down a video, he would comply immediately. He himself ultimately decides whose features he obscures, allowing for such factors as number of views, the cost of editing and privacy considerations.

Resistance on the streets

Van Gastel's hobby is not without its risks. Pickpockets have been known to recognise him, leading to the occasional threatening situation. He shrugs off being spit upon and yelled at. 'If I minded, I wouldn't do it in the first place. I'm never afraid.'

Referring to a gang of thieves that he filmed at the Designer Outlet in Roermond, he says, 'I know that if I come across them again, they'll assault me.' Van Gastel is in fact no longer welcome at the Designer Outlet because the management was unhappy with what he was doing there. 'I guess they didn't think it was a good advertisement for their shopping centre.'

What does the police pickpocketing team think?
According to a member of the Amsterdam pickpocketing team, ‘We’re very happy with Van Gastel’s work. There are few people who are as talented as he is at spotting pickpockets. We used to have civic patrols and citizen participation projects, but they tended to attract people who went too far and acted as judge and jury. Van Gastel is well aware of the limits. The videos are presented in court to prove pickpocketing. Witnesses can be very useful. After all, the police can’t be everywhere at once. But not everyone is cut out for it. Assaults are not unknown and witnesses have to be absolutely certain that the suspect truly is a pickpocket. Some video recordings have to be rewound and reanalysed ten times before the situation becomes clear.’

The police generally do not look favourably upon online vlogs about suspects because they ‘name and shame’. They would, however, like to work more closely with private citizens such as Van Gastel. Wouldn’t Van Gastel rather join the police force? ‘Of course I’d love to be a member of the pickpocketing team, but the problem with the police is all the rules. There are so many. And a plainclothes officer doesn’t do what I do all day long.’ And so Van Gastel continues to spot pickpockets as a hobby, using his ‘gift’ for the public good.

5 Report on focus group sessions

5.1 Introduction

In the previous chapter, we showed that very few studies have been carried out in the Netherlands addressing its inhabitants' opinions on the use of sensors. To examine the views and arguments of the Dutch on this subject, we undertook focus group research. This chapter reports the results and outlines the main opinions, considerations, concerns, wishes and feelings of the focus group participants. It is not our aim to present a complete record of the focus group sessions but to show the extensiveness of the arguments and considerations. We do not report on each of the six focus group discussions separately, but whenever necessary we do indicate in which of the six groups the discussion took place. Direct quotations are displayed in single quotation marks. The texts of the 'scenes' that were read to the focus groups prior to their discussions are shown in box texts preceding the report on those discussions.

We have divided the reports into four sections corresponding to the four phases of the focus group research. We start with a 'baseline assessment', in which we sketch the participants' initial attitudes towards sensor technology and the police (5.2). We then discuss the results of the focus group discussions addressing the three socio-technical scenarios, i.e. more mobile (5.3), smarter (5.4), and more elaborate (5.5), and describe how the focus group discussions of each scenario unfolded. An analysis of the focus groups can be found in the following chapter.

5.2 Attitudes towards the use of sensors

At the start of the group discussions, the participants were asked what immediately springs to mind upon hearing 'using sensors to improve quality of life and security'. Most participants gave familiar examples: the door of an elevator that opens and closes automatically, 'smoke detectors', or as one respondent said 'I thought of my car. If I drive too close to the pavement, it beeps at me'. Two participants gave a more abstract description of sensors: an 'observation instrument' and a 'measuring device'.

In one group participants gave many examples of using sensors for security purposes: 'detecting hazardous objects', 'video surveillance', 'speed cameras',

‘airport security’ and ‘drones above crowded squares and high-risk urban areas to ensure visitor safety’.

Although most of the responses were descriptive, a number of participants also expressed their opinions. One person said, ‘I feel more comfortable in a place that has detectors than somewhere that doesn’t have them’, and another person commented, ‘but of course it also tracks things that we may not want it to track and that we may not know are being tracked’.

Participants mentioned a number of sensor applications that would be discussed in more detail later, such as ‘smart lampposts’ and ‘facial recognition’. Five of the six groups included security cameras in their lists.

After this discussion, the focus groups were given a definition of sensors.

Box 1 What are sensors?

Sensors are devices that measure and collect input from the physical environment. Examples include cameras, microphones and your smartphone’s GPS receiver. These sensors generate certain data, for example about your location, but they also supply camera images and sound recordings. Today we are discussing the use of sensors to improve quality of life and security. Quality of life refers to minor infractions, such as littering. Security concerns more serious crimes that make people feel unsafe, such as being mugged or threatened with physical violence.

Participants in all the groups mentioned better security as an important reason for using sensors, for example to prevent crime and serious offences (‘mugging’, ‘robbery, ‘murder’, ‘terrorism’ and ‘serious violations’) or to track down the culprits sooner. Some participants made the connection between quality of life and security, for example by stating, ‘Quality of life and security are very closely linked. I don’t feel safe with a bunch of lowlifes walking around’. Participants said that the line between acceptable and unacceptable use of sensors was ‘thin’. Some saw it as a way of tackling littering, while others thought that went too far. They were concerned that the use of sensors would ultimately compromise quality of life: ‘Then people will be uncomfortable going to places [with sensor surveillance].’ Another voiced his concern in the following way: ‘There’s no spontaneity. You’d feel

restricted in your behaviour because you'd feel like you're always being watched. That's not a society I'd want to live in.'

Criticisms
Participants had some criticisms regarding the use of sensors. 'You're not quite yourself walking down the street because you're viewed as a potential suspect.' Participants felt uncomfortable about being monitored. 'I'm all for security, but if every single corner of the street had sensors, I'd feel spied on.'

Several participants cited examples from other countries to describe what they did not like about camera surveillance. One participant had been in Beijing three months before the focus group and said, 'There are cameras on every corner. It was very creepy the first few days, but I got used to it. After a while, I felt safe again'. Others said they felt uncomfortable with heavy camera surveillance on the streets. 'This is the 1984 effect, where you're constantly being watched for all sorts of reasons. But who's watching the watchers?' 'In London and India, cameras are everywhere. I think it cultivates a false sense of security. I think it's better in the Netherlands. When I'm in the Netherlands, I notice that I feel much safer.' Another participant described how vigilant she was in Singapore about not littering because of the strict (camera) surveillance.

'Infringement of privacy' was frequently cited in connection with sensor use: 'It's damaging to privacy.' Participants were worried that security came at the expense of privacy: 'I'm all for security, but it shouldn't be at the expense of [privacy].' Participants asked themselves how data were stored, whether data were anonymised, whether they were adequately protected against hackers, and whether they could themselves access surveillance camera images.

Ambivalence
Most participants saw both the pros and cons of using sensors and indicated that they felt 'ambivalent'. 'When it comes to terrorism, it's useful to be able to track people. But do I really want my data to be used for other purposes, without my knowledge? At some point, they come to know everything about you, like Facebook. Businesses want to know everything about you. Big data is on the rise and everybody wants to profit from it.' Another person mentioned the same feelings of ambivalence, but drew a different conclusion. 'I'm ambivalent about it too, but then I think "I've got nothing to hide, I'm only being filmed". The images will only be used in the event of a serious crime. So why make a big issue out of it?'

Several participants described the problem as a dilemma between security and privacy and identified various factors. A number of them put security first. 'I mean, what if we can guarantee a 2% improvement in security by just filming a few

places?' Another said, 'I'm all for it. Certainly when it comes to security. Privacy law doesn't permit much nowadays, but if you have nothing to hide, you shouldn't mind.'

There were also concerns about the effectiveness of sensor applications. One participant wondered whether the quality of the sensor data was satisfactory, and another said, 'People are still being robbed at ATMs. I don't think it prevents crime'. One participant asked whether there were no better alternatives to monitoring and surveillance. Another noted that it was important to agree on the purposes for which sensor data were being used. 'They shouldn't be used for inappropriate purposes. They start out saying, "We won't do this or that," but then three years later they change all the rules.'

Another of the participants' worries was access to sensors and sensor data. 'Not everyone is allowed to just view and record stuff.' Many participants were critical of sensor data being used by businesses for commercial purposes. 'Government use and the police viewing images after a burglary are fine by me. But I don't want companies to be able to buy my data and track me. That's not okay.' Another participant said it was unethical to sell data to businesses that then get to know you 'better than you know yourself'.

Several participants said that they considered it important to have a choice, and that sensors should not collect data automatically. One participant explained that she had chosen to activate a feature on her phone that would transmit her location and take pictures in the event of an emergency. A number of participants felt that they did not have much influence on the way this technology was being used. 'My feeling is that it's going to happen anyway. Sure, you can do everything in your power to resist, but how?' Another comment: 'I think Facebook and Google already know everything there is to know about us.'

Trust in the police force

Before discussing the scenarios, the moderator asked the participants what they expected of the police force. When do the police do their work properly? Participants thought that it was the police's job to protect the public and to enforce the law. One participant put it this way: 'I see Old Bill as the person who's supposed to keep me safe and who intervenes when something happens.' Another participant cited the motto of the Dutch national police, vigilance and service, and added, 'I think that requires some humanity. Not every offence is a deliberate act, enforcement of the law should be reasonable'.

The participants had varying expectations about how officers should carry out their duties. Some of the participants emphasised that officers should be helpful and approachable. 'On an equal footing, so that you don't feel he's superior to you.

Accessible.' Other participants, however, felt that police officers lacked authority and that they could be tougher on people than they now were. 'I think they lack authority. The police also have an instructive role. That isn't there nowadays.' One participant from the Amersfoort area missed '...the local constable who walked around the village with his baton. Anyone acting up got a bash on the head.' One of his fellow group members continued this line of thought: 'There used to be one constable for a whole village, and that was enough. The mentality has changed completely. People used to respect police officers, just like they respected the clergy'.

In general, participants stated that they 'want to see more cops on the streets'. Some commented that even when there was a visible police presence, officers didn't do enough. 'They're there, but the general consensus is that they hardly do anything. They don't make much of an impression anymore.'

When asked to what extent they trusted the police, participants gave varying responses. Some had a very favourable view of their contact with the police. 'I'm glad they're around. I've needed them on a few occasions and things have always ended well.' Others did not trust the force to follow up on reported crimes. 'If my house were burgled, I wouldn't put much faith in them. I don't think they'd work on solving the crime. Robbery and crimes like that, they're not taken seriously enough.' A few of the participants were critical about police follow-up. 'Nothing. Sorry to say, they do nothing.' Several participants who live in Rotterdam thought there was little point in reporting crimes. 'Everyone in Rotterdam knows it's not worth the effort to report a theft. People don't even bother anymore.'

Participants in different groups felt that police officers focused on the wrong things. 'Handing out tickets for driving three kilometres an hour too fast, and that with the four of them. Go catch some real criminals! But if I get robbed and they come straightaway, then all's well.'

Participants in five of the six focus groups cited workload and staff shortages to explain why the force could not do everything and had to prioritise. 'When I call them, I do expect them to come. But I understand that they're very busy and might be involved in another situation.' Another said, 'I think policing is getting harder. I think the force is being eroded and that needs to be addressed.'

5.3 More mobile

After the introductory round of general impressions, the discussions turned to the various socio-technical scenarios. We began with the ‘more mobile’ scenario, which explored the shift from stationary to mobile camera surveillance.

Box 2 stationary camera surveillance

We see a lot of cameras on the streets. Altogether, local governments and the police force operate about 4,000 security and surveillance cameras in public places. Shops, businesses and private individuals have even more cameras to secure their business premises and homes. The police are keen to access their images when investigating a crime.

Almost all of the participants were content with the police viewing images taken by private cameras to help track down suspects after a crime. ‘I agree completely. There’s a much better chance of catching perpetrators when there are camera images.’ Participants considered it an advantage that cameras helped to track down suspects sooner and that they had a preventive effect. Some said that they had or would like to have their own (dummy) cameras for the same reason.

Participants in all of the groups identified criteria that the police should meet when using camera images. They wanted to know about data security and the purposes for which the camera images would be used.
One participant wondered how long the images were kept and thought it was important to let people know that they were being filmed. Another participant wanted to be asked for explicit consent to be filmed. An opt-in feature appeared to be important for several participants. Several members of one focus group said that the surveillance itself needed to be monitored. ‘The police shouldn’t be allowed to use the images at their own discretion. They should only use them after the fact and with a court order. There should be a guarantee that the police are using them for the right reasons.’ They considered third-party supervision important. ‘Separation of powers is crucial. Those who use the images shouldn’t be deciding whether viewing them is permissible.’

Real-time surveillance with privately owned cameras

Box 3 Live meekijken met camera's van burgers

The police are testing real-time, i.e. live, surveillance using security cameras set up by private citizens. People who live in a neighbourhood in Amersfoort where there have been a lot of break-ins have received money from the local authority to install security cameras. The cameras are trained on places where there is frequent criminal activity. To protect people's privacy, the surroundings are obscured. The police have permission to watch the live camera feed online at agreed hours of the night. They receive an alert when a camera detects movement. It could be a car thief or burglar, but it could also be someone coming home late, or even a fluttering spider web. The police can watch in real time and decide whether they need to intervene.

Opinions were divided regarding the next question, which addressed real-time surveillance using privately owned security cameras. Some of the participants took a decidedly positive view. 'I'd be happy for them to install a security camera at my door. It would only make me feel safer.' And another said, 'If the police respond properly, then I'm all for it. The police are there to protect us, and if the purpose is clear, then I'm prepared to sacrifice a lot to ensure my safety. You can't argue that we're sacrificing privacy, given how little it even exists nowadays. If we want the police to do their job then we have be willing to compromise on almost everything else.'

Most of the participants had no issue with the police monitoring privately owned cameras in this case, but they did mention a number of conditions that should be met. The cameras should be properly secured, the objective should be clear, and irrelevant images should be obscured (blurred). Several participants also wanted the cameras to be removed once the purpose of placing them had been achieved. Participants wondered whether the costs were proportional and whether police capacity was adequate to the task. 'How many officers would be detailed to view the camera images? We don't have enough officers on patrol as it is, and then you stick a bunch of them behind cameras?' Some participants worried that the cameras would get 'too close'. One wanted to know for sure that cameras wouldn't be filming indoors. Another thought it would be better not to train the cameras on

private homes but on public spots. ‘I don’t want everyone to know what time I get home.’ Several participants found the set-up acceptable as long as they had opt-in consent.

Participants again mentioned police follow-up of crimes captured on camera as an important proviso. ‘If they don’t do anything, what’s the point?’ Two other participants thought it was a bad idea, because criminals would simply move to neighbourhoods without camera surveillance or strike at times when the police were not watching in real time.

Security firms

The moderator then asked what participants thought about having a private security firm watch the live camera feed, instead of the police. Across all groups, most of the participants had a generally negative view of real-time surveillance by security firms. ‘That’s going too far.’ ‘They sell all the data for cash.’ Several participants worried that a firm’s commercial interests would override their own. One participant argued that security firms benefitted when safety was at risk. ‘Anything for a profit.’ Following on from this, participants cited various reasons for criticising real-time surveillance by security firms. For example, they claimed that they were subject to fewer rules than the police, and that police staff were more likely to be held accountable and that they swore an oath.

A number of participants welcomed cooperation with private firms, under certain conditions. For example, one said, ‘It doesn’t have to be the police. It can also be a private firm. But subject to firm agreements.’ One participant, who works for a fire protection company, noted that he trusted security firms just as much as the police. ‘Of course. It’s their core business, after all. If it gets out that they’re doing something wrong, then their reputation will suffer and they’ll definitely feel it in their revenue.’ And a few participants thought that security firms actually worked faster and better because they could ‘focus more on scanning video images’.

Surveillance with bodycams

Box 4 Surveillance with bodycams

Mobile cameras are also used as surveillance devices nowadays. The police are currently testing ‘body cams’, video cameras that they attach to their uniforms. The officers decide for themselves when to turn on the camera and what to record. The body cam is meant to observe people’s behaviour and how officers and the public act towards one another. The purpose is to prevent aggression and to help the force investigate and collect evidence.

The moderator asked what participants thought about being filmed on the street by an officer wearing a body cam. Hardly anyone was opposed, provided that the surveillance was subject to specific conditions. The most frequently cited was that officers should not decide for themselves when to turn the body cam on or off. As someone explained, ‘The police face a lot of aggression. They can hardly make a move without telephones getting shoved in their faces. So I think it’s a good idea to show both sides, but in that case, it’s important to record the whole story.’ Another said that it felt like being ‘spied on’, but that ‘the end justifies the means’.

Various participants felt that the context was important. A number of them said they would feel uncomfortable if body cams got ‘too close’. ‘It’s one thing to record a passer-by with your camera, but another thing to follow that person home.’

Other organisations using body cams

The moderator asked the participants how they felt about Dutch Railways security staff wearing body cams. Virtually all of the participants approved of this. They felt it would help to identify fare dodgers and improve the chances of their being caught. Participants believed that wearing body cams would also discourage crime. The purpose appeared to be the deciding factor here. ‘It’s for your own protection. And in that sense, I think it should be allowed.’ Another group reasoned that people took the train voluntarily. ‘No one’s forcing me to get on a train.’

When the moderator asked them how they viewed body cams on pizza delivery drivers, the participants were extremely negative. ‘They show up at the door and start filming? Unnecessary.’ None of the focus groups had a single participant who thought that putting body cams on pizza delivery drivers was a good way to improve

security. The participants also argued that, unlike the police and railway staff, pizza delivery drivers did not belong to an official entity and were not trained to deal with the responsibility, that there were commercial interests involved, that they did not know what happened to the data collected, and that they did not trust pizza delivery drivers to deal discretely with the images.

Another factor was that pizza delivery drivers came to people's homes. 'They show up at your front door. And start filming inside without permission.' 'You might just open the door wearing pyjamas. It's too intrusive.' 'No video recordings indoors, on private property. Record all you want in public, but not inside.'

Horizontal surveillance

Box 5 Horizontal surveillance

Private citizens also have mobile cameras, i.e. on their smartphones. They can use them to record burglars or suspicious individuals walking around the neighbourhood, and then post the images in a local WhatsApp group or on Facebook, asking if someone recognises them. The person they have photographed or filmed is often identifiable.

The final question in this scenario was: What do participants think about private citizens videoing suspicious or hazardous situations with their mobile phones? Participants asked for more details, for example, 'What do you mean by suspicious?' and 'What will happen to the images?' In each of the groups, several of the participants criticised the idea of posting images online. They worried about private citizens playing judge and jury and naming-and-shaming others (unfairly). 'Photos and videos should be taken to the police,' was the assertion. Participants recounted anecdotes in which persons were 'intentionally' treated unfairly when someone shared images of them online. The images could continue to 'resurface' for many years.

Participants also objected to horizontal surveillance of this kind on the grounds that private citizens were not professionals. Press photographers were subject to rules, as were police officers, who received training and had to swear an oath. That was not the case for private citizens.

There were also participants who accepted or did not object to suspicious or hazardous situations being recorded. ‘If I came across something that I thought was unacceptable, then I might record it to prove that someone else had been wronged.’ Some participants thought it was fine to then share the images online. ‘Why not, if someone’s doing something wrong?’ They add, however, that the person posting the images online had to be absolutely sure of their claim. ‘It’s okay if you have footage of someone beating another person up, but not of someone who just walks funny.’ Another participant: ‘If it’s only a hunch, then they shouldn’t.’ Two participants thought that people increasingly played judge and jury themselves because they did not trust the police to solve the crime for them. ‘I think people do it if they’re one of those sixteen thousand [unsolved] cases.’

5.4 Smarter

The second scenario is about ‘smarter’ sensors. The emphasis is on the software that analyses sensor data and permits automatic recognition or automated responses. Four of the focus groups discussed this scenario.

Box 6 Automatic facial recognition (1)

One well-known example of automatic facial recognition is on Facebook. If you post a photograph of someone on your Facebook page, Facebook tags that person by comparing the new photograph with other photographs you posted and tagged earlier. You can then confirm whether or not the new photograph is of that person.
Facial recognition may also be a feature of surveillance cameras. In that case, the software compares the live images with the images stored in a database.

Schiphol Airport is testing an automatic facial recognition system. Once the system has stored an image of a passenger’s face in its database, the passenger can check in without producing their passport. To do so, they pass through a special security checkpoint that has a camera equipped

---

with facial recognition software. The system is meant to speed up security checks and shorten waiting times.

Most of the participants had a positive attitude towards using cameras with automatic facial recognition at Schiphol Airport. Some participants agreed with the advantages cited. ‘Things move faster.’ Another said, ‘Cuts down on waiting.’ Participants also said that automatic facial recognition relieved staff of some of their workload and helped in the fight against drug-related crime and terrorism. Another felt it was comforting to ‘know that everyone gets checked’.

Two participants asserted that devices were more reliable than people. ‘The devices don’t get tired. They look at more than the name. Devices make fewer mistakes than people.’ Another participant explained why, in her opinion, a camera with facial recognition was more accurate than human judgement. ‘I have more faith in [a camera with facial recognition] than in human judgement. I didn’t understand why they were asking some of the questions they asked me at the airport. It felt like the man behind the counter was interrogating me.’ Another person in the same group commented that algorithms may also contain errors.

One participant contemplated the purposes for which automatic facial recognition would be used. ‘Depends on the purpose. I think it’s fine for checking in to flights, but it should only be used for that, and not be linked to other purposes.’ Finally, some participants mentioned being worried about infringements of privacy, citing the risk of data abuse or a data hack.

Cameras with automatic facial recognition (2): The police force

Box 7 Automatic facial recognition (2)

The police force could also use cameras with automatic facial recognition. By recording passers-by in a retail zone and having software compare these to images in a database, the police can detect known shoplifters and pickpockets or other known suspects and decide whether to take action on that basis.

The moderator asked the participants how they would feel if law enforcement filmed them on the street using cameras with automatic facial recognition. Participants were more critical of this than the Schiphol Airport example. One participant who had disapproved of facial recognition at the airport was equally opposed to its use by law enforcement. ‘I’ve got nothing to hide, but maybe I’m with someone and then the spotlight’s on me for no reason.’

Another participant worried that smart cameras would eventually be used for other purposes. ‘Pretty soon they’ll be using it to pick out the people who travel abroad a lot. Datasets are getting bigger all the time. Some things that weren’t crimes a hundred years ago will be made criminal again. All it takes is a different line of reasoning.’

Other criticisms were also raised. The first was the concern of being tracked for no good reason. ‘Even shoplifters aren’t *always* shoplifting. Why keep an eye on them when they aren’t?’ Second, participants were sceptical about how consent would be obtained. One participant referred to the General Data Protection Regulation (GDPR) and wondered how people visiting a shopping centre were supposed to consent to being recorded.

Only a few participants were in favour of the police using automatic facial recognition. There was one participant in each group who said that security was top priority. ‘I consider myself subordinate to the big picture. I don’t mind if they film me. I’ve got nothing to hide.’ Another said that it would have few consequences for them personally. ‘…I wouldn’t be recognised, they wouldn’t single me out.’

Participants did mention several criteria that they felt the police should satisfy before using cameras with automatic facial recognition. One was that the

technology should only be used for the agreed purpose and only within the context of an investigation. Other criteria addressed how the police should deal with data, such as:

- solid protection against hacking;
- no sharing of images with third parties;
- images must be deleted;
- compliance with the GDPR privacy rules;
- subject's consent required;
- people entering an area where they will be filmed must be notified accordingly.

Participants also distinguished between the various targets of such an application. One participant thought facial recognition should only be applied in the case of those 'high up on the wanted list – criminals who are armed and dangerous, psychopaths. Not pickpockets.' Another member of the same group stated that even 'minor' security threats, such as a mugging, were reason enough for victims to look favourable on such technology.

Cameras with automatic behaviour recognition

Box 8 Automatic behaviour recognition

Studies are under way using smart cameras that can recognise suspicious behaviour, such as suspicious walking or activity patterns. Pickpockets, for example, move around the streets differently than normal shoppers. Such cameras make it possible to detect suspicious behaviour in crowded areas like shopping malls. The camera system then issues an alert that the police can act on.

Almost all of the participants in both of the relevant focus groups were 'against' cameras with automatic behaviour recognition in public places. Their first response was to question the effectiveness of the application. 'Is there proof?' Someone else said, 'It's not airtight.' These comments led to a discussion of what 'suspicious behaviour' was and whether smart cameras could in fact recognise such behaviour. Some participants thought that such cameras would be unable to recognise pickpockets because they were professional criminals and operated in small gangs. Several participants worried that people displaying irregular behaviour would be wrongly singled out as suspicious. 'Psychiatric patients also have an unusual way

of walking, just like people with hernias or stroke victims.' The presence of cameras could also make people nervous, causing them to behave differently. One participant summed up the shared concerns in the following words: 'It's best to exercise restraint. Nervous or odd behaviour doesn't necessarily mean something's wrong.'

A few participants said that what mattered to them was how the police responded to the smart camera's alert. They would rather have an officer check out the situation on the ground first than have the police take immediate action. Some participants would use cameras with automatic behaviour recognition in specific situations, such as 'at airports or railway stations' to combat 'terrorism', or at 'big events, including to detect football hooligans at matches –in extreme cases. At festivals they're just a nuisance. It's right on the edge or just over the edge, in my view.' One participant added, 'I'm okay with it at Schiphol Airport, but I don't think it's necessary to send the cops to my block just because someone's speeding or jaywalking.'

A number of participants from Amsterdam thought that the technology would be less likely than humans to discriminate. 'I still think it's a creepy idea, but I also think that technology won't just assume that someone wearing a headscarf looks like a terrorist. That's not how technology works.'

5.5 More elaborate

The third scenario, 'more elaborate', describes how all sorts of sensors operated by multiple parties converge in a specific context. The discussion started with a video clip about Amazon Go's smart stores, where smart sensors and automatic behaviour and facial recognition cameras make cashierless shopping possible.[72] The moderator asked the participants whether they would do their grocery shopping at a smart store. The responses were mixed.

Many of the participants were positive about the smart store. 'It's easy and you have more freedom, similar to self-scanning registers. You don't have to wait in line and it's fast. It feels very modern.' Other participants mentioned similar advantages, for example 'no lines', 'handy', 'easy', 'simple', 'faster', 'efficient', 'convenient' and 'relaxed'. Two participants said that waiting in line was now 'old-fashioned'. Another advantage cited by a few participants was security. The technology could well prevent shoplifting and robbery. One participant wanted to see the technology

72 Link to video: https://youtu.be/NrmMk1Myrxc

applied more broadly. ‘It’s ideal! You grab what you want and leave. I’d like to see every shop use it, and pubs too.’

One concern raised by participants in all of the groups was that human contact would be sacrificed in smart stores. ‘No, I’d rather have a real cashier,’ said one participant. ‘A little human contact is nicer than those kiosks.’ Another said, ‘My father-in-law is a manic-depressive, and he really only interacts with people when he goes shopping.’ Participants were also concerned that the technology would erect a digital barrier for the elderly or people who did not use a smartphone.

Besides loss of human contact, job losses were also a concern for participants. After watching the video, they also questioned whether the technology actually worked and was sufficiently secure. ‘What if your phone crashes?’ ‘Is it secure?’ ‘What if you forget your phone?’

Responses after explaining how sensor technologies and sensor data are used

The moderator gave a more detailed description of the technology used in the smart store.

Box 9 Amazon’s smart store

The smart store has sensors that monitor everything. Customers are photographed upon entering and can then be tracked through the store by cameras with facial recognition. Weight sensors and cameras detect whether items have been removed from the shelves. Wi-Fi trackers monitor customer movement patterns by picking up signals from their smartphones.

Amazon knows precisely what customers put in their bag, what they return to the shelf, and which products they are unsure about. Virtually everything that customers do in the store is recorded. Amazon can use this information to send them personalised advertisements. When customers leave the store, the amount they owe is deducted automatically from their account just a few minutes later.

Some participants wondered whether there were no easier, less intrusive alternatives. Lively discussions ensued about data use and abuse. ‘It’s nobody’s business if I eat hash stew every day three years in a row,’ one participant said. Another, referring to shops registering customer preferences, said, ‘I wouldn’t mind them knowing that I bought a bottle of water, but what if you have a weird sexual preference or you buy something like a dildo. You don’t want people knowing that.’ Only a few participants found it acceptable for data to be shared with other commercial enterprises. Others thought that the data should remain strictly within the business. Several participants were opposed to data being shared with health insurers, for example. ‘That store probably sells cigarettes. That information gets passed on to your health insurer. Then you’ll have to pay for having an unhealthy lifestyle, because your premium will go up.’

Participants also associated this feeling with worries about the abuse of power by the biggest technology companies. ‘Amazon is a giant. In five years’ time it will have taken over our health insurers and then it will be telling us that we’re eating too many sweets.’

The scenario stated that Amazon would be able to use information collected in its store to send customers personalised advertisements. A small number of participants thought that this could make life easier and ensure that customers found the products they wanted in the shops. One participant was prepared to give Amazon full control. ‘They can take charge of everything! I’d love to have my life optimised. One algorithm making the right choices for my life. Food too, that would be ideal. People like me who enjoy certain foods, dishes with certain ingredients, like this other dish too, with a bottle of beer. It would be ideal.’ Several participants objected to the idea of personalised advertisements, however. As one of them explained, ‘It makes people greedy. They feel like they have to spend more, and work harder to make more money.’

Two participants mentioned the importance of alternative shops for vulnerable groups in society. ‘I think it would work well in big cities. But there has to be an alternative for children, mentally impaired people and so on.’ Participants considered it important to be able to choose whether or not to shop in a smart store. ‘That would be objectionable, to not have a choice.’

Smart city

The moderator continued the conversation by introducing the second example, the smart city.

Box 10 Smart city

Amsterdam, Eindhoven and other urban centres are working with IT companies and the police to improve quality of life and security in the city using smart innovations. Local governments are using sensors to collect all sorts of data for this purpose. They include:

- Wi-Fi trackers that track motorists' mobile phones to detect heavy traffic. Motorists are automatically directed to the nearest free parking space.
- Cameras that count how many people are walking around the city centre, to manage pedestrian traffic.
- Smart lampposts fitted with microphones that measure noise levels to detect quarrels in the vicinity.
- Software that analyses posts on Twitter, Facebook and other social media. A rash of negative posts on Facebook may, for example, suggest that rioting is imminent.

The moderator asked whether participants would like to live in a 'smart city'. A number of people said that they felt 'ambivalent' again, as they had before. They see that there are advantages and also disadvantages. 'Your freedom of choice is restricted, but it's handy too, being guided to a parking space.' Some participants mainly saw the positive side. 'Cool. I think it's about optimisation. Convenience. You can achieve more with fewer people.' But other participants said, 'This is the ultimate form of Big Brother. It's the local authority, i.e. the state, which will have access to the data, knows what you're doing and where you've been. I'd pack up and move right away.' A discussion arose in several groups about freedom being curtailed in the smart city. 'The authorities think for people and organise everything for them. People become sheeple. It's safe, it's quiet, and they tell you what's best for you.' Another said, 'We're being treated like herd animals…' As one of them explained, 'A city is made to be lived in. Now we're being guided from A to B in an almost clinical manner. Do you want to live in the city or do you want your life in the city to be lived for you?'

Several participants were concerned that such sensor applications would mean fewer officers on patrol. 'This example gives government a reason to pull all the police officers off the streets.'

The group from the Amersfoort region discussed the difference between cities and villages. Several participants appreciated that such applications could be useful in large cities, such as Amsterdam, but they did not want these applications in their own village. ‘I wouldn’t want this in Nijkerk or Zeist.’ Some participants thought that there was no way to stop the rise of the smart city. ‘Once it happens in one place, then at some point it will happen everywhere.’ Another said, ‘In that case, I’ll just have to accept it’.

Difference between the smart store and the smart city
Some participants were less troubled by the smart city scenario than the smart store. The purpose of sensors in the smart city was clearly to improve security, not to advertise, they said. On the other hand, one participant found sensors in stores more acceptable than Wi-Fi tracking in cities because their purpose in the former was clear and only Amazon would see the data. This prompted another person to comment on freedom of choice: it was harder to move to another city than to switch to another shop.

Technology in the smart city
We differentiate between four sensor technologies that can be applied in the smart city.

Wifi-tracking
Some participants felt that Wi-Fi tracking, i.e. tracking mobile phones, intervened too much in people’s private lives. They wondered whether it was possible to accomplish the same objective by less invasive means. One participant was clearly worried and said, ‘If they can scan my phone, they can look inside it too’. Another person found Wi-Fi tracking undesirable because parking ‘has nothing to do with security’.

People-counting cameras
Several participants thought that people-counting cameras were a useful application. Some thought it was fine to use a people-counting camera when Amsterdam’s main high street, Kalverstraat, became overcrowded. Another participant disagreed with using such cameras in city centres on Saturdays, but approved of them during, say, a victory parade celebrating the local football team if it won the league title. In that case, it was nice to be warned to avoid a certain area or to walk a certain route. Participants had no objection to the use of people-counting cameras for a clear purpose, for example if there was a risk of rioting. Some participants thought that people-counting cameras were unnecessary because until now, ‘everything has always gone smoothly in crowded places’, for example in Amsterdam on the King’s Birthday, a national holiday.

Smart lampposts fitted with noise-detecting sensors
The ‘smart lampposts’ that measure noise levels, for example raised voices in an argument, sparked the most discussion. Participants questioned whether the technology actually worked. ‘It must be very clever software’ to be able to differentiate between ‘ordinary’ loud noises and aggression. Participants gave a variety of examples that the system might report unnecessarily, for example ‘loud conversations and joking around’, ‘yelling at your dog’, ‘a balloon bursting’, ‘singing’, ‘Arab men talking loudly’, ‘young people messing around’, ‘students coming home at night’, or ‘a wailing child’. One participant wondered what precisely the police did when a lamppost reported noise. Another participant did not think that a smart lamppost could detect a shooting.

There were also participants who noted advantages. A shot or screaming could result in closer surveillance of a place. One participant thought smart lampposts could be of specific help in preventing fights at schools and addressing recurring noise issues in neighbourhoods. Some participants called the ‘smart lamppost’ the most appealing of the four sensor applications. One, for example, would prefer not to have camera images and thought it was less intrusive to record noise levels. Another explained, ‘This could be very useful. A smart lamppost makes police intervention possible’.

Software to analyse social media
Opinions differed about using software to analyse social media, for example to anticipate rioting. Some participants considered it a good idea to use this technology, with several arguing that people themselves chose to post comments on public platforms such as Facebook. ‘You can tell Facebook to limit what the public sees on your profile.’ Even so, the same participant wondered, ‘How do I decide what to make public and what to keep private?’ Other participants had a very negative opinion of this application because software analysis of social media felt to them like ‘being bugged’, as one of them put it.

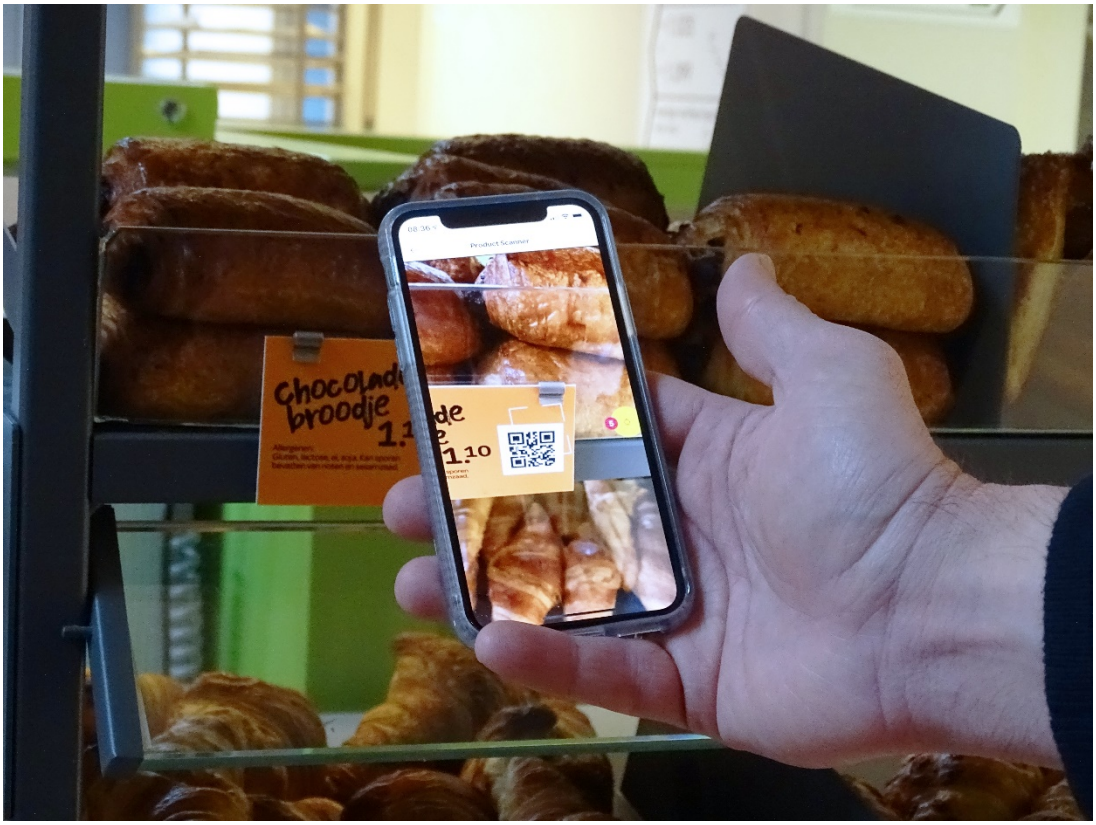
5.6 Concluding remarks

We reported on the focus group discussions in this chapter, sticking as closely as possible to the conversations as they took place. We structured the chapter on the basis of the outline of the sessions and made liberal use of quotes to give readers an impression of how the discussions unfolded. In the following chapter, we will analyse the overriding themes and findings of the focus groups and address the sub-question ‘How does the public perceive the deployment of sensors and sensor data for security and quality of life, and what factors underpin this perception?’ We

will base our account on the conceptual framework (described in Chapter 4) and compare our findings with the findings of our literature review.

Intermezzo: goodbye to queues

‘Smart shops’ use sensors to simplify and speed up purchasing for customers. Several supermarkets in the Netherlands are testing the ‘smart shopping’ concept. Erwin Binneveld of SPAR University Utrecht gave us a tour of the first shop in the Netherlands to use scan-and-go technology.



Source: Rathenau Instituut

Concept and technology

SPAR University grocery has been experimenting with self-checkout stations since 2013. The experiment has sometimes led to even longer queues because customers are less familiar with scanning than the shop’s cashiers. Self-checkout is a good solution in off-peak hours, when the shop is quiet, but something more is needed during peak times. SPAR University is now testing ‘skip-the-queue’ technology, which allows customers to bypass checkout altogether. They scan the products they want using an app on their mobile phones and then simply leave the shop with their purchases. They receive a mobile payment request along with a separate QR code that could yield them a freebie. ‘It’s a reward system that we’ve

added to encourage customers to pay with the app.' Binneveld shows us how he scans individual buns and apples and how they are registered in the app.

Employees and customers

According to Binneveld, the ultimate goal is not to rid the shop of all its employees. 'In fact, I think we'll actually be hiring more people, but they'll have a different role to play. Employees will be tasked with promoting or selling products, making fresh sandwiches, or interacting with customers.' In other words, their duties will shift from simply scanning products to a form of hospitality, according to Binneveld.

In the United States, Walmart has already abandoned its scan-and-go checkout system. 'Walmart tested cashierless checkout, but there was too much shoplifting. Research has shown that people in the Netherlands and Germany are more honest, so a scan-and-go system can work here.' But isn't SPAR University afraid that the new system will lead to a rise in shoplifting? 'Shoplifting is just as bad in traditional supermarkets. They don't check customers either.' Because SPAR University employees are not occupied with operating registers, they can play an important role in challenging 'opportunistic' thieves, who decide to steal something on the spot. 'Having employees identify and challenge shoplifters can help supermarkets improve their margins, especially the ones that use cashierless systems like self-scan checkouts,' says Erwin Binneveld.

SPAR University does not expect its 'skip-the-queue' system to become the sole method of payment. 'Not everyone likes apps or having to pay for purchases with an app.' Nevertheless, internal research shows that 40% of customers have already downloaded the app. 'We send all our special offers to customers through the app and online. We no longer offer discounts offline, only online. So you can certainly shop offline with us, but you won't get any special deals.'

Shopping in the future

By tracking shopping behaviour with its app, SPAR University collects a considerable amount of data. At present, SPAR is mainly interested in collecting and analysing data, but eventually it may use the app to make personalised offers. For example, it could 'nudge' shoppers to stick to a healthy and sustainable diet. New technology can enhance this feature. 'We can have the app offer shoppers personalised advice, for example "Haven't had enough fruit this week? Grab a free piece of fruit when you shop." Who cares if the message comes from a friend or SPAR University?'

SPAR University is looking to extend the technology in the shop. 'We're working on smart cameras and Wi-Fi tracking. Once we have that kind of data, we can rearrange the shop, for example set out baskets with products. Another, more

practical option is to alert customers to certain ingredients, for example if they want to buy nut-free products.' SPAR University is also investigating whether sensors can be used to track people in the shop, so that it can offer a customer a discount on chocolate when he's standing in the sweets aisle.

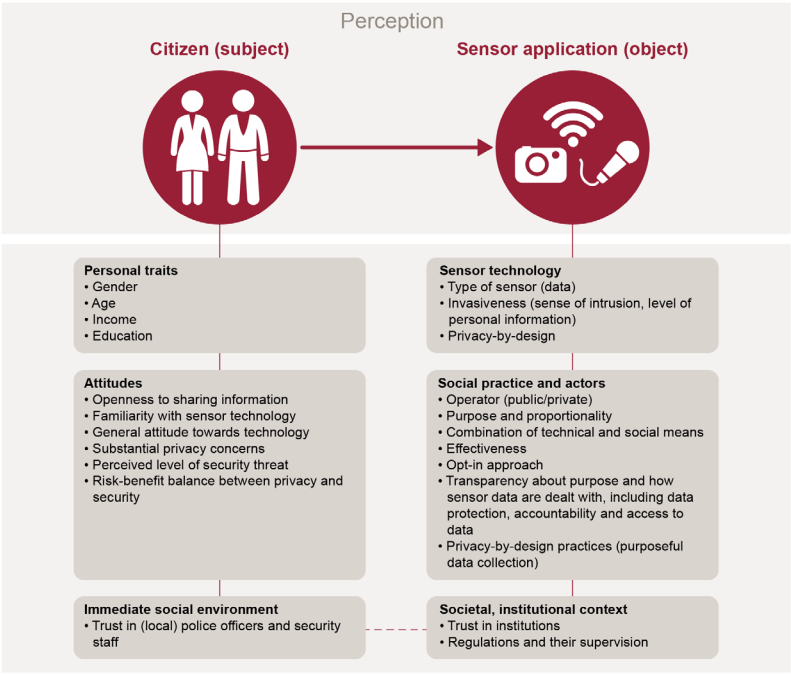
But all this lies in the future. The first step is to make sure that the skip-the-queue system works flawlessly. It didn't when our interviewer tried the cashierless payment system. The app started up and immediately crashed.

6 What the focus groups teach us

6.1 Introduction

In this chapter, we analyse the outcomes of the focus groups using the conceptual framework introduced in Chapter 4. The focus groups gave us a glimpse of what the public thinks of sensor applications, and in this chapter we therefore discuss their perceptions and the three dimensions of sensor applications that we identified earlier, i.e. 1) sensor technology, 2) social practice and actors and 3) societal and institutional context (see right-hand column in Figure 6.1).

Figure 6.1 Conceptual framework of public perceptions



Source: Rathenau Instituut

Each of the following three sections describes the participants' discussions of one of the three dimensions of sensor applications. Section 6.2 covers their discussion of sensor technology, section 6.3 their discussion of social practice and actors, and section 6.4 their discussion of the institutional context. Each section first outlines how the participants felt about the use of specific sensors at the outset, how much they knew about the technology, and what their general attitudes were.

We structure our focus group analysis as much as possible around the factors that emerged from our literature review (see right-hand column in Figure 6.1). This approach also allows us to compare the outcomes of the focus groups with the results of our literature review as presented in Chapter 4. We make this comparison at the end of this chapter (section 6.5).

6.2 Sensor technology

The focus group sessions yielded a broad range of opinions and arguments concerning sensor deployment. Nearly all of the participants were familiar with the use of sensors. Many, however, were unacquainted with some applications, such as shop cameras with automatic behaviour recognition. Participants recognised the trends we addressed and were capable of seeing the connections between our examples, allowing them to discuss them in a meaningful way as part of the same phenomenon. One crucial development in the discussions was that, as the focus group sessions went on, participants learned from one another, changed their minds and dug deeper into reasons. The group discussion format allowed the participants to explore issues in greater depth, ask detailed questions, and consider the social implications of sensor and data system use. For example, they asked themselves:

- how sensor data are stored;
- how reliable the data are;
- to what extent the data concern personal data;
- whether they are adequately shielded from hackers, and
- who has access to the camera images and data.

The tension between privacy and security

Each of the focus groups associated sensor deployment with privacy issues and raised arguments for and against their use. Participants were greatly concerned that sensors were being used at the expense of privacy, with ‘invasion of privacy’ being a common objection. Participants regularly mentioned the tension between privacy and security. While some participants were immediately in favour of and some immediately opposed to using sensors in certain contexts, many said that they felt ‘ambivalent’, i.e. unable to decide how they felt even after weighing up all the pros and cons. As one participant put it, ‘I’m of two minds. It’s useful for fighting terrorism, but what if my data are used for other purposes, without me knowing? Is that really what I want?’ Several other participants described this feeling as a dilemma between security and privacy.

Tipping points
Various participants reached a ‘tipping point’ during the discussions, where they changed their minds about using sensor technology. For example, some participants were initially in favour of sensor technology, but later on came to think that a particular sensor application crossed the line in terms of privacy. That occurred during the ‘smart city’ discussion, for example. Some participants who were initially positive about using individual sensors in public places came to find their deployment in a smart city network unacceptable.

The tipping points show that we cannot discuss public acceptance of certain sensors or technologies without also considering the practical and broader context. We cannot say that the public approves of body cams or opposes Wi-Fi trackers. We need to discuss how, what, where, when and, above all, why sensor technology is being used.

Participants appeared to be more critical of new forms of technology, such as cameras with automatic behaviour recognition or noise detection sensors, than of familiar applications, such as stationary security cameras. Uncertainty about how such technologies actually function, for example behaviour recognition or noise detection, was a factor here. Participants especially regarded new, smart technologies – for example those incorporating AI – as more confusing and less transparent.

6.3 Social practice and actors

The discussions showed public acceptance of sensor use hinges on the how, what, where, when and why. In addition to the features of the technology itself, the focus groups discussed sensor use in specific social and societal contexts, as well as the potential implications.

Important points in the discussions were the purpose and target of surveillance. The vast majority of the participants were positive about using sensors to secure specific situations and/or to monitor specific (problematic) locations or target groups. People were more willing to accept sensor applications when they were trained on crowded places or events, for example on special occasions, to secure football stadiums, ‘a victory parade celebrating the local football team if it won the league title’, at festivals in the city centre, during Carnival celebrations, in overcrowded conditions (such as in a busy high street) and at events where there is a reasonable likelihood of unrest.

Participants differed with regard to the people they felt should be the target of sensor applications. Some wanted sensors to be aimed only at persons who presented a serious threat, while others said that crime prevention and minor threats offered enough reason to use sensors. A few participants mentioned specific groups that they felt the police could target with sensors, such as habitual offenders in Amsterdam. For example, one participant thought that the force should be allowed to use every available means to catch the top 600 on the wanted list. ‘If it means infringing their personal freedom and privacy, well, they’ve only themselves to blame.’

In short, the purpose is a major factor in public acceptance of sensors. However, people also find transparency about the purpose and the way sensor data are used important. As one participant said, ‘I should be able to see which information is being shared where to ensure transparency and achieve the aim. How do I know what they’re doing with my data?’

Sensors for security

With respect to the various scenarios discussed by the focus groups, participants were more likely to accept sensors being used for security reasons than to improve the quality of life. Participants in all of the groups mentioned an improvement in security as an important advantage of using sensors, for example to prevent crime and serious offences or to track down culprits sooner. They thought sensors could help to solve a wide range of crimes, from ‘littering’ to ‘mugging’ and ‘robbery’, but also ‘serious violations’, ‘murder’ and ‘terrorism’. However, they clearly preferred sensors to be used to combat serious crime and terrorism rather than minor offences. When asked what security means, they listed a number of blatant offences, such as ‘firing a gun around children’, ‘criminal acts’, ‘your child being attacked’, ‘combating crime’, ‘fighting criminals’ and ‘people posing on Facebook with Kalashnikovs’.

Social proximity

Participants were more sceptical about using sensors explicitly to improve the quality of life. They mentioned monitoring a ‘normally quiet residential area’, ‘noise nuisance’, ‘quarrelling, smoking dope and public intoxication’ and ‘cars double parked in front of the bakery’ as situations that did not call for the use of sensors. Their reasons included the perceived high cost of such surveillance, wrong policing priorities and infringements of personal freedom and privacy.

Some participants were concerned that the use of sensors would compromise quality of life. They thought that using sensors at specific locations could result in

changes in behaviour, known in the literature as the 'chilling effect',[73] and wondered whether the use of sensors would cause people to avoid places because they 'feel constrained in their behaviour', or 'because they feel they're constantly being watched'.

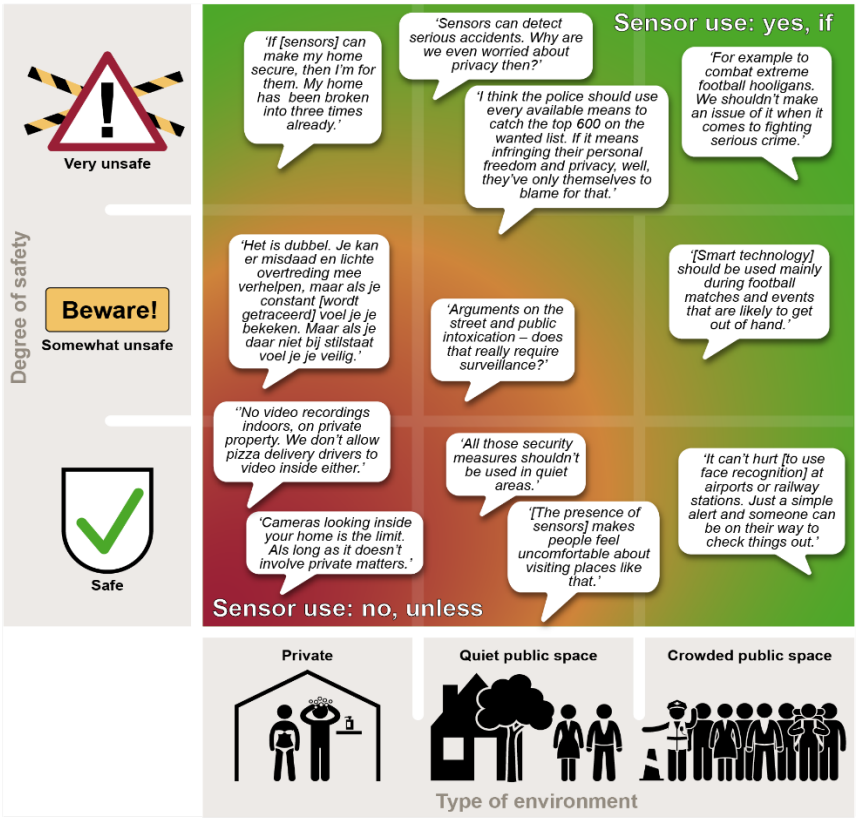
One explanation for this critical attitude is that focus group participants often associated quality of life with 'social proximity'. Many participants felt uncomfortable having sensors intrude too much on their private situation or home. Several participants felt that there was no justification for using sensors to detect relatively minor incidents, such as littering. However, if specific measures were put in place to protect such values as privacy, security or transparency, then they would feel more positively about using sensors in these contexts.

Figure 6.2 shows public acceptance of sensor use to promote quality of life and security. The figure is plotted along two axes. The vertical axis shows three levels of security, i.e. safe, slightly unsafe, and very unsafe. The horizontal axis differentiates between three settings, i.e. private setting, quiet public place and crowded public place. Several representative quotes are given in the figure. We see that acceptance of sensors depends on perceived level of safety: the more risk people perceive in a situation, the more they tolerate the use of sensors to improve security and quality of life. Acceptance also depends on the setting: the use of sensors in private settings is less acceptable than their use in public places, especially in crowded situations.

On the one hand, people *do* approve of the use of sensors in very unsafe circumstances and crowded public places, *but only* if the situation meets a number of important criteria (see the eight rules below). On the other hand, people *do not* approve of using sensors in private homes or in quiet public places that feel safe or only slightly unsafe, *unless* doing so clearly improves quality of life *and* meets a number of important criteria, for example relating to privacy and personal freedom (see the eight rules below).

73 White, G.L. & Zimbardo, P.G., (1975). *The Chilling Effects of Surveillance: Deindividuation and Reactance*, Defense Technical Information Center.

Figure 6.2 Public acceptance of sensor use to promote quality of life and security.



Source: Rathenau Instituut

Policing practices

Several participants argued that sensor technology can help to make policing more effective and to identify where and when officers should be deployed. Their idea was that technology allows the police to operate more effectively and efficiently, thereby increasing the force's ability to catch criminals. They also thought that technology improved information-gathering, which in turn improved the quality of policing. Sensors could also help to collect evidence. One participant thought that sensor technology would make the police better prepared and that noise sensors, for example, could detect possible escalations before they got out of hand.

Some participants argued that policing needed to be modernised in this way because criminals were equally adept with technology. Sensors were a necessary weapon in the fight against new types of crime, such as cybercrime. Several participants did wonder whether the police could handle such innovations and whether the force had the right people for it. 'There are so many older constables in the force. They need fresh recruits. The fifty- and sixty-year-olds won't be up to it.'

Several participants stressed the importance of police follow-up. Their confidence in police crime-solving depended on that. They understood the potential of sensor technology, but felt that if the police failed to make good use of sensor data, then it would be a waste of tax-payer money and undermine public confidence in the force's ability to take action. If the police collected sensor data, then they should also commit themselves to using it responsibly. If they failed to do so, then the public could come to regard the use of sensors as excessive.

Several participants were also concerned that using sensors would lead to there being fewer officers on the streets. There were two sides to this concern. First of all, they feared that the 'gigantic cost' of sensors and monitoring sensor data would have an impact on police officers' salaries. Secondly, they were worried that sensor deployment would automate policing, with police deployment on the streets being considered superfluous (whereas the public felt differently about that). In their discussions of policing or police deployment, the focus groups often meant 'officers on the streets' and not police data analysts. Various participants found a scenario in which sensors replaced officers on patrol and 'people sit behind screens' an unattractive prospect.

6.4 Societal and institutional context

The broad social and institutional context in which sensors are used influences their public acceptance. In this section, we focus on the public's trust in the police. We also consider how trust in the police differs from trust in other public and private institutions.[74]

Trust in government

Some participants felt that it was important to not only trust government *now* but also going forward. They felt that the use of sensors set a precedent. They wondered 'What if a different regime comes to power, like the one in Brazil now?' Another explained, 'The aim is very noble, but it can be used coercively as well.' One concern was that continuous monitoring made 'everyone a suspect' and that government would have too much power over its citizens.

Discrimination

Another recurring theme was discrimination stemming from faulty data or data analysis. A number of participants living in large cities wondered whether the system would remain fair and whether prejudice and false assumptions would not

74 The subject overlaps with 'social practice and actors' (section 6.3), but we have moved it here because it mainly addresses institutions.

make it ‘biased’. For example, they worried that the way sensor systems were programmed would increase the risk of re-arrest or re-prosecution for people and population groups who had been in repeated trouble with the law. Some participants saw this differently. They argued that technology was in fact more neutral than police officers and had the potential to curb discrimination.

When discussing discrimination, participants made a conscious or unconscious distinction between the practices of specific police officers and ‘the force’ as an institution. One of them said, ‘I hope they do the right thing, but I’ve accepted that this isn’t always the case. You’d like them to show empathy in certain situations and hope that they can rise above their ethnic biases, but you don’t know if they will.’

Trust in public institutions such as the police

Research by Statistics Netherlands (CBS) shows that the Dutch place a great deal of trust in public institutions.[75] The police, the courts and the army earned the highest scores, with 74.5% of the Dutch population regarding the police as trustworthy. Indeed, Dutch people trust the police more than they trust other people in general. The focus groups were similar in that regard, although participants had numerous criticisms about police behaviour in general discussions of police trustworthiness. In terms of sensor deployment, participants appeared to trust the police much more than other parties involved in deploying sensors for purposes of security and quality of life. Their reasons were: the police are not motivated by profit, they have a stronger sense of values, they are more closely regulated than the private sector, and their methods are more transparent than those of commercial parties. The majority of the participants were therefore relatively confident that the police would use sensors correctly, whereas many participants were critical of businesses using sensors and sensor data.

Participants did not feel confident that private institutions acted ethically. They did not trust them to respect important values, such as privacy, personal freedom or autonomy and human dignity. They also feared that the balance of power would be skewed by large international technology companies ‘knowing you better than you know yourself’. They viewed companies such as Facebook and Amazon – given as examples during the focus groups – with suspicion when it came to handling data properly. However, they stressed in various discussions that the decision to make use of such digital services was up to the individual. The importance of freedom of choice came up repeatedly in their discussions.

A number of participants were explicitly concerned about situations in which it was impossible to avoid sensors, especially in public places. As one participant put it, ‘If

75 See https://www.cbs.nl/nl-nl/nieuws/2018/22/meer-vertrouwen-in-elkaar-en-instituties

you have a shop loyalty card, then that's up to you. But at least you have a choice in that case'.

With some exceptions, the participants were highly critical of private security firms using cameras. They were concerned about commercial interests overriding those of the public.

There were also worries that private firms would not handle data discreetly and that their staff did not have the same qualifications as police officers. Participants found police and railway security body cams acceptable, for example, but no one approved of body cams on pizza delivery drivers. Some respondents, however, thought that private firms could be hired for simple security activities to alleviate the pressure on the police.

Regulations and supervision
The focus groups did not discuss 'regulation and supervision' in detail. Participants had some critical comments to make about the Dutch Intelligence and Security Services Act (Sleepwet) and the GDPR, including the latter's impact on policing and other matters. Generally speaking, participants had positive views of legislation and regulations as instruments that provided guidance for both technology and supervisory tasks. Examples of statements about regulation include 'As long as [sensors] operate within the framework of the law, I'm fine with it', and 'The police must comply with legislation'. A few individuals called for 'clear guidelines and rules' to govern the use of specific technology, for example facial recognition cameras.

6.5 Focus groups versus literature review

To gain a better understanding of the output and added value of our focus group research, we compared the results of the focus groups with those of our literature review in Chapter 4. Table 3 summarises this comparison and shows that the results of the two studies are very similar. Almost every factor that the literature cites as important in the shaping the public's opinion of sensor applications was also raised in the focus groups (either implicitly or explicitly).

In addition, the focus group research augments the literature review by providing a qualitative examination of public opinion on the use of various sensors and sensor data. The focus groups furthermore offer new insights and more details on the factors that the public considers important. In the following section, we discuss the most significant differences and similarities between the focus groups on the one hand and the literature review on the other, doing so for each dimension (sensor technology, social practice and actors, and societal and institutional context).

Sensortechnology

The SurPRISE study, which examined public opinion in Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom between 2012 and 2015, highlighted the importance of privacy-by-design principles. Although this precise term did not come up in the focus groups, the concept of privacy-by-design was discussed. According to the literature, privacy-by-design involves minimising sensor data, automatically anonymising data and safeguarding information, among other things. The focus groups identified these ideas as important prerequisites for deploying sensor technology. As one participant said, 'Personally, I'm in favour of 24-hour camera surveillance, but the recordings should be erased as soon as they've been viewed'.

One difference that we noted between prior research and our focus group outcomes concerns Koops and Vedder's (2001) claim that the effectiveness of the sensor application is hardly relevant to the public. They conclude that people are concerned about the amount of personal information being collected and the purpose for which sensor data are used, but are seemingly less worried about whether the technology actually does what it is supposed to do. Our own research contradicts their conclusion. Our participants not only made frequent mention of the effectiveness of sensors but also stressed the importance of follow-up – i.e. actually using the sensor data (see also section 6.3).

Social practice and actors

Focus group participants were more inclined to accept privacy-sensitive interventions to solve serious crimes than to tackle petty offences. Dinev et al. and Koops and Vedder reached similar results.[76] Seventy percent of their respondents considered using investigative or surveillance equipment, such as cameras, permissible in relation to serious crimes, compared with less than half in relation to minor infringements.

Social proximity was also a defining factor in the aforementioned SurPRISE study. The more people felt that technology was intruding into their personal or everyday life, the less likely they were to find the technology acceptable. The more sensor technologies targeted specific groups (such as suspects and criminals), the more acceptable people found them compared with blanket surveillance technologies.

Research has identified a number of values that play an important role in public acceptance of sensor technologies. Both our literature review and our focus group

76 Koops, E.J. & A. Vedder (2001, p. 41). *Opsporing versus privacy: de beleving van burgers*. Den Haag: Sdu Uitgevers; Dinev, T. et al. (2005). 'Internet Users, Privacy Concerns and Attitudes towards Government Surveillance - An Exploratory Study of Cross-Cultural Differences between Italy and the United States'. *BLED 2005 Proceedings* 30.

research show that people consider transparency, purposeful action, and appropriate use of data to be important. Like Schildmeijer et al., our focus group research shows that the public considers it important to know what happens to personal data and the purpose for which such data are being used.[77]

The focus groups also reveal what the Dutch expect of policing. For example, our participants expect the police to have the technology to fight modern crime and to use it. They question whether the force currently has the necessary ability to innovative. They expect the police to use sensors effectively and to follow up on alerts and reports. Many would be unhappy about sensors replacing police officers on the street.

Societal and institutional context

The SurPRISE study shows that when people perceive institutions as trustworthy, they are more likely to find sensor technologies acceptable. This matches the outcomes of our study. If the police fail to live up to certain standards or to act reliably, it will also erode trust in the use of sensor technology. Like the respondents in Schildmeijer et al., our focus group participants said that they trusted the police more than private security firms.[78]

Table 3 Factors identified in the literature and in our focus group research as important in shaping public opinion about the application of sensors and sensor data.

Literature review	Focus group research
'Sensor technology'	
Type of sensor (data)	Participants are more critical of new forms of technology than of familiar technology. That is in part because they are uncertain about how such technology actually functions.
Invasiveness (sense of intrusion, level of personal information)	Privacy is important to participants. They recognise that there is tension between privacy and security.
Privacy-by-design	Participants do not use the term 'privacy-by-design', but do mention various related conditions that they feel should be imposed on the use of sensors (see Social practice).
	Participants stress that the technology should be effective.

77 Schildmeijer, R., C. Samson & H. Koot (2005). *Burgers en hun privacy: opinie onder burgers*. Amsterdam: TNS NIPO Consult.

78 Idem.

'Social practice and actors'	
Operator (public/private)	Participants trust the police force more than private parties when it comes to the use of sensors.
Purpose and proportionality	Most participants have a favourable attitude towards using sensors if the purpose is clear. The legitimacy of sensor deployment depends on the level of security (safe, slightly unsafe, very unsafe) and the setting (private, quiet public place, crowded public place).
Combination of technical and social methods	Sensors should not be deployed at the expense of police officers on the streets.
Effectiveness	Participants stress the importance of police follow-up. They expect the police to be capable of using modern technology effectively. They also expect the police to use technology that will improve public safety.
Opt-in approach	Participants would like to have a say in whether they are being monitored and whether sensors are being used in their immediate surroundings.

Literature review	**Focus group research**
Transparency about purpose and how sensor data are dealt with, including data protection, accountability and access to data	Participants want to know what sorts of sensors the police are using, what they are using them for, and what happens to the sensor data they collect.
Privacy-by-design practices (purposeful data collection)	People want data to be as anonymised as possible, to be secure, and for sensor data collection to be proportional and minimal.
	The police must treat all people the same. Discrimination must be precluded.
'Societal and institutional context'	
Institutional trustworthiness	Most of the participants see the police as very trustworthy. Participants trust the police force more than private parties when it comes to the use of sensors.
	Participants also think about the future political climate and government. They wonder whether sensors, which are legitimate in the current political context, could be misused under a different regime.
Regulations and supervision	Participants are more critical of new forms of technology than of familiar technology. That is in part because they are uncertain about how such technology actually functions.

Intermezzo: an algorithm that recognises brawls

Tinus Kanters is the project manager for the Stratumseind Living Lab. Stratumseind is a nightlife area in the city of Eindhoven. The Living Lab is an experiment in which sensors are being used to improve the atmosphere on the streets. Kanters is overseeing an algorithm that can predict when a brawl is likely to break out. We visited his office to have a look at the project.

Source: Rathenau Instituut

Office like a sciencefiction lab

It's a drizzly Wednesday afternoon and the locked doors and empty streets of the Stratumseind district do not look very inviting. This is not where you'd expect to find crowd-detection sensors. Nevertheless, it is one of the Netherlands' best-known labs for testing and analysing security and quality of life sensors in public places. The City of Eindhoven is cooperating with the police, pub owners, property owners, breweries and local residents to improve the atmosphere and quality of life there.

The project involves installing numerous sensors on the streets that are, at first glance, undetectable.

Our expert is Tinus Kanters, the project manager of the Stratumseind Living Lab, whose office is located above a pub along the main strip. His office resembles a laboratory in a science fiction film, with dozens of screens, sensors, cables and technology prototypes. We have a conversation with him about whether Stratumseind represents the future of Dutch nightlife districts.

Fights and false positives

There are some eight hundred incidents a year on the Stratumseind strip. In an effort to cut down on this number, the project researchers are keeping track of the 'atmosphere' in the street in real time. They do this by collecting data from various sources. 'We count how many people enter and leave the strip, where they come from, what the weather's like, how noisy it is, the intensity of the light and the amount of rubbish. They also monitor social media, a calendar of events, police statistics and how much beer has been delivered to the pubs.

They use people-counting cameras to tally the number of visitors to the strip. The cameras automatically convert people into unrecognisable points. 'That way we can register visitor numbers anonymously. I'm not the police. I'm not allowed to scrutinise the camera images.' The algorithm uses data on the group behaviour of the 'points' and noise analyses to predict, two to three seconds in advance, when fighting will break out.

The system is not without its flaws. 'The noise analysis still produces a lot of false positives. It's accurately detected all the brawls that have occurred, but it's also misconstrued some stag parties as fighting. The police tell us if what we've detected actually turned out to be a scrap and we feed that into the algorithm so it can learn.'

Improving the atmosphere on the street

Among the tools being deployed to influence the atmosphere are coloured lamps and scent diffusers. Research has shown that orange light and the scent of oranges have the most calming effects. The question is whether it will actually work down on the ground. 'The scent of oranges gets mixed up with the stench of stale beer and kebab, so it's hard to assess the effect,' says Kanters.

In the meantime, researchers and students are busy looking for correlations between the various data streams, for example what's listed on the calendar of events and where people come from. These data are in the public domain and can be retrieved from the City of Eindhoven's open data portal. The researchers

supplement them with data purchased from mobile phone providers that provide an accurate indication of how many visitors are in an area. All data are displayed on an internal dashboard that will soon be shared with the police.

Cooperation with the police force
‘People have to get used to this technology, and the same goes for the police. New technology can seem threatening, but we think it makes an important contribution.’ For example, notification of an incident could trigger an alert that’s automatically sent to police officers patrolling the area. Kanters believes this could be crucial when every second counts. Everyone – police, victim and perpetrator – is better off. The data may also show a need for a heightened police presence or, conversely, that fewer officers are required.

Data principles are leading
Kanters does not believe that technology and privacy are always mutually exclusive. Technology can in fact help to improve privacy. For example, the images that cameras relay to incident rooms can be ‘blacked out’ until sensors detect irregular activity. ‘In the absence of relevant legislation in the Netherlands, we have drawn up our own data principles. To build a house in the Netherlands, you have to comply with stacks of rules before you lay even the first brick. But when it comes to data use, there’s nothing. You might reason, “It’s not against the law, so why not,” but that’s not the right way to look at it.’

The data principles address such matters as privacy, public participation and supervision of those who control the technology. The Eindhoven project, for example, has a modular setup. In other words, the algorithm that converts the data into useful information has been developed in-house. ‘If you let the big global commercial operators do that, you’ll lose control altogether.’

Another advantage of this approach is not having to rely on a single software supplier. Known as ‘vendor lock-in’, Kanters says that it happens all too often in projects such as the Stratumseind Living Lab. It then becomes prohibitively expensive to make even relatively minor changes to the software structure. Kanters has other recommendations for the police. ‘Don’t depend on just one firm, and install an ethics committee.’

Results
The Stratumseind Living Lab has been running for about four years. Does Kanters think the strip is safer now? ‘Eindhoven University of Technology did a study showing fewer brawls than four years ago. And the people who frequent the pubs here say they feel safer. In all honesty, overall visitor numbers have declined, although pub and nightclub revenues are stabilising. That probably means that the

visitors who remain have more money to spend. Whatever the case, Stratumseind is a lot more fun now than it used to be.’

7 Conclusions: from values to rules

This study shows that the public's perception of the use of sensors and sensor data depends on three key interrelated dimensions: 1) sensor technology, 2) social practice and actors and 3) societal and institutional context. This means that people are not simply in favour of or opposed to a particular sensor application. Their views on a technology and whether they accept it depend on various contexts, such as the features of the technology itself, the social practice in which it is used, and the societal and institutional context in which that social practice is embedded.

It is not only context that shapes people's opinions, however; values do as well. The focus groups have revealed the multi-faceted interaction between the values that people believe play (or should play) a role in sensor and sensor data use. Our literature review and focus group research have also allowed us to identify a number of rules that the public believes the police should follow when using sensors. These rules are closely related to the values that people care about, and they lend those values a more specific meaning.

7.1 Striking a balance between disparate values

The discussion about sensor technology is often framed as a trade-off between security and privacy. The people participating in our focus groups were no different in this regard. At the same time, our study makes clear that, in the case of sensor applications, people value a broader array of underlying ideals. People expect law enforcement to strike a healthy balance between these disparate values, in consultation with the public. In addition to physical safety and privacy, these values include democratic rights, efficient and effective operations, innovativeness, transparency, quality of life, autonomy or personal freedom, and human contact.

First of all, the public expects the police, as a crucial guardian of the democratic rule of law, to abide by that law. Most of the focus group participants said that they trusted the Dutch police. Second, people expect the police to be capable of using modern technology effectively, and to use technology that will improve public safety. However, they question whether the police are innovative enough to do so, and whether they will be able to follow up on the data that sensors generate. Third, the public expects the police to respect their privacy. In the narrow sense, this means dealing properly with personal data. People would like to be able to take for granted that the police apply privacy-by-design principles when developing sensor

systems. In the broader sense, respect for privacy means minimising interventions into people's private lives. The concepts 'quality of life' and 'personal freedom' play an important role in this context.

Last of all, the public considers it important to limit the technological dimension of policing. Policing is regarded as people work and the public does not wish to be deprived of direct contact with police officers or of officers patrolling the streets. Meaningful human contact is, in other words, a highly significant factor in policing.[79] The purpose of a sensor should not be to replace police officers but to improve the work of the police force and the relationship between its officers and the public.

7.2 Eight rules for police use of sensor technology

In the real world, the aforementioned values can be at odds with one another. The public expects the police to take each one of these values seriously when using sensors and sensor data, and to try to strike a healthy balance between them in policing practice. The question then is how the police – assuming that their work is underpinned by the set of values described above – should act in various specific situations involving sensors.

We have taken the results of our focus group research to come up with a set of rules governing the interpretation of these values in real-life situations. Here, they are aimed specifically at law enforcement, but our research shows that the public would like other branches of government, businesses and their fellow citizens to play by these rules as well. These rules therefore also pertain to various forms of sensor surveillance, i.e. top down (surveillance), bottom up (sousveillance) and horizontal.

Table 3 is the starting point for defining the rules. It summarises factors identified in the literature and focus group research as important in shaping public opinion about the use of sensors and sensor data (see Table 3, section 6.5). Since these factors are important to the public, we assume that the police must take them into account. Every factor thus leads to 'rules' (the exercise itself can be found in Appendix 3). The list is divided into clusters, producing the following set of rules by which the police can ensure that they use sensors and sensor data in a socially responsible manner in practical situations.

79 According to Est, R. van & J. Gerritsen with the assistance of L. Kool (2017). *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE).* The Hague: Rathenau Instituut.

1. The police should use sensors in a way that inspires public trust.

Many Dutch people currently view public institutions, and the police in particular, as trustworthy, an observation that has emerged from various public surveys and that was corroborated by our focus group research. Having trust in the police influences what people think of the use of sensors and sensor data. An erosion of that trust in turn undermines trust in police use of sensor technology The reverse is also true: an erosion of trust in police sensors undermines trust in the police. That is why it is important for the police to use sensor technology in a way that inspires public trust and that therefore builds rather than undermines trust in the police. The public considers compliance with the following rules to be trust-building behaviour.

2. Provide the public with straightforward, transparent information about the use of sensors.

Many people are not sure what role police sensors play, how they operate, and what purpose they serve. They are even more confused about sensor data. Needless to say, the biggest unknown is the use of new sensor technology. We therefore recommend engaging with the public when introducing (new) sensors and sensor data and explaining their purpose and how they operate. It is also important to explain publicly that the police use sensors for monitoring purposes, as that is how people tend to come across sensors in specific situations. One of the main lessons that we can learn from the focus groups is that the more people talk about sensors and sensor deployment, the more they come to understand their use. In view of this social learning effect, we recommend informing the public about sensor surveillance and its implications for security and quality of life and engaging in discussions. People do not consider the use of sensors to be self-evident in private settings or in normal public spaces that they consider safe or slightly unsafe (see rule 7). In those situations, it is important to engage with the public in determining whether sensors should be used at all.

3. Apply privacy-by-design principles

Although the precise term ‘privacy-by-design’ did not come up in the focus groups, the concept itself was discussed. It means considering data protection, both technical and organisational, at an early stage of the design process and incorporating such protection into the design of socio-technical systems. The public wants privacy-by-design to be standard in sensors and believes that the use of sensor technology should be subject to the following criteria:

- sensor data should be minimised;
- data should be automatically anonymised;
- information should be secure.

The focus group discussions gave rise to the following lessons in that regard:

- Use data for the agreed purpose.

- Choose solutions that collect as few personal traits as possible. For example, anonymise data as much as possible.
- Protect data properly against hackers.
- Have firm rules about interlinking data.
- Store data reliably, set firm rules for this and do not keep data in storage for too long (to prevent future misuse).

The discussion about privacy-by-design is closely linked to discussions about privacy-related legislation and regulations, such as the GDPR. Generally speaking, people have positive views of such legislation and regulations as instruments that provide guidance for both technology and supervisory tasks. They understand the importance of these guidelines and agree that data collection should always comply with national and international legislation.

4. Citizens do not want the employment of sensors to lead to a reduced amount of presence of and contact with police officers.

Some focus group participants were concerned that using sensors would lead to there being fewer officers on the streets. There are two sides to this argument. First of all, people fear that the expense involved in using sensors will put a strain on the police budget and affect the size of the force.

Second, they are afraid that sensors will automate policing and replace the deployment of officers on the streets. In their discussions of policing or police deployment, the focus groups often meant ‘officers on the streets’, and not police data analysts. Various participants find a scenario in which sensors replace officers on patrol and ‘people sit behind screens’ an unattractive prospect. To maintain public trust in the police, it is important not to use sensors at the expense of trust-building police services, such as the physical presence of police officers on the streets and human contact between people and officers.

5. Citizens want the police to be both innovative and effective in the employment of sensors.

People think that technology allows the police to operate more effectively and efficiently, thereby increasing the force’s ability to catch criminals and to gather more information for investigations. They expect the police to be innovative enough to continue fighting modern crime. Several focus group participants did wonder whether the police could handle such innovations and whether the force had the right people for it. When the police use sensors, people expect them to do so effectively and to follow up on the alerts and data. They recognise that sensor technology has potential but would regard it as a waste of tax-payer money and harmful to public trust in policing if the police were unable to use sensor data effectively.

6. The use of sensors may not lead to discrimination.

People want sensors to be used fairly and to be programmed to preclude prejudices and false assumptions. Some believe that the use of technology can eliminate bias. Others, however, worry that the way sensor systems are programmed will increase the risk of re-arrest or re-prosecution for people and population groups who have been in repeated trouble with the law. The issue of discrimination and ethnic profiling should therefore be prioritised in sensor deployment, and the police must use sensors in a manner that safeguards the right to equal treatment.

7. Ensure personal freedom by restricting the use of sensors for security purposes to unsafe situations and crowded public places.

This study shows that public acceptance of sensor use depends on the context, specifically the level of security and the setting. People are often prepared to accept the use of sensors in unsafe situations and crowded public spaces for security reasons. They find security sensors less acceptable in a private setting or normal public places and when they regard the situation there as safe or slightly unsafe. In those cases, they prefer not to be constantly 'watched' by sensors because such surveillance may curtail their personal freedom or the exercise of that freedom (e.g. the 'chilling effect'). Indeed, many people are prepared to put up with minor inconveniences (short-lived noise) and relatively minor offences (litter) to safeguard their personal freedom. They want the police to exercise restraint when using sensors in such situations.

As for sensors used to promote quality of life (e.g. to determine whether a rubbish bin should be emptied, or to alert cyclists to empty parking spaces), people are more willing to accept them in quiet settings and close to home, provided that they do not collect too much data on personal traits. It is important to them that those recording personal data should exercise restraint. They worry about how such data might be used in the future.

8. The foregoing rules equally apply to cooperation between the police and other parties.

When it comes to sensor deployment to promote security and quality of life, people trust the police more than private parties. Their reasons are: the police are not motivated by profit, they have a stronger sense of values, they are more closely regulated than the private sector, and their methods are more transparent than those of commercial parties. People fear that cooperation between law enforcement and businesses will be detrimental to important values such as privacy and transparency and their democratic rights. This particular perception has implications for cooperation between the police force and private firms. Important in such contexts is for the underlying reason for the cooperation to be clear, for privacy-by-

design principles to prioritised (for example personal data protection and data minimisation), and for the cooperation to be underpinned by public values.

Literature review

Berg, J. ter & Y. Schothorst (2010). Het EPD: opvattingen van burgers. Verslag van een focusgroeponderzoek. Den Haag: Rathenau Instituut.

Biesiot, M., Jacquemard, T., Van Est, R. (2019) Overal ogen en oren. De inzet van sensordata voor leefbaarheid en veiligheid. Den Haag: Rathenau Instituut.

Biesiot, M., de Bakker, E., Jacquemard, T., Van Est, R. (2019) Hoe kijken burgers naar het gebruik van sensordata voor leefbaarheid en veiligheid? Den Haag: Rathenau Instituut.

Boenink, M., T. Swierstra & D. Stemerding (2010). 'Anticipating the interaction between technology and morality: A scenario study of experimenting with humans in bionanotechnology'. *Studies in Ethics, Law and Technology* 4, nr.2, pp. 1-38.

Déville, W. & T.A. Wiegers (2012). *Herijking stedelijke achterstandsgebieden 2012*. Utrecht: Nivel.

Elliott J, S. Heesterbeek, C. Lukensmeyer, N. Slocum & S. Steyaert (2006). *Participatieve methoden: Een gids voor de gebruikers*. Brussel: Vlaams Instituut voor Wetenschappelijk en Technologisch Aspectenonderzoek.

Elzen, B., F. W. Geels & P. S. Hofman (2002). *Sociotechnical Scenarios (STSc)* Development and evaluation of a new methodology to explore transitions towards a *sustainable energy supply*. Twente: Universiteit Twente.

Est, R. van (2004). *Dictaat: Toekomstverkenningen en socio-technische scenario's*. Eindhoven: Technische Universiteit Eindhoven.

Est, R. van & J. Gerritsen with the assistance of L. Kool (2017) *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE).* The Hague: Rathenau Instituut.

Est, R. van, E. de Bakker, J. van den Broek, J. Deuten, P. Diederen, I. van Keulen, I. Korthagen & H. Voncken (2018). Waardevol digitaliseren – Hoe lokale bestuurders vanuit publiek perspectief mee kunnen doen aan het 'technologiespel'. Den Haag: Rathenau Instituut.

Ferrari, A. et al. (2018). Additive bio-manufacturing: 3D printing for medical recovery and human enhancement. Brussel: Scientific Foresight Unit.

Jong, S. de, J. Smit & L. van Drooge (2016). 'Scientists' response to societal impact policies: a policy paradox'. *Science and Public Policy* 43, nr.1, pp. 102-114.

Kitzinger, J. (1994). 'The methodology of focus groups: the importance of interaction between research participants'. *Sociology of Health & Illness* 16, nr.1, pp. 103-121.

Kosow, H. & R. Gaßner (2008). Methods of future and scenario analysis: Overview, assessment, and selection criteria. Bonn: Deutsches Institut für Entwicklungspolitik.

Krueger, R. & M. A. Casey (2000). *Focus groups: A practical guide for applied research*. Californië: Sage.

Kruijff, A. W., & R. F. Schreuder (1999). *Toekomstscenario's voorspellende geneeskunde*. Den Haag: Rathenau Instituut.

Meulen, B. van der, P. M. Pont, P. Faasse, J. Deuten & R. Belder (2015). Keuzes voor de toekomst van de Nederlandse wetenschap: Analyse van beleidsopties bij vier scenario's. Den Haag: Rathenau Instituut.

Morgan, D. L. (1996). 'Focus groups'. *Annual Review of Sociology* 22, pp. 129-152.

Morgan, D. L. (1998). *The focus group guidebook*. Californië: Sage.

Notten, P. W. F. van, J. Rotmans, M. B. A. van Asselt, D. S. Rothman (2003). 'An updated scenario typology'. *Futures* 35, nr.5, pp. 423-443.

Schothorst, Y. (2014). Burgers over thema's voor het werkprogramma 2015-2016 van het Rathenau Instituut. De resultaten van een kwalitatief onderzoek. Amsterdam: Veldkamp.

Schuijff, M. & G. Munnichs (red.) (2012). *Goed, beter, betwist. Publieksonderzoek naar mensverbetering*. Den Haag, Rathenau Instituut.

Schwartz, P. (1991). *The art of the long view*. New York: Doubleday.

Sim, J. (1998). 'Collecting and analyzing qualitative data: Issues raised by the focus group'. *Journal of Advanced Nursing* 28, pp. 345-352.

Stewart, D. W., P. M. Samdasani & D. W. Rook (2007). *Focus group: Theory and practice*. Californië: Sage Publications.

Appendix 1: Focus group procedure

General introduction (25 min)
Getting acquainted (10 min)
Welcoming remarks
Moderator explains 'ground rules':

- Asks participants to speak out, we're interested in your opinion and why you think as you do. There are no right or wrong answers and we don't always have to agree – in fact, don't hesitate to say you disagree with someone's opinion.
- Recording session to study *what* was said later. We will not report *who* said what.
- Anonymity
- The organisations commissioning the research signed a statement in advance undertaking to deal confidentially with information shared in the group.
- Brief round of introductions (first name, occupation/daily activities, family status).

Attitude towards sensor technologies and the police (15 min)
Moderator: today we are going to talk about sensors: instruments that are used to improve quality of life and security. We want you to tell us what you know about them, what you think of them, and how we, as a society, should deal with them.

- Before I go into more detail, I would like to ask you what first springs to mind when we refer to using sensors to improve security and quality of life.
- Offer information on sensor technologies
- Moderator: I have a brief definition here of what it means to use sensors to improve quality of life and security.

INFORMATION ON SCREEN; moderator reads text out loud:

We see a lot of cameras on the streets. Altogether, local governments and the police force operate about 4,000 security and surveillance cameras in public places. Shops, businesses and private individuals have even more cameras to secure their business premises and homes. The police are keen to access their images when investigating a crime.

Moderator:
What do you think of using sensors to improve quality of life and security? Are there advantages? Are there disadvantages?

Again: we want to hear *YOUR* opinion. There are no wrong answers.

Moderator: Any discussion of quality of life and security soon turns to the role of the police.

- Can you tell me what you expect of the police, in general? (When does the force do its job properly? When are you satisfied with the police? To what extent to you consider the Dutch police force trustworthy?)

INFORMATION ON SCREEN; moderator reads text out loud:

Sensors are devices that measure and collect input from the physical environment. Examples include cameras, microphones and your smartphone's GPS receiver. These sensors generate certain data, for example about your location, but they also supply camera images and sound recordings. Today we are discussing the use of sensors to improve quality of life and security. Quality of life refers to minor infractions, such as littering. Security concerns more serious crimes that make people feel unsafe, such as mugged or threatened with physical violence.

Round 1: Option A 'More mobile' or Option B 'Smarter'

OPTION A: 'More mobile' (45 min)
Moderator: Now we're going to talk about a specific type of sensor: a camera.

Example 1: camera surveillance using stationary cameras (20 min)
Question (general impression):

- What do you think about the police viewing the camera images recorded by private individuals and businesses to help them track down suspects?

INFORMATION ON SCREEN; moderator reads text out loud:

The police are testing real-time, i.e. live, surveillance using security cameras set up by private individuals. People who live in a neighbourhood in Amersfoort where there have been a lot of break-ins have received money from the local authority to install security cameras. The cameras are trained on places where there is frequent criminal activity. To protect people's privacy, the surroundings are obscured. The police have permission to watch the live camera feed online at agreed hours of the night. They receive an alert when a camera detects movement. It could be a car thief or burglar, but it could also be someone coming home late, or even a fluttering spider web. The police can watch in real time and decide whether they need to intervene.

Questions:

- What do you think about the police watching live images from people's private security cameras so that they can spring into action in suspicious situations?

- What are the advantages, and what are the disadvantages?
- What do you think about a private security firm being able to watch live camera feeds?
- Where relevant: why is this different in your opinion?
- Where relevant: at what point does this become acceptable/unacceptable?

Example 2: surveillance using mobile cameras (20 min)
INFORMATION ON SCREEN; moderator reads text out loud:

Mobile cameras are also used as surveillance devices nowadays. The police are currently testing 'body cams', video cameras that they attach to their uniforms. The officers decide for themselves when to turn on the camera and what to record. The body cam is meant to observe people's behaviour and how officers and the public interact. The purpose is to prevent aggression and to help the force investigate and collect evidence.

Questions:
- What do you think about being filmed on the street by a police officer wearing a body cam?
- What are the advantages, and what are the disadvantages?
- And what do you think about railway security staff wearing body cams at train stations and on trains? What about a pizza delivery driver, as protection against being robbed?
- Where relevant: why is this different in your opinion?
- Where relevant: at what point does this become acceptable/unacceptable?

INFORMATION ON SCREEN; moderator reads text out loud:

Private citizens also have mobile cameras, i.e. on their smartphones. They can use them to record burglars or suspicious individuals in the neighbourhood, and then post the images in a local WhatsApp group or on Facebook, asking if someone recognises them. The person they have photographed or filmed is often identifiable.

Questions:
- What do you think about ordinary people videoing suspicious or unsafe situations with their smartphones?
- What are the advantages, and what are the disadvantages?
- What do you think about people 'taking the law into their own hands' this way?
- Where relevant: at what point does this become acceptable/unacceptable?

OPTION B: 'Smarter' (40 min)
Moderator: We're going to continue our discussion by focusing on a specific type of sensor: a 'smart' camera. Smart cameras record images but also have software

that analyses these images. Some smart cameras have other functions as well, for example they can alert the police. Our first example concerns cameras with automatic facial recognition.

Example 1: automatic facial recognition (20 min)
INFORMATION ON SCREEN; moderator reads text out loud:

> One well-known example of automatic facial recognition is on Facebook. If you post a photograph of someone on your Facebook page, Facebook tags that person by comparing the new photograph with other photographs you posted and tagged earlier. You can then confirm whether or not the new photograph is of that person. Facial recognition may also be a feature of surveillance cameras. In that case, the software compares the live images with the images stored in a database.
>
> Schiphol Airport is testing an automatic facial recognition system. Once the system has stored an image of a passenger's face in its database, the passenger can check in without producing their passport. To do so, they pass through a special security checkpoint that has a camera equipped with facial recognition software. The system is meant to speed up security checks and shorten waiting times.

Questions:
- What do you think about cameras with facial recognition being used at the airport?
- What are the advantages, and what are the disadvantages?

INFORMATION ON SCREEN; moderator reads text out loud:

> The police force could also use cameras with automatic facial recognition. By recording passers-by in a retail zone and having software compare these to images in a database, the police can detect known shoplifters and pickpockets or other known suspects and decide whether to take action on that basis.

Questions:
- How would you feel if law enforcement filmed you on the street using cameras with automatic facial recognition?
- What are the advantages, and what are the disadvantages?

Follow-up questions:
- Can you explain why you find it acceptable or unacceptable for Facebook, Schiphol Airport or the police to use automatic facial recognition?
- Why do you think that?

- (Where relevant: If I understand you correctly, you find it acceptable on Facebook because you yourself decide whether to post a photograph. What about the other examples?)
- Where relevant: at what point does this become acceptable/unacceptable?

Example 2: automatic behaviour recognition (20 min)
Our second example concerns cameras with automatic behaviour recognition.

INFORMATION ON SCREEN; moderator reads text out loud:

Studies are under way using smart cameras that can recognise suspicious behaviour. such as suspicious walking or activity patterns. Pickpockets, for example, move around the streets differently than normal shoppers. Such cameras make it possible to detect suspicious behaviour in crowded areas like shopping malls. The camera system then issues an alert that the police can act on.

Questions:
- What do you think of using cameras with automatic behaviour recognition in a shopping district, for example
- What are the advantages, and what are the disadvantages?
- Can you explain why you find it acceptable or unacceptable for the police to use cameras with automatic behaviour recognition?
- What about security firms using it, for example at a clothing shop? How does this differ?
- Where relevant: at what point does this become acceptable/unacceptable?

Follow-up question:
- Moderator: Some people object to smart cameras because they question whether face and behaviour recognition systems work faultlessly and with 100 percent accuracy. An error could lead to an innocent person being unjustly accused of something.
- Question: Does this change your mind about the use of smart cameras?

Round 2: 'More elaborate' (45 min)

Moderator: In the first round, we discussed examples of one particular type of sensor: camera surveillance/smart cameras. In this round, we'll be talking about situations involving all sorts of different sensors. The first example is the smart store.

Example 1: the smart store (15 min)
SCREEN VIDEO WITH DUTCH SUBTITLES

Question:
- What do you think of the smart store? Would you shop for groceries here?

Moderator: now we're going to give you a more detailed description of the technology used in the smart store.

INFORMATION ON SCREEN; moderator reads text out loud:

> The smart store has sensors that monitor everything. Customers are photographed upon entering and can then be tracked through the store by cameras with facial recognition. Weight sensors and cameras detect whether items have been removed from the shelves. Wi-Fi trackers monitor customer movement patterns by picking up signals from their smartphones.
>
> Amazon knows precisely what customers put in their bag, what they return to the shelf, and which products they are unsure about. Virtually everything that customers do in the store is recorded. Amazon can use this information to send them personalised advertisements. When customers leave the store, the amount they owe is deducted automatically from their account just a few minutes later.

Questions:
- What do you think about all these sensors in the store?
- What are the advantages, and what are the disadvantages?
- What is a company like Amazon permitted to do with the data it collects about you?
- Where relevant: at what point does this become acceptable/unacceptable?

Example 2: the smart city (20 min)
Moderator: we've just had the example of the smart store. Our next example is the smart city.

INFORMATION ON SCREEN; moderator reads text out loud:

Amsterdam, Eindhoven and other urban centres are working with IT companies and the police to improve quality of life and security in the city using smart innovations. Local governments are using sensors to collect all sorts of data for this purpose. They include:
Wi-Fi trackers that track motorists' mobile phones to detect heavy traffic. Motorists are automatically directed to the nearest free parking space.
Cameras that count how many people are walking around the city centre, to manage pedestrian traffic.
Smart lampposts fitted with microphones that measure noise levels to detect quarrels in the vicinity.
Software that analyses posts on Twitter, Facebook and other social media.
A rash of negative posts on Facebook may, for example, suggest that rioting is imminent.

Questions:

- Would you live in a smart city like this? What are the advantages, and what are the disadvantages?
- What do you think of the different types of sensors that local governments are using? Is there a difference between camera surveillance, lampposts fitted with microphones, and Wi-Fi tracking of smartphones? How do they differ, in your view?
- In this example, it's local government using sensors to collect data. How do you think the police would be able to these data?
- Follow-up question: in which situations, for which purposes, and concerning which groups of people do you think the police should be allowed to use the data? At what point does it become acceptable/unacceptable?
- By cleverly combining and analysing data from different sensors, the police get hold of more information. They can check out a situation sooner that way and intervene when necessary. What do you think about the police combining these types of data? For example, if Facebook posts show that people are upset about an event or occasion and that crowds are on their way there, then the police can intervene sooner to prevent a confrontation or brawl.
- Do you think the police should be permitted to use all the public data on your Facebook page when monitoring posts on social media?
- What do you think are the main differences (and similarities) between collecting data in a smart store and collecting data in a smart city?
- Where relevant: at what point does this become acceptable/unacceptable?

Closing remarks (5 min)

Moderator: We are doing our research for the Rathenau Instituut in The Hague.

Co-moderator: The Rathenau Institute studies how science and technology influence society. It makes the public and politicians aware of the awkward questions and difficult decisions involved.

Moderator: The Rathenau Instituut is doing this research at the request of the police. The Rathenau Instituut will be writing a report on the results. The police want to use the results to spark a debate, both inside and outside their organisation, about the sensible use of sensors.

During the discussion, we were observed by Rathenau Instituut and police employees in the adjoining room.

(If there is enough time) Observers' questions.

Appendix 2: Advisory committee

- Erwin Muller (chairperson), Leiden University and member of Rathenau Instituut board
- Hans Boutellier, Verwey-Jonker Instituut
- Leen van Duijn, KLM
- Cecile Kosterman, Dutch national police force
- Jack Mikkers, Mayor of ‘s-Hertogenbosch
- Ido Nap, Dutch national police force
- Evelien Tonkens, University of Humanistic Studies
- Rob van de Velde, Geonovum
- Rejo Zenger, Bits of Freedom

Appendix 3: Detailed rules

Literature review	Focus group research	Rules
'Sensor technology'		
Type of sensor (data)	Participants are more critical of new forms of technology than of familiar technology. That is in part because they are uncertain about how such technology actually functions.	Tell the public the purpose of (new) sensors and explain how they work. People would like to be able to take for granted that privacy-by-design principles are applied.
invasiveness (sense of intrusion, level of personal information)	Privacy is important to participants. They recognise that there is tension between privacy and security.	Choose solutions that collect data on as few personal traits as possible; for example, make sure that data is anonymised whenever possible.
Privacy-by-design	Participants do not use the term 'privacy-by-design', but do mention various related conditions that they feel should be imposed on the use of sensors (see Social practice).	People would like to be able to take for granted that privacy-by-design principles are standard.
	Participants stress that the technology should be effective.	Technology must be effective. The public will not accept any ambiguity about the purpose of the technology or confusion about what happens to sensor data.
'Social practice and actors'		
Operator (public/private)	Participants trust the police force more than private parties when it comes to the use of sensors.	Make public values central to cooperation with private parties so that such cooperation does not undermine trust in the police.

Literature review	Focus group research	Rules
Purpose and proportionality	Most participants have a favourable attitude towards using sensors if the purpose is clear. The legitimacy of sensor deployment depends on the level of security (safe, slightly unsafe, very unsafe) and the setting (private,	Use data for the agreed purpose.

	quiet public place, crowded public place).	
Combination of technical and social methods	Sensors should not be deployed at the expense of police officers on the streets.	Make sure that the sensor data value chain includes human contact.
Effectiveness	Participants stressed the importance of police follow-up. They expect the police to be capable of using modern technology effectively and to use technology that will improve public safety.	Make sure there is follow-up.
□Opt-in approach	□Participants would like to have a say in whether they are being monitored and whether sensors are being used in their immediate surroundings.	Give people as much choice as possible about being monitored and the use of sensors in their immediate surroundings.
Transparency about purpose and how sensor data are dealt with, including data protection, accountability and access to data	Participants want to know what sorts of sensors the police are using, what they are using them for, and what happens to the sensor data they collect.	Be transparent about how the collected data will be used.
Privacy-by-design practices□ (purposeful data collection)	People want data to be as anonymised as possible, to be secure, and for sensor data collection to be proportional and minimal.	Protect data properly against hackers.
	The police must treat all people the same. Discrimination must□ be precluded.	Treat everyone the same and make sure the technology does too.

Literature review	**Focus group research**	**Rules**
'Societal and institutional context'		
Institutional trustworthiness	Most of the participants see the police as very trustworthy. Participants trust the police force more than private parties when it comes to the use of sensors.	Keep data-sharing with third parties to a minimum, especially commercial parties. Have firm rules about interlinking data. Store data reliably.
	Participants also think about the future political climate and government. They wonder whether sensors, which are legitimate in the	Do not keep data in storage (for too long) (to prevent future misuse, for example infringements of privacy).

	current political context, could be misused under a different regime.	
Regulations and their supervision	Participants want sound privacy legislation important and want it to be enforced properly on the ground.	Always collect data in compliance with national and international law.

Contact information
Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut