Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: "Towards a European framework for integrated decision making"
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable D2.2:
Report on mutual shaping processes between technologies and conceptions of security

Authors:	Govert Valkenburg, Irma van der Ploeg (Zuyd University), Arnold Rosendaal, Noor Huijiboom, Anne Fleur van Veenstra(TNO)
Reviewers:	Rachel L. Finn (Trilateral), Michael Friedewald (Fraunhofer ISI)

Dissemination level:	Restricted to a group specified by the consortium
Deliverable type:	Report
Version:	1.0
Due date	31 January 2013
Submission date:	26 March 2013

CONTENTS

PART I: ANALYSIS

PART II: CASE STUDIES

LIST OF ACRONYMS

AMS	Active millimetre-wave scanner
ANPR	Automatic number plate recognition
ATD	Automatic target detection, automatic threat detection
CBP	College Bescherming Persoonsgegevens (Dutch watchdog for the protection of personal information)
CI	Critical infrastructures
DPI	Deep packet inspection
DSM	Demand-side management
DSO	Distribution system operator
ICS	Industrial control systems
ICT	Information and communication technology
ISP	Internet service provider
IT	Information technology
OT	Operational technology
PBD	Privacy by design
PRISMS	Privacy and Security Mirrors
SCADA	Supervisory control and data acquisition
TSO	Transmission system operator

EXECUTIVE SUMMARY

This report presents the results of a study into the mutual shaping of sociotechnical practices and conceptions of privacy and security. As deliverable 2.2 of the PRISMS project, the report materializes task 2 of work package 2. The report consists of a general analysis (part 1), accompanied by five self-contained case studies (part 2).

Building on five case studies, the report articulates how different privacies and securities are engendered in various sociotechnical practices. Rather than approaching privacy and security as values that are defined through theoretical inference, the present study approaches them as values that emerge in practice. By closely looking at what people say and do, what technologies allow people to say and do and what technologies do themselves, it is charted what privacy and security *de facto* consist of.

The case studies are conducted within the tradition of *actor-network theory*. Central to this tradition is the idea that for a proper understanding of how histories unfold, equal attention should be paid to the roles played by human beings and to the roles played by things, machines, animals, laws of nature, etc. Thus, it matters not only what people make of privacy and security in their discussions, politics, and social interactions, but also what devices do, how the state of affairs in technological development makes some things possible and others impossible, and how practices are arranged around those technologies.

Thus, highlighting the roles played by technologies as well as people, the case studies make clear that the meanings of privacy and security are *inscribed* in sociotechnical practices: they are contingent upon what arrangements in these practices allow and disallow. In turn, these arrangements are (also) the consequence of how ideas of privacy and security are *translated* into product requirements, procedures, and assignment of responsibilities. The ways privacy and security issues are made into particular *problem definitions*, serve as important points of observation in the case studies. As different definitions of privacy and security are articulated, by consequence also different relations between privacy and security come to existence.

Case study 1 concerns *active millimetre wave scanners*, a particular type of body scanners deployed at airports. Characteristic for these scanners is that they are able to locate 'suspect' elements and indicate those on an abstract mannequin picture, without actually showing the body of the scanned passenger. While these scanners are presented as a non-privacy-invasive method of investigating the passenger's body and what is carried upon it, the case study shows that the elimination of nude pictures comes at the cost of novel concerns of privacy. In particular, medical conditions in passengers are leading to new discomforts. Thus, privacy issues are not merely eliminated, but rather translated into new problems, entailing a displacement of costs and benefits.

Case study 2 interrogates *automatic number plate recognition* (ANPR). Described in uncritical terms, the system records and recognizes the licence plates of cars at various locations, after which inferences of some sort can be made by automatic mechanisms, regarding e.g., the speed of the vehicle, air pollution at specific positions, and road safety considerations such as the time a driver has been driving without a break. Privacy considerations are generally addressed by specifying data retention periods. In practice, what ANPR systems do is a whole lot more complex than reading plates and issuing speeding tickets. Their sociotechnical layout reverses the presumption of innocence: people are

considered suspects, until their ANPR data is concluded to provide no evidence of illegal action. This is thus a very specific translation of security.

Case study 3 addresses privacy and security issues in *smart grids* and *smart meters*. One on-going development in the electrical energy infrastructure is the proliferation of the data that is used in the operation of the network. Part of this data concerns the energy use of end consumers; part of it concerns the operation of the network at the macro level. Both levels have their own vulnerabilities, as well as their own opportunities for new applications and business propositions. Opportunities include enabling the end user to attune their energy consumption to e.g., fluctuating supply, and making more efficient use of energy transport networks. Threats include the profiling of end users through the abuse of their data, and cyber terrorist attacks on the stability of the energy network. Through the sociotechnical arrangements in smart grids and smart meters, security and privacy get primarily shaped as forms of data protection, data minimization, segmentation and role separation.

Case study 4 investigates *deep packet inspection* as a method for Internet surveillance was the subject of the fourth case study. The method is used to inspect private communication in an allegedly non-privacy-invasive way. Since the modern age, letters and other forms of communication have been subject to a regime of secrecy. However, at the level of bits and bytes that are transported over the internet, it is not obvious which data must be thought of as 'concealed' like the content of an envelope, and which as 'overt' like the address information on the outside of the envelope. From a technical perspective, there is no difference between the two. Indeed, deep packet inspection subjects both the content and the address information of packets, i.e., the 'chunks' into which any form of data is split before it is sent over the Internet, to analysis. In this case, privacy is apparently thought of as including 'analysing data content by not doing anything meaningful with it'.

Case study 5 examines *biometric access control* and the issues that surround it. Biometric technologies are inherently paradoxical. On the one hand, they harness the uniqueness of human body properties in favour of identifying persons with a high degree of certainty. Through this connection to particular identities, biometric data become imbued with social consequences, and thereby very much a personal form of data. On the other hand, numerous measures are taken to arrange biometric data such that it becomes void of any social or other consequences: by technically transforming them such that they cannot be connected to the individual they derived from, or by embedding their use organizationally in such a way that nothing can be 'done' with the biometric information. In this case, the privacy problem is translated into the challenge of making data void of consequences. The security problem, in turn, is translated into some form of identity verification, with all the ambiguities that are congenital to biometrics.

Part I: Analysis

1 INTRODUCTION

Privacy and security are not singular concepts. To the question 'What is privacy?', or 'What is security?' for that matter, no single answer can be given. Instead, each situation in which privacy matters may require a different answer. Sometimes one situation can raise privacy issues that invoke different or conflicting ideas of privacy. The following examples raise the question of how much help such a definition is. (The examples are based on actual findings, but small modifications were made in order to create telling examples. Therefore, they can best be seen as very plausible fiction.

> ***Biometrics securing cargo***
> *A truck driver enters the compound of a major stevedoring company in a sea port area. Upon entering the compound, he inserts his personal chip card in a reader and places his left hand in a hand geometry scanner. The system measures the hand geometry and encrypts the results through a mathematical algorithm, which are then sent to the card chip. If the encrypted data matches the recorded data on the card, the card releases information regarding the formal identity of the driver, the cargo company he works for, and the safety-training certificates he holds that are necessary for handling hazardous goods. The same system is deployed by numerous companies across the whole port area. No connection to a centralized database is necessary, as all relevant information is contained on the card. Thus, no central log can be kept of which driver enters exactly which compound. At the same time, the stevedore has ascertained that cargo has shipped with the right driver.*

> ***Licence plate recognition for a safer road***
> *A car passes an automatic camera, and a snapshot is taken of the front of the car. Not because the driver of the car is speeding or doing something wrong, but because a snapshot is taken of every car that passes. An automated process distils the licence plate number from the picture. A similar system a few kilometres ahead does the same, and from the time elapsing between the two passes, the average speed is calculated, leading to a fine being issued if the speed is too high. If, on the other hand, no speeding is observed, the picture and accompanying data could be destroyed. That is right, it* could *be; but it is not. It turns out that the data collected by such systems offer a gold mine for purposes of criminal investigation. Patterns in persons' movements might be indicative of particular forms of crime, such as theft from trucks parked on highway parking lots. Police are continuously looking for new ways to deploy the scanned number plates in their crime-fighting tasks, and they are pushing the limits of how long data can be stored legally.*

In these two small examples, which were loosely inspired by the empirical research on which this report is based, do not represent straightforward examples of what privacy is. In either case, privacy is not simply a 'right to be let alone'. In the first case, what an individual discloses to a corporate party is limited to a formal identity and safety certificates. It explicitly does not include the whereabouts of a driver, and the system configuration is such that these whereabouts are impossible to distil from all the informational interactions in the system. Privacy here comprises invisibility of moment, but not invisibility in a particular place. Contrastingly, what enters the system from the licence plate recognition system is *exactly* the whereabouts of a person. Maybe one's whereabouts are discarded in case no traffic offence is

committed, but they may just as easily be retained longer. What is more, they are not anonymous, because licence plates are connected to specific vehicles, and it is only a small informational step to the owner of that vehicle. Also, the driver's portrait is likely to be available on the photograph. Privacy here consists of the right to have one's data deleted, but in practice it also turns out that this right is easily compromised. These two different examples show that what privacy exactly is, depends strongly on how technologies are configured, how people operate these technologies, which problem the technologies were originally developed for (i.e., cargo administration vs. traffic law enforcement), etc. The social and technical arrangements that ultimately determine the exact definition of concepts such as privacy and security are at the core of this research report.

The present document presents the aggregated results of five case studies into privacy and security technologies, conducted as task 2.2 of the PRISMS project. Each of the case studies examines one technology or class of technologies and questions the forms of privacy and security to which they are correlated. In the case studies, the concepts of privacy and security are investigated empirically as arrangements that are constructed in practice, not as moral values from the book. This document thus complements the exploration of on-going developments, conducted as task 2.1 of the PRISMS project. The combination of macro and micro analyses provides contextual knowledge for the pan-European survey conducted in Work Package 9.

The micro-perspective part of this study articulates the particular forms of privacy and security that emerge in these sociotechnical practices. Rather than seeing privacy and security as singular and fixed ideas, this research views them as multiple, situated and contingent. In each situation, the concepts of privacy and security describe or refer to different content. Many elements potentially play a role in the shaping of these particular privacies and securities: human persons with their interests, socio-cultural structures and routines, as well as technological artefacts, infrastructures and technological standards. By bringing these elements into view in various case studies, we demonstrate *that* privacy and security are multiple concepts, and *how* they emerge in such multiplicity.

The case studies presented in this report were guided by an interest in how privacy and security are shaped in various social and technical practices associated with various privacy and security technologies. More concretely, the case studies investigated how people, procedures, routines, technological artefacts and social structures – even if technological artefacts and social structures are often hard to disentangle – contribute to particular constructions or 'enactments' of the concepts of privacy and security.[1] Also, the case studies identified what meanings people attribute to these concepts, both from a more abstract perspective and from the perspective of their connectedness to the particular practice. The purpose of the studies was not to produce a systematic, comprehensive account of privacy and security – neither as a taxonomy that conclusively specifies all kinds of privacy and security that could emerge, nor as an anatomy that specifies all their elements. Rather, the purpose was to produce an inventory of rich accounts of constructions of privacy and security, in order to offer a broad conceptual base by which problems, challenges or best practices around privacy and security can be captured.

[1] For the concept of 'enactment' see Law, John, "Enacting Naturecultures: a Note from STS", Centre for Science Studies, Lancaster University, Lancaster, 2004. http://www.lancs.ac.uk/fass/sociology/papers/law-enacting-naturecultures.pdf. The paper includes many references to seminal texts by a.o. Annemarie Mol, Bruno Latour and Donna Haraway.

This document is structured as one integrated overview of research results, complemented by five appendices that can be read as self-contained case studies. The first case study discusses body scanners for airport security, in which a specific take on what is private about the human body comes to the fore. The second case study concerns automatic number plate recognition. By scanning and processing the licence plates of cars, these systems transform the way in which movement through public spaces is understood culturally. Third, smart grids, smart meters, and how they function as critical infrastructures are discussed. This study sheds light on how information on customers' energy usage can be (ab)used as well as protected. The fourth case is concerned with so-called deep packet inspection, a technique for surveillance of internet traffic. This case shows that it is far from obvious what privacy and security consist of when data communication is concerned, and that different interests favour different technological configurations, entailing different conceptions of privacy and security. The final case study discusses biometric access control. Biometric access systems record properties of the human body, and use the (high degree of) uniqueness of these properties to verify the identity of a person and grant them access rights. Importantly, the case studies are not confined to very specific situations or devices, but rather address coherent clusters of closely related practices, thus attaining a broader scope.

The cases show a range of different versions of privacy and security, or rather: a range of different privacies and securities. While it is neither possible nor desirable to draw universal conclusions from a small number of case studies, some common structures can be discerned at a more abstract level. For example, in cases in which technologies are presented as *increasing* privacy or security, a closer look often reveals that they rather *substitute* existing privacies and securities with *different* ones. These substitutions might in the end be improvements, but they are never *simply* improvements of what was already there. They incur displacements of tasks and responsibilities, revision of criteria and categorizations, and forms of privacy and security that may not even resemble the privacies and securities that were there before. Also, the cases show that the widely assumed model that places privacy and security in a trade-off relation, is often significantly challenged.

The general analysis in this first part of the document is structured as follows. Section 0 further elaborates the research questions and explains the methodology. Section 3 will describe the conceptual framework in detail. Section 4 will present an overview of the observations from the case studies, from which some suggestions for further research, in particular the survey in Work Package 9, will be derived in section 0. Some general conclusions will be drawn in section 0.

2 RESEARCH APPROACH

2.1 RESEARCH QUESTIONS

The aim of this research project is to articulate *privacy and security as they exist within various practices*. As was illustrated by the two examples in section 0, the meaning of these concepts is deeply entangled with technological and social arrangements. Thus, meanings are not just a matter of what people say things mean in a particular context. Instead, in a more comprehensive sense, meanings are a matter of what people do when dealing with privacy and security related issues, what kind of events are possible or impossible, what choices are available, how procedures, laws and routines are established as well as enforced, etc. It is in these entanglements with privacy and security technologies that the concepts of privacy and security will be investigated in this report.

The entanglement of social and technical elements makes it impossible to clearly distinguish between the two. Therefore, we speak of *sociotechnical practices*, when we refer to the ensemble of elements that together impact how privacy and security are exactly shaped. We presume that behind any phenomenon, social as well as technological factors play a role, and that phenomena can only be properly understood if such social and technical factors are subsumed in one comprehensive account. In fact, in such an account, it will typically be difficult to draw a clear line between social and technical factors; there is no fundamental difference that separates them.

The main question guiding this report and the underlying case studies is *how versions of privacy and security are co-constructed with privacy and security technologies*. That is to say, whenever a privacy or security technology is designed, ideas of privacy and security are designed together with it. And conversely, ruling conceptions of values such as privacy and security will make some technological configurations more logical to appear than others. This report investigates such relations of mutual shaping between values and sociotechnical configurations, and section 3 presents a conceptual framework that helps to capture them.

2.2 RESEARCH METHOD

Given the emphasis on the interrelations between technologies and privacy and security and the multiplicity of ways these are interconnected, we focus on specific case studies in order to illuminate how privacies and securities relate to sociotechnical practices. Our research approach is largely qualitative, as it aspires to articulate meanings, particularly how these meanings are co-constructed with and within sociotechnical arrangements. As meanings are not directly observable, two proxies of meaning are investigated. First, we investigate what people *think* privacy and security to be: what elements people think these (by themselves unspecific) values consist of, to whom the values pertain, how they are or should be protected, etc. Second, we investigate how these concepts are possible to *enact* in practice: what is possible or impossible to do, and how material, organisational and social arrangements dictate a particular understanding of privacy or security.[2]

[2] From the tradition in which this approach is rooted, namely *actor-network theory*, these two should actually not be seen as 'proxies' but as actually *being* themselves meaning. However, for the present research this has no further consequences, provided that we remain aware that values are not approached as something that can be

In order to complete the particular case studies for this report, we relied upon academic sources such as journal articles and conference proceedings to gain important insights into the problems that occur within privacy and security technologies, the solutions that are proposed to them, etc. In addition, public sources such as (corporate and other) websites, media appearances and brochures provided insight into how privacy and security technologies are presented, how privacy and security are argued to be arranged in a particular way, and how such sociotechnical arrangements evolve in practice. Of course, this is not to imply a very strict separation between these kinds of sources and the purposes they serve, but rather to represent the broad empirical orientation of the research. Perhaps most importantly, through semi-structured expert interviews, we gained in-depth insight into processes of design and development, practical hurdles and solutions, and implicit practical knowledge. For each of the case studies, we conducted between five and ten interviews. The interviews in specific were open ended and anonymous, allowing for a free discussion that covered in some cases delicate and/or confidential issues. It should be noted that quotes from these interviews have been paraphrased in this report both in the following analysis and in the case studies in part 2.

Our selection of cases is intended to cover a broad range of versions of privacy and security, which have themselves been roughly divided along two dimensions. First, cases differ in the emphasis they entail on our embodied lives, or on the sphere of information and data. Second, cases differ in whether their focus is on individuals and their private lives, or on collective lives and the public sphere. The selected cases, namely body scanners, automatic number plate recognition, smart grids and smart meters, deep packet inspection, and biometric access control, offer a diverse set over the two mentioned dimensions.

conceptually established. See e.g. Akrich, Madeleine, "The description of technical objects", in Wiebe Bijker, and John Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, Mass, 1992, pp. 205-224. Akrich, Madeleine, and Bruno Latour, "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies", in W. E. Bijker, and J. Law (eds.), *Shaping Technology, Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, MA, 1992, pp. 259-264. Latour, Bruno, *Science in Action: How to Follow Scientists and Engineers Through Society*, Harvard University Press, Cambridge, Mass., 1987.

3 CONCEPTUAL FRAMEWORK

The case studies provide 'snapshots' of sociotechnical configurations: an account of how things are positioned, including human, technological and social arrangements. They focus on how things are currently arranged, not so much on the history of how things came to be situated the way they are now – though of course some historical background is indispensable to make sense of the configurations. What makes the view *sociotechnical* is the assumption that human beings and their social relations are not the sole cause of how things are (social reductionism), as well as the assumption that the course of events is not fully determined by the technologies and 'things' that happen to be around us (technological determinism). 'Sociotechnical' suggests that there is no sharp distinction, or even any fundamental difference, between social and technical entities. Phenomena that initially appear as social, will upon closer examination reveal social as well as technological causes. Similarly, artefacts that appear as technological at first sight will upon closer examination be the consequence of a mixture of social and technological causes. Indeed, the case studies will demonstrate, privacies and securities prove contingent on both technical and human causes.

In order to capture these sociotechnical configurations, the research relies upon three central concepts: inscriptions, problem definitions and translations. First, the notion of *inscription*[3] captures the idea that our behaviour, values, norms and meanings can be (rigidly or leniently) constrained by our material surroundings. This may be the result of deliberate actions by technology designers, but it may also occur in a more emergent and accidental way. Within sociotechnical configurations, 'inscription' provides an important link between on the one hand persons and on the other hand things like devices, media, and the way a practice is organized: it articulates how elements such as behaviour, the attribution of meaning and making judgment are not the merely 'human' categories they appear to be, but are in fact partly the consequence of technologies, buildings, or any other material entities surrounding us.

Second, the concept of *problem definitions* directs attention to the fact that seemingly the same problem will appear in different shapes in different situations. Because of these multiple shapings, each situation will therefore require a different approach to the problem. By articulating how people *define* the problem in a particular situation, different conceptualizations of privacy and security will be revealed. This entails that problems people engage with will emerge differently in different situations. The concept of problem definitions helps in articulating that different parties working on seemingly the same problem are at closer look working on their own 'version' of the problem.

Third, the concept of *translation* directs attention at the work that goes into making different problem definitions work in different situations. People are compelled to shape a problem appropriately across different contexts, and to recreate it in different times and places. The concept of translation captures the hard work that goes into negotiating the specifics of

[3] Akrich, Madeleine, "The description of technical objects", in Wiebe Bijker, and John Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, Mass, 1992, pp. 205-224. Latour, Bruno, *Science in Action: How to Follow Scientists and Engineers Through Society*, Harvard University Press, Cambridge, Mass., 1987. The notion of inscription is closely related to the idea of *material semiotics*. Also, it is directly related to the idea of *delegation*: routines, procedures, behavioural patterns and even morality can be 'delegated' to our material world if we arrange this world in a way that forces us to behave in no other way than according to those procedures, routines, patterns and morals. See Latour, Bruno, *La clef de Berlin et autres leçons d'un amateur de sciences*, Éditions la Découverte, Paris, 1993.

problems and their solutions, such that both become recognized in a particular situation. It is through work of translation that different definitions of seemingly the same problem remain connected.

Through the use of the concepts of inscription, problem definition and translation, the multiplicity of concepts such as privacy and security can be articulated. The concept of translation helps identifying the effort that goes into shaping privacy in a particular way, for example producing a picture without body details is largely accepted as a privacy-friendly approach to body scanning at airports. Similarly, it helps articulating that security might in one place be moulded into intercepting unwanted goods like guns and bombs, whereas in other places it rather means keeping people physically out.

Likewise, the idea of problem definitions helps articulating that in each case, different threats figure against which security is to protect. In the case of the energy infrastructure, this refers to the stable provision of energy, whereas in the case of biometric access control it refers to certifying the identity of a person. These are different problems, with different stakes and different consequences.

The concept of inscription finally captures how the content of concepts is partly dependent on material and other contextual factors. In the case of body scanners, it helps articulating that privacy *in effect* consists of alerts that are triggered even by benevolent items, forcing passengers into revealing some sensitive personal information. Similarly, with automatic number plate recognition, the concept draws attention to the behaviour ANPR promotes among drivers, which is relevant to the idea of privacy as freedom of decision.

4 CASE STUDIES IN BRIEF

The following subsections briefly present the case studies underlying this report. Each description contains a 'vignette' that is composed from insights from the case study. The vignettes do not necessarily correspond to configurations that have been observed in the real world, but utmost care is taken to give them a full degree of realism, as they are built on elements that are technically and socially possible to exist today, not on promises or expectations.[4] To acquire further insight in the constructions of privacy and security, the reader is encouraged to read the full case studies at the end of this report.

4.1 BODY SCANNERS

First, we investigated *body scanners* deployed in airport security situations, focusing on so-called *active millimetre-wave scanners* (AMS) that promise to be able to identify and render things that are carried on the body, and that are not clothes. In an abstract sense, these scanners identify *anomalies*: anything that is not typical, i.e., not human flesh nor fabric, will raise an alert. Ideally, in the context of airport security, this would only concern guns, bombs, and drugs. However, alerts are also triggered in practice by stomas and other prosthetic devices, and it has been reported that even business cards stored in one's chest pocket trigger an alert.

> *Active millimetre-wave scanners are installed at airports. In contrast to the long-established walk-through metal detectors that respond to amounts of metal above a certain quantity, the scanner is able to identify the shape of objects, a more specific estimate of the material it is made from, and with a higher sensitivity than the metal detector. By vendors as well as people in charge of security processes, the scanner is presented as increasing convenience, as security officials can now be much more specific in which passengers to 'bother' and which not. The scanner presents results to officials in the form of an abstract image, a mannequin, on which zones are highlighted that contain suspect materials and need further inspection. Vendors and policy makers argue that privacy of passengers is largely respected, because the pictures do not convey anatomical details. However, with anatomical detail, also other details are 'lost' in the process of computing the image. Consequently, the system is unable to distinguish between a stoma and a bomb belt. Therefore, the Association of Stoma Patients has negotiated with airport security offices that stoma patients may reveal themselves to custom officials prior to going through the scanner, and receive a special treatment. While this special treatment guarantees the same level of security as is achieved with other, 'normal' passengers, it also means that stoma patients are receiving a treatment that is more discomforting than before, and perceivably stigmatising at that.*

Rather than simply eliminating body properties from the process and identifying security threats, the AMS brings about a complex transformation of the practice of airport security. It may seem straightforward that bombs should be kept away from airplanes, and that this is

[4] Research activities in other work packages of the PRISMS project also use vignettes. To those activities, the present vignettes may serve as exemplars, although they were not devised with the methodology of those activities in mind but merely as showcases for the present work package.

what the scanner should reveal. However, the many steps between the waves reflecting on the body and the mannequin representation on the screen each perform smaller or larger transformations on the information, such that the final representation corresponds only in very specific ways to the original body and what is located on it. By corollary, privacy is inscribed as the revelation of very specific aspects of our bodies, and with very specific consequences of those aspects.

4.2 AUTOMATIC NUMBER PLATE RECOGNITION

The second case study focuses on *automatic number plate recognition* (ANPR). Described in uncritical terms, the system records and recognizes the licence plates of cars at various locations, after which inferences of some sort can be made by automatic mechanisms, regarding e.g., the speed of the vehicle, air pollution at specific positions, and road safety considerations such as the time a driver has been driving without a break. Privacy considerations are generally addressed by specifying data retention periods.

> *Cameras equipped with ANPR technology are installed above the lanes of an important highway corridor. They are placed on a dedicated portal on which no road signs are mounted. They are very visible. They take pictures of the fronts of cars passing under the portal, including a view of the faces of the driver and the front-seat passenger. The pictures are taken for multiple purposes. The purpose that is communicated to the public most clearly is the control of speed, as the timing of the photo is compared with the timing of a similar system a few kilometres ahead. However, prior to discarding the photos for privacy reasons, they are kept for three months. Thus, the police can analyse traffic patterns in relation to information on crimes, and subject photos to further inspection. People feel surveilled as their photos are potentially inspected even if they only behave in law-abiding ways. Even though the police explicitly disavows the use of ANPR in fighting 'petty offenses' such as a broken headlight, people increasingly opt for 'better safe than sorry' and make sure their tail lights are fixed and their seatbelts fastened. At the same time, people feel more secure, as they know the police have disposal of a new technology that makes it easier to track down serious criminals.*

In practice, what ANPR systems do is a whole lot more complex than reading plates and issuing speeding tickets. By their presence, they push drivers towards compliance with traffic rules. Importantly, ANPR systems may be interpreted as reversing the presumption of innocence: people are considered suspects, until their ANPR data is concluded to provide no evidence of illegal action. Additionally, ANPR systems invite police officers to mine data that might be relevant for their investigation, but that was not collected for that purpose. The security problem is here translated into the desire to trace vehicles. The privacy problem is then translated into seeking a balance between retaining and disposing of data, and into negotiating the purposes for which collected data may be put to use.

4.3 SMART GRIDS AND SMART METERS

Third, we investigated privacy and security issues in *smart grids* and *smart meters*. The electrical power infrastructure is perpetually in development. One of the current developments is a proliferation of the data that is used in the operation of the network. Part of this data

concerns the use of end consumers; part of it concerns the operation of the network at the macro level. Both levels have their own vulnerabilities, as well as their own opportunities for new applications and business propositions. Opportunities include enabling the end user to attune their energy consumption to e.g., fluctuating supply, and making more efficient use of energy transport networks. Threats include the profiling of end users through the abuse of their data, and cyber terrorist attacks on the stability of the energy network.

> *Household appliances have their own typical patterns of energy use. The power consumption by a refrigerator is different from the consumption by an electric kettle. Monitoring the total power consumption of a household at intervals of a few seconds can reveal which appliances are used at what time. While it is not plausible to regard the individual event of using a kettle as sensitive information, the whole of information on all appliances used in a household can be telling about the number of people living in it, the times at which they do particular activities, and when they are away on holiday. At the same time, fine-grained monitoring power use at 15-minute intervals also offers some benefits for purposes of power network management. The smart energy meters that are currently rolled out among households allow for such fine-grained measurements, and moreover enable measurement from a distance. In order to gain use-data for network management without revealing potentially sensitive information about households, mathematical algorithms transform use-data into data that looks like nonsense to the human eye. These pieces of seeming nonsense can then be summed over a number of households, after which the sum can be retransformed into sensible data. This offers an aggregate of fine-grained use-data, enabling advanced network management but not inspection of the use patterns of individual households.*

Through the sociotechnical arrangements in smart grids and smart meters, security and privacy get primarily shaped as forms of data protection, data minimization, segmentation and role separation. Interestingly, security is translated rather differently at different levels of the system. At the consumer level, security is translated primarily into data security; at the system level, it is mostly translated into physical security and the security of power supply: the provision of electrical power is deemed to be vital for modern life and the functioning of modern society. This is owing to the fact that at these different levels are associated with radically different security problems. By consequence, the way security is implemented differs between the levels.

4.4 INTERNET SURVEILLANCE AND DEEP PACKET INSPECTION

Deep packet inspection as a method for Internet surveillance was the subject of the fourth case study. The method is used to inspect private communication. Since the modern age, letters have been subject to a regime of secrecy, as is reflected by laws and even the constitutions of various states. Electronic forms of communication have been subject to similar regimes. For example the German constitution of 1919 already protected telephone and telegraph communication.[5] However, at the level of bits and bytes that are transported over the internet, it is not obvious which data must be thought of as ‘concealed’ like the content of an envelope,

[5] Weimarer Verfassung, "Die Verfassung des Deutschen Reichs vom 11. August 1919", Reichsgesetzblatt, Jg. 119, Nr. 152 vom 14. August 1919, S. 1383-418.

and which as 'overt' like the address information on the outside of the envelope. From a technical perspective, there is no difference between the two. Indeed, *deep packet inspection* subjects both the content and the address information of packets, i.e., the 'chunks' into which any form of data is split before it is sent over the Internet, to analysis.

> *Over the past decade, the use of data connections has moved from the periphery of mobile communication to its core. At its introduction, data plans could be offered by mobile phone companies relatively cheaply alongside mobile phone subscriptions. Revenues were primarily generated by the charges for actual phone calls and text messages. However, the different uses of data connections have proliferated, and many new services have emerged that offer keen competition to the traditional calling and messaging service. In effect, the new services have reduced revenues from traditional services, without stepping up the revenues through data plans. Therefore, phone companies have sought to offer more granular data plans, such that data use is charged higher if it more strongly cannibalizes the profitable services. DPI is used to differentiate between different kinds of service. Opponents argue that the phone companies violate privacy as it is none of the company's business to know exactly what kind of data people transmit over their data connection. Also, this use of DPI would be against the ideal of 'net neutrality', which posits that the Internet should be accessible independent of the kind of information people consume. Phone companies argue that net neutrality is respected because everything is still available, but perhaps not at the same price. Also, they argue that they do nothing with the intercepted data, other than analysing the kind of service for which the data is used.*

This case shows that privacy on the Internet is even more of a construct than in some other situations: where an envelope (kind of) naturally has an inside and an outside, there is no such thing as a naturally private or naturally public byte. In this case, privacy could be interpreted as including of 'analysing data content by not doing anything meaningful with it': as the snippets of data are not recombined and integrated into a whole, Dutch legal authorities found nothing unlawful in the use of DPI.[6] This is at least remarkable as it suggest a sensible boundary can be established between 'doing something' and 'doing something meaningful', whereas others argue that privacy consists of 'doing nothing at all with the data', which is equally remarkable as data transport by definition entails doing something with the data.

4.5 BIOMETRIC ACCESS CONTROL

The final case study examined *biometric access control* and the issues that surround it. There is something paradoxical about this type of biometric access systems. On the one hand, they harness the uniqueness of human body properties in favour of identifying persons with a high degree of certainty. Through this connection to particular identities, biometric data become imbued with social consequences, and thereby very much a personal form of data. On the other hand, numerous measures are taken to arrange biometric data such that it becomes void of any social or other consequences: by technically transforming them such that they cannot be connected to the individual they derived from, or by embedding their use organizationally in such a way that nothing can be 'done' with the biometric information.

[6] Vermeer, Reinier, "'DPI-gebruik van KPN geen strafbaar feit'", *Webwereld*, 3 August 2011. http://webwereld.nl/nieuws/107507/-dpi-gebruik-van-kpn-geen-strafbaar-feit--.html.

> *A sports club decides to replace the conventional access policy based on membership cards by the use of a fingerprint scanner. This allows members leave their wallet at home, if they want to. As the members are large in number, a multimodal scan is needed: not only the ridges of the fingerprint are sensed, also the pattern of veins in the finger-tip skin is registered. Using a fingerprint and nothing else would produce too many false readings, since comparison of fingerprints is problematic for large numbers. The biometric data, i.e., the fingerprint plus vein pattern, is stored in a central database in a coded form. The encoding of the fingerprint is unidirectional, which means that the stored data cannot be re-transformed in such a way that the original biometrics become visible. The vast majority of members are happy to use the new system and acclaim it as being convenient. The very small number of persons that held concerns still enrol after they received extensive explanation of the non-reversibility of the encryption. In scholarly papers, in many senses fairly remote from the gym, scientists have proven that known versions of 'irreversible encryption' are actually reversible if sufficient computing power is available. Nonetheless, it is argued by the gym managers that even if a fingerprint is retrieved from the data, almost nothing can be done with it.*

In this case, the privacy problem is translated into the challenge of making data void of consequences. Resulting inscriptions vary widely between biometric practices, but what they share is that always at some point, biometric data are connected to identity, which connects consequences to the biometrics. The elimination of consequences is partly pursued through technical means such as the irreversible encryption as described in the vignette, and partly through discursive strategies such as the use of particular examples, arguments and guarantees.

5 CONSTRUCTIONS OF PRIVACY AND SECURITY

5.1 BEYOND THE TRADE-OFF MODEL

One of the assumptions underlying the whole PRISMS project is that privacy and security are not mutually exclusive values, i.e., that serving privacy entails compromising security, and that providing security entails breaching privacy. Instead, this study assumes that privacy and security each emerge in between sociotechnical factors in a unique way in each situation, entailing unique and complex relations between privacy and security in each of those situations. Indeed, in the various case studies, different exemplars of such relations have been observed and articulated.

In a world in which the processing of information plays an ever more central role, it may seem straightforward to identify the primary implementation of privacy at the protection of that very information. Indeed, most case studies involve the protection of information in some way. However, the strategies of protection are radically different. For example, in the case of body scanners, protection is translated into the (attempted) elimination of properties of the body. Information on the body is presented to security officers through a series of transformations, such that supposedly no private details are revealed. At the same time, these transformations entail particular chains of behaviour that might well be qualified as breaching privacy – not in the sense of poor data protection, but in the sense of the kind of discomfort, and even perceived discrimination and violation of human dignity, that people have to go through when they are treated in particular ways. These are two different privacies, one of which is respected – not showing body details – and one of which is compromised – forcing people to go through procedures they might find humiliating.

Quite a different version of privacy is constructed in the case of automatic number plate recognition. There, privacy is typically translated into a specified retention period. This connects privacy not so much to exactly what is known about a person, but to the entitlement of that person to have that knowledge 'forgotten'. Also in this case, a technical implementation of such forgetting is only half of the story. Even if the forgetting is technically successful, what happens with the information prior to forgetting might still have considerable consequences. As the ANPR case shows, quite some delving into private lives, with important consequences, takes place before things are forgotten.

These two examples of constructed privacies – selected from the case studies – show that privacy is ambiguous. They show that there is no univocal way in which privacy would be detrimental to security. Or the other way round: there is no unambiguous sense in which security can be identified as the primary cause for violations of privacy. It is always a *particular* form of security that may or may not impede a *particular* form of privacy. In the body scanner case, privacy suffers most from the interpretation of security as "anything that is not flesh nor garment poses a threat". In the ANPR case, it suffers from a shifting understanding of security: from photographing only in case of misconduct, to photographing unconditionally. While it would still be a hasty conclusion to state that privacy is hampered by security as such, it is clear in these cases that particular *translations* of security have particular consequences, some of which may be ranked under privacy problems.

An example of privacy and security being potentially supportive of one another is found in the case of smart grids and smart meters. Initially, it was thought that the potential of

electrical power infrastructures would increase with the amount of data becoming available. However, it was immediately realized that uncritical collection of such data would incur (a general sense of) privacy problems. Increasing awareness can be discerned regarding the fact that things are more secure *and* more privacy-safe if certain measures are taken. For example, both privacy and security are, in this case, served by the fact that no data connection exists between smart meter and higher-level system elements. Also, a strict separation between different business propositions – not least instigated by the pursuit of liberalization of the energy market – entails data separation and minimization. Of course, these are not panaceas that eliminate any problem, and indeed considerable doubt and mistrust has been reported. Yet, these concern the efficacy of the solutions as such, not so much the thought that privacy and security are mutually irreconcilable.

5.2 MANY DIFFERENT PRIVACIES

Altogether, the case studies reveal a broad range of different privacies that are constructed in different contexts. To name only a few, privacy can be translated into elimination of representations of body details (AMS), into the right to have one's data deleted (ANPR), into rendering our body properties unique yet void of social consequences (biometric access control), into data separation (smart meters), or into analysing data in such a fragmented way that all meaning is lost (DPI). Additionally, this entails that no taxonomy of privacies or elements of privacy can be established. Rather, only a set of privacies can be collected that are connected through what Wittgenstein has termed *family resemblances*: properties that are not necessarily shared by all members of a collection, but that unite a number of family members into a cluster. Members belong to multiple clusters centred on various properties, and through these multiple clusters, the family is tied together. By consequence, the boundaries of the family are not that clear.[7] For example, one element that occurs in some forms of privacy, is the transformation of personal data into something that can be presented as 'irrelevant': it happens in the AMS that produces generic rather than specific body images, it happens in biometric access control where biometrics are transformed into something otherwise unusable, but it does not happen in a very clear way in ANPR. Privacy in an ANPR context is translated not into irrelevance, but into deletion.

One point of focus in privacy debates is whether certain information is personal, and whether it is privacy-sensitive. According to the legal definitions, personal information is information that can with a reasonable effort be connected to one person. This includes name and address, but also fingerprints.[8] Specific subsets of personal data are identifying personal data which on their own suffice to identify a person, and sensitive personal data which are for one or other reason considered none of others' business.[9] However, whether something is privacy-sensitive, depends on the context, how information is connected to other information, to

[7] Wittgenstein, Ludwig, *Philosophical Investigations/Philosophische Untersuchungen*, Blackwell, Oxford, 1953.
[8] Directive 95/46/EC, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data", *Official Journal of the European Communities*, L 281, 23 November 1995, pp. 31-50. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. Government of the Netherlands, "Privacy", Dutch Government, The Hague, 2013. http://www.government.nl/privacy. (Accessed: 2013.01.31)
[9] Koorn, Ronald, Herman van Gils, Joris ter Hart et al., "Privacy-Enhancing Technologies - White Paper for Decision-Makers", Ministry of the Interior and Kingdom Relations, The Hague, 2004. http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

processes and decisions, etc. The same piece of information may be sensitive in one context and not in another. Indeed, discursive games are continuously played, and technological measures are taken, to construct some personal data as not sensitive and not identifying. Even then, things remain ambiguous. In the case of body scanners, considerable effort is put in presenting data in a way stripped of all sensitive personal information. In a way, things are made impersonal. But at the same time, the only purpose that this information serves is the construction of conclusions *about the person*. What is more, the technical operations on images of the body become ever more complex, which entails that they become increasingly opaque and less intelligible for those who are not involved in their design and operation. In a way, this is a deterioration of privacy: people have less of an idea about what is happening to their data.

A similar paradox is found in biometrics. Fingerprints are unique (or at least, so we may assume for this part of the argument). Therefore, they are certainly personal (uniquely connecting to one person) and identifying (the person can be traced using the fingerprints). The fingerprints might even be sensitive: it is telling if your fingerprints are found at places where you would rather go unnoticed. However, as was argued by one operator of a biometrics access control system, fingerprints 'in the wild' are for all practical purposes not privacy-sensitive, because it would take a disproportionate effort to make them into anything usable. Also, fingerprint access systems are arranged such that (at least ideally) nothing can be done with the fingerprints after they are encrypted, rendering them to some extent privacy-insensitive.

In another example, operators of ANPR systems claim that the photos made of passing cars are not personal data: they connect to vehicles, not to persons. This claim is at least questionable from the perspective of the legal definitions of personal data. First, pictures taken by ANPR systems recognizably show drivers, which makes those pictures personal data as they connect uniquely to those drivers. Second, the ANPR data are *used* for a particular purpose, which always has consequences for individual persons. Even if this use is formally aimed at vehicles, the unique persons connected to those vehicles are only a small step away. Even if ANPR pictures are used with technical and procedural prudence, it is questionable to see them as non-personal data.

One final construction of privacy discussed here is the aggregation of data, as relates to practices surrounding smart energy meters. While data on the energy consumption of a single household might be telling about the structure and habits of that household, the combined use-data of a dozen of households tells little more than the rough number of persons living in a neighbourhood. Also aggregating data over time, i.e., collecting meter readings at a larger time interval, entails that information becomes less personal and hence less privacy-sensitive. Additionally, this practice shows numerous forms of data segmentation that are indeed aimed at making privacy less personal: the less is 'known' at a particular locus, the lower the probability that it can be traced back to a person or household (or at least so by reasonably available means), and the lower the probability that the data can be reckoned privacy-sensitive. Smart meters also bear influence on our private lives by their explicit aim at demand side management: creating awareness among consumers and shaping their energy consumption in such a way that it matches the supply. While this is as such not a violation of privacy, the interference in private decisions comprises a rearrangement of the public and the

private in some way. One type of privacy is *privacy of behaviour and action*.[10] While the meter does not, strictly speaking, challenge our autonomy in energy usage, it does change the way in which decisions are made, and therefore it has some relevance.

As elaborated in PRISMS deliverable D1.1, privacy can be classified into seven types:[11] privacy of the person, privacy of thought and feeling, privacy of location and space, privacy of data and image, privacy of behaviour, decision and action, privacy of communication, and privacy of association. However, these seven types are defined in a largely analytic style, which deflects attention from the fact that in practice, numerous versions are found, some of which are mutually conflicting, and some of which are actually conflicting with the content of the seven types. The latter are the result of stripping privacy down to its constituents, whereas the former are the result of fleshing out full accounts of all that seems to matter when it comes to enacting privacy.

5.3 MANY DIFFERENT SECURITIES

In a similar way, different securities are constructed within the case studies. In airport security, security was translated into the detection of particular materials, which unintentionally included non-flesh and non-garment elements that were not actually any security threat. Alternatively, security was translated into tracking the whereabouts of any citizen (ANPR), into separating data streams and placing them under regimes of data security (smart meters), into using the (presumed) uniqueness of body properties to identify people (biometrics), or into detecting very specific content in data communication that remains otherwise concealed.

At first sight, it seems that two referent subjects qualify well to function as a centre of gravity for an account of security: the individual person, and the state. However, as the different cases show, these two reference subjects appear differently in each practice, if at all. For example, in the case of smart grids, security means (among other things) securing the provision of electrical energy. While electrical energy is indispensable for both individual lives and the functioning of governmental structures, it is also clear that quite some translation takes place before clear technological requirements are arrived at. Also, the final technological requirements reflect not only such considerations of security, but also economic and cultural ones.

Even if we were to conclude that all cases show some form of data protection as the primary implementation of security, it must also be mentioned that the implementation as well as the consequences of these implementations vary widely. In biometrics, data protection builds on (mostly irreversible) coding. With body scanners it builds on moulding the data into (arguably) impersonal information and hence the elimination of personal data. With smart grids it builds on aggregation and segmentation. With ANPR it builds on ‘forgetfulness’ which is a sort of elimination, but a rather different translation of it than is seen with body scanners. And with DPI it builds on taking very small snippets of data as the object of reference, such that the data themselves become meaningless.

[10] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.
[11] Finn et al. 2013. Friedewald, Michael, David Wright, Kush Wadhwa et al., "Central Concepts and Implementation Plan", PRISMS Deliverable 1.1, 2012.

The case of body scanners shows that considerations of security are very particularly translated. While it seems obvious that we do not want bombs, guns and drugs to be taken on board planes, it is much less obvious how these unwanted items are translated into what triggers an alarm in the body scanner. At closer look, these translations are also contingent on which electromagnetic waves it is possible to work with and with which it is not, considerations of what is deemed to be detrimental to health, and indeed, what is deemed to pose a threat to privacy. The contrast is even sharper if we realize that the preceding practice of walk-through metal detectors responded only to metals of quantities above a certain threshold: apparently, the new configuration entails an expansion of the range of items labelled 'suspect'.

Also, security in the form of access control plays out differently between the cases. In the case of smart grids, in particular the nodal devices in the network, security is often a matter of strictly regulating physical access by 'classical' door locks: measures are taken to prevent one from entering premises on which devices are located that is critical to the operation of the power infrastructure. Additionally, the critical nature of such devices demands instant action rather than a strict identification and certification of the person who does the operation. Therefore, no user accounts and passwords are used. In contrast, received security paradigms in ICT with their focus on data and network security typically do demand such use of accounts and passwords. Now that the increasing use of information technology within the energy infrastructure seems to enforce a further entanglement of these two cultures, the difficulty of their reconciliation becomes apparent. In contrast, in the Rotterdam harbour area, which served as one of the examples of biometric access control, physical access control is made strictly dependent on the safety training certificates a person holds, which are connected to their identity through the use of biometrics. Thus, in this case, physical access is much more of a rigid classification of safety skills.

5.4 LEGITIMATIONS

Each sociotechnical construction needs justification of some sort for its existence. That is to say, for a situation to emerge or persist, there must be *some* account of why the benefits outweigh the costs. While it might be expected that security itself is often a trump in justification, it remarkably often takes company with other justifications, such as efficiency, convenience, etc. Even arguments of environmental pollution serve as justification of security systems, as is the case in for example ANPR. In the case of body scanners, it continues to be an important argument that the radiation deployed by the scanner is completely harmless. However, this harmlessness plays out differently in the US than in the EU. In the US, backscatter X-ray scanners are used that offer a very low dose of radiation, far below the dose of natural radiation that a passenger is exposed to on the actual flight. In the EU, these scanners are not allowed, based on the argument that X-rays are principally ionizing, and even though they cannot be harmful at this dose, it is still undesirable to expose people to such ionizing radiation. Instead, the millimetre-wave spectrum is chosen. Whether X-rays in the US or millimetre waves in the EU, in both cases it turns out that the fact that the device is not detrimental to health serves as an important discursive element to legitimizing the arrangement.

The case study on body scanners yields a picture as if the legitimacy of body scanners in support of airport security is generally endorsed. One significant episode in their development was when the Association of Stoma Patients sought contact with security operations at

Schiphol in order to seek a solution for the fact that stoma patients typically cause an alarm in body scanners. Importantly, they sought solution in a procedural way, but did not argue for an exemption from the security process as such, nor from the scanner as such. This suggests that the AMS as a means to attain security is largely accepted and unchallenged, at least by this subset of stakeholders.

A different example is provided by smart meters. These are presented as obligatory passage points towards the use of sustainable energy sources. However, as some interviewees argue, this is a bit of a fiction, as the power network at the macro level is not dependent on smart meters for its stability. Also, it is argued by vendors[12] that smart meters contribute to efficiency, the benefits of which would then accrue to the general public. However, this accrues also to all members of society, not only holders of a smart meter. Also, the fact that the network does not depend on the smart meter for its stability sheds different light on the political legitimation of smart meters.

[12] European Smart Metering Industry Group, "Position Paper on Smart Metering in the energy efficiency directive (COM 2011/370)", 2012. http://www.esmig.eu/press/filestor/eed_pp. (Accessed: 12 March 2013)

6 CONCLUSIONS

6.1 CONSEQUENCES FOR SOCIOTECHNICAL RESEARCH

As was explained at the beginning, one assumption underlying this research project was that privacy and security are not necessarily placed in a mutually exclusive relation. More privacy does not always mean less security and the other way round.[13] This idea has been confirmed by the discussion of various emergences of privacy and security. Both privacy and security are multiple, and there is no obvious way in which they are detrimental to one another – though obviously, it is possible that they are in some cases. This multiplicity of privacy and security finds a correlate in the fact that no general or universal way exists in which instances of privacy or security emerge. There is no single conclusion on what 'goes into' the construction of privacy or security, or what determines how a security technology will eventually be shaped. Instead, each construction of privacy, security, and privacy and security technologies is unique.

This entails that moral and other evaluative judgments remain bounded to the situation to which they pertain. Even though PRISMS is not primarily aimed at offering moral judgment or ethical reflection, it must be borne in mind that whenever something apparently laudable or despicable is observed, its assessment must take place against the background in which it emerged and the norms and values that are embedded in that background. Evaluation is not to be done by pre-defined criteria of what a good privacy or security practice should be, but by the frames and definitions that emerge in the practice itself. A similar contextualization for moral judgment is also needed for other evaluations. Importantly, classifications such as 'the social' and 'the technological' must be understood as emergent in practice. It follows from the above that such distinctions cannot be made a priori, even though in common parlance 'the social' and 'the technological' are clearly distinguished. Therefore, categorizations like this one cannot be used as analytical or explanatory tools, but at best as heuristic ones.

Ultimately, these contextualisations entail that the objects of inquiry are themselves first revealed after the networks in which they are embedded have been articulated. This means that the 'direct observables', i.e. things that can be investigated directly, such as opinions, courses of action, formal and informal relations between people, etc., require some further analysis of the context before they start to make sense. Of course, this does not take away that we may start our inquiry at people's interpretations of values, the technologies they work with, the roles they have and the way they justify things, etc. Yet, once more, such observations and understandings must be appreciated critically, as they will in general be highly contextual.

6.2 CONSEQUENCES FOR FURTHER PRIVACY AND SECURITY RESEARCH

Despite the impossibility of separating the technical from the social, modern everyday life is full of situations in which the only possibility is acting as if there were a clear separation between the two. Nonetheless, the tight connections between the technical and the social, or rather the absence of a clear boundary between them, entail that technical interventions often

[13] van Lieshout, Marc, Michael Friedewald, David Wright and Serge Gutwirth, "Reconciling privacy and security", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1-2, 2013.

have significant social consequences. In particular, problems that are argued to be solved along technical lines, often are only partly so, leaving the unresolved parts of the problem for social accommodation. This could be called an *overflow*: issues imperfectly or not completely contained in the technical sphere, flow over into the social sphere.[14] Such overflows necessitate a critical view on technologies in their social context.

Because of, amongst other things, these overflows, it is often preferable to speak of displacements rather than improvements. While it may appear at face value as if a new body scanner or a new generation of licence plate recognition technologies offers an improvement of the way things were previously arranged, a closer look often reveals that burdens, tasks and responsibilities are just rearranged and start appearing elsewhere. For example, in the case of body scanners, the technical impossibility of distinguishing a bomb belt from a stoma leads to particular social arrangements that are (apparently) acceptable to the Association of Stoma Patients, but not necessarily pleasant. However, it is far from obvious that stoma patients should carry this burden, and even if it were somehow possible to quantify 'burden' and 'effort' and to conclude that they are reduced, then still 'shifting' burden is a better description than 'eliminating' it.

The entanglement of social and technical entities entails that examples used in survey research must shed sufficient light on social as well as technical contextual elements, rather than only investigating social realities and moral positions. Such vignettes must be thoroughly contextualized, rather than abstracting from context in an unfortunate pursuit of generalizability. In fact, generalizations inherently risk misrepresenting the meaning of concepts, as those meanings are bound to context. If validity over a range of different situations is desired, this can only be achieved by using a range of diverse, yet contextualized examples.

[14] Callon, Michel, Pierre Lascoumes and Yannick Barthe, *Acting in an uncertain world: an essay on technical democracy*, The MIT Press, Cambridge MA, 2009.

Part II: Case Studies

7 BODY SCANNERS FOR AIRPORT SECURITY

Govert Valkenburg

7.1 INTRODUCTION

This case study concerns the *active millimetre-wave scanner* (AMS), one particular type of security body scanner currently being introduced at airports. They locate objects on the human body, and then indicate the location of these objects on a screen, by highlighting parts of a generic body shape. Vendors and security managers argue that the absence of a photograph or similarly realist picture provides a customer-friendly security procedure, with less manual body searches, and without a security officer inspecting photos of the passenger's body. Also, it is explained that the waves are completely harmless, and do not pass through the body.[15]

Security scanners at airports are supposed to help making airports and the flights departing from them safer places. Yet, when looking at them more closely, we see that they do a lot more. Security scanners influence how security officers do their work. They make distinctions between people who are normal – against a very specific idea of what counts as normal – and people who are not – which in many cases will have nothing to do with them being potential terrorists. Scanners tell security officers whom to search. And they represent bodies, even if it is only as an abstract, mannequin-like shape that is claimed to be impersonal and respectful to privacy. In addition, the way security scanners are presented stretches beyond mere considerations of security: they are acclaimed as conducive to comfort and efficiency[16] and as medically safe.[17] Interviewees position them as privacy-preserving.

Security scanners, much like security technologies in a broader sense, are often assessed in a discourse that understands privacy and security as mutually exclusive assets: a practice of high security would need to compromise privacy, whereas a practice in which privacy is well cared for, would be likely to show considerable weaknesses on security. Yet, this trade-off between security and privacy is at best a superficial representation of all that goes into the complex reality of security scanners at airports. This case study aims to show that the opposition is indeed a false one, and that by abandoning it, a more nuanced view of how privacy and security operate in practice can be obtained.

Drawing on empirical work, this case study will describe body scanners and the practice in which they function. By looking at the details of the practice, it will be articulated how specific, contingent forms of privacy and security emerge. Choices to be made in practice seldom take the shape of 'do we want privacy, or do we want security?' Rather, they are about which specific forms of privacy we want, which forms of security we want, and which specific forms of security and privacy are possible under particular technological and social circumstances and under the everlasting pursuit of increasing efficiency, turnover and service quality.

[15] Schiphol, "Airport secuity: Security scan", 2013. http://www.schiphol.nl/web/file?uuid=2a47b6ff-3a71-4054-a603-6e68aae51cfa&owner=fc5889a9-e049-442a-b208-b416f05e180d. (Accessed: 13 March 2013)
[16] Ibid.
[17] Ibid.

7.2 METHODOLOGY

Part of the empirical base of this case study is provided by five interviews. Three technological experts were consulted, one policy maker at the national level, and one security manager at the airport level. A brief telephone interview was held with a representative of the Association of Stoma Patients. The interviews are complemented by a review of academic literature, press coverage, corporate communication and websites, material from watchdog and other societal organisations, and so on. From this base, a 'snapshot' is composed of the practice of security scanners at airports, that should make clear how privacy and security are 'done' or enacted in practice.

7.3 THE ACTIVE MILLIMETRE-WAVE SCANNER

The active millimetre-wave scanner (AMS) produces a very small amount of electromagnetic radiation in the millimetre spectrum to illuminate the body of the scanned person. Upon illumination, the millimetre waves are reflected by the body as well as by anything worn on the body. Some 1000 sensors receive the reflected waves and record their amplitude and phase. By means of complex signal processing techniques, the system calculates which kinds of materials are worn on the body and where. If any kind of material is present on the body that should not be there according to the specific rules of security, its location is communicated to the security officer as a mannequin-like shape on a screen, of which one particular part is highlighted. [18] This part of the body is then to be searched manually.

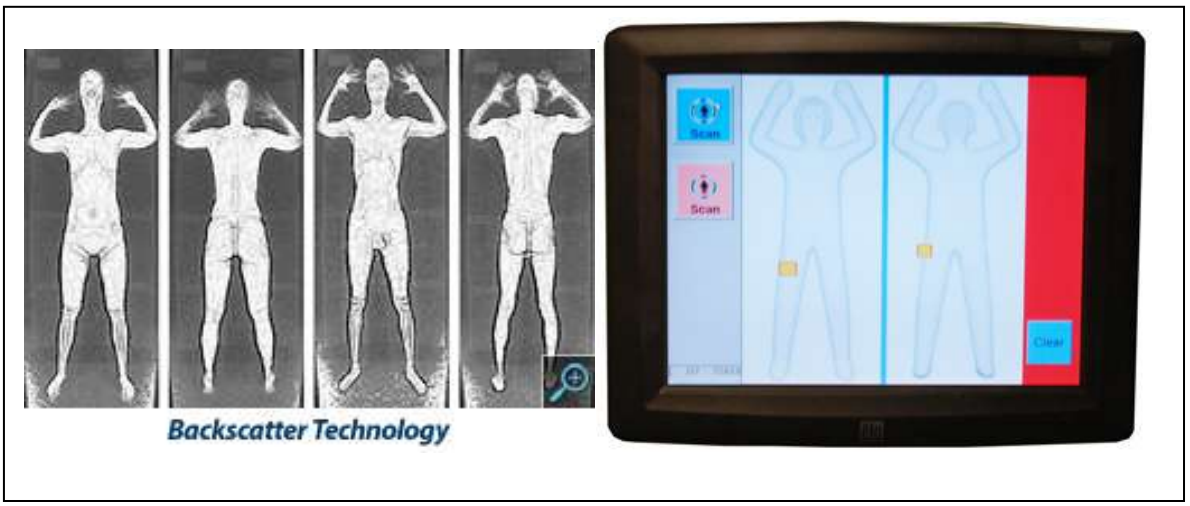

Figure 1: X-Ray backscatter picture that reveals anatomical details (left), and AMS-generated mannequin representation without anatomical details (right) (Source: TSA (USA Transportation Security Administration) 2013)

The frequency spectrum in which these AMS devices work, typically ranges from 70 to 80 GHz. It is argued by vendors, operators, and security policy parties, that millimetre-wave radiation is completely harmless.[19] It is used in very low doses, but even if it were used in

[18] Source: interview with technological expert.

[19] NCTb, "NCTb Q&A Security Scan", 2010. http://english.nctb.nl/Images/Factsheet%20security%20scan%20UK_tcm92-246192.pdf. (Accessed: 14 March

much higher doses, it would still be unable to have any effect on the human body, whether in the form of harm or any other effect. In this respect, the millimetre-wave spectrum differs significantly from e.g., X-rays. Moreover, we are continually exposed to millimetre-wave radiation from car radars and mobile telephones, and even in much higher intensities than the scanner produces. Also, developers indicate that radiation in this particular spectrum does not pass through the body nor even penetrate the skin. [20] At the same time, its use is not limited to specific classes materials (e.g., metals), but active millimetre-wave scanners are able to detect a broad range of materials.[21]

Different types of active millimetre-wave scanners exist. They differ in how the reflected waves are sensed, how data are processed, and how processed data are transformed into an image that is presented to the security officer. For example, the scanner that is currently developed by Rohde and Schwarz,[22] calculates items directly from the reflected waves. The waves are not transformed into a photographic picture which could reveal anatomical details, nor do the waves contain sufficient information to do so. In contrast, the L3 Provision ATD,[23] does create a photographic image with anatomical details, upon which object recognition is applied such that the original image needs not to be shown to the security officer.

7.4 BACKGROUND

Security scanners are not just currently emerging out of the blue, but must be seen against the backdrop of decades of developments in aviation security. For instance, metal detection was introduced after the first hi-jacks in the early 1970s. Another key event has been the Lockerbie assault in 1988, which led to more stringent checks of baggage. Late 2001, the so-called 'shoe bomber' urged several airports to pay closer attention to people's shoes,[24] and in 2006 the attempt to blow up aircraft by with liquid explosives lead to more stringent rules on what could be taken on board. These events provided call for the introduction of more sophisticated inspection than walk-through metal detectors could offer. While pilot cases of security scanners had been operated from 2006 onwards, it was the attempted attack by 'underwear bomber' Abdulmutallab in 2009 that gave their further development a considerable impetus.[25]

To the problem of checking what people might hide under their clothes, millimetre-wave scanners are not the only possible solution from a technical perspective. The most important alternative is provided by the so-called backscatter x-ray scanners. These scanners illuminate the body with a small amount of x-ray radiation, which is reflected by the body and made into a two-dimensional visual picture in much the same way a camera works. However, x-rays are ionizing, which means that the radiation potentially damages human tissue. The European

2013). Schiphol, "Airport secuity: Security scan", 2013. http://www.schiphol.nl/web/file?uuid=2a47b6ff-3a71-4054-a603-6e68aae51cfa&owner=fc5889a9-e049-442a-b208-b416f05e180d. (Accessed: 13 March 2013)

[20] Source: multiple interviews with technological experts.

[21] L3 Communications, "Security and Detection Systems", 2013. http://www.sds.l-3com.com/advancedimaging/provision-at.htm. (Accessed: 13 March 2013)

[22] http://www.rohde-schwarz.de/

[23] Gonzalez Fuster, Gloria, and Rocco Bellanova, "Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices", *International Political Sociology*, Vol. 7, 2013, p. Forthcoming.

[24] WikiPedia, "Richard Reid", 2013. http://en.wikipedia.org/wiki/Richard_Reid. (Accessed: 20 March 2013)

[25] European Commission, "On the use of security scanners at EU airports", European Commission, Brussels, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0311:FIN:EN:PDF.

Commission issued guidelines that security scanners deploying such ionizing radiation shall not be used.[26] Nonetheless, the United Kingdom declined the part on ionizing radiation and continues to use the x-ray backscatter scanners they had already installed, by appeal to security concerns that are not further specified.[27] In fact, this latter type of scanners is currently being installed on a wide scale in the US. These different implementations draw attention once more to the fact that universality or general representativeness are not among the aims of this case study, and instead we focus on accounts of particular arrangements different contexts.

7.5 ACTIVE MILLIMETRE-WAVE SCANNERS IN PRACTICE

To understand how specific versions of privacy and security emerge around a technology, it is not enough to explain just the technical details. Rather, we need to attend to the technology in operation, how the technologies behave in unexpected ways, the kinds of behaviour they make possible and impossible, etc. Also, the social arrangements around them, the laws and regulations under the rule of which they reside, economic circumstances and any other reason why things are one way and not another need to be taken into account. The following analysis will assume a number of foci through which the emergence of particular versions of security and privacy become clear.

7.5.1 Anomalous anomalies

At face value, all the scanner does is identify anomalies and represent them as highlighted zones on the rather impersonal shape of a mannequin. Yet, precisely the issue of what counts as an anomaly merits further attention, as the exact specification of the boundary has far-reaching consequences. The anomalies that developers and security policy workers have in mind obviously include bombs, guns and drugs. However, as one interviewed policy maker indicates, a business card stored in a chest pocket also causes an alert to be triggered. This raises an important question: if a business card triggers an alarm, then what to think of items that are considerably more delicate to many. The fact that a business card *de facto* counts as an anomaly epitomizes the difficulties that this technology faces when applied in the real world

Indeed, it is reported by interviewees from both operations and patient associations that stomas represent a challenge in the practice of security scanning using millimetre-wave scanners. Technically, scanners are unable to differentiate between stomas and bomb belts. Two things help explaining this conflation of bomb belts and stomas into the same collection of items that cause alerts. First, thinking things through, it seems that the identification of a stoma as being something suspicious is the consequence of the very specific idea of anomalies that has informed the design of the scanner. The design idea has been to discern between, on the one hand, human skin and garments, and on the other hand anything that is neither human

[26] European Commission, "Commission Implementing Regulation (EU) No 1147/2011 of 11 November 2011, amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports", *Official Journal of the European Union*, L294, 12 November 2011, pp. 7-11.

[27] Greening, Justine, "Airport security scanners. Written statement of the Secretary of State for Transport.", Department for Transport, London, 2011. https://www.gov.uk/government/speeches/airport-security-scanners.

skin nor garments. Then, indeed, stomas and guns land beyond the pale of flesh and fabric in the same suspicious category.

Second, it appears that making a different design choice, and setting the normal-abnormal boundary somewhere between guns and stomas, would have been impossible with this kind of scanner. For this, we have to look at experience with the earlier ATD version of millimetre-wave scanners, the one that creates a visual image upon which object detection is applied. One interviewee explains that on the underlying pictures, a stoma just looks like a bomb belt. In other words: if the picture is too unclear for the human eye to see the difference, it is not straightforward that a technology based on visual recognition will be able to do better. Thus, the fact that stomas and bomb belts land in the same anomalous area is not only owing to anomalies being defined as 'not flesh nor garment', but also to the choice for a particular wavelength spectrum in which belt bombs appear identically to stomas – much like a dolphin and a shark are indistinguishable if all we can see is size and colour.

In response to this *de facto* criminalization of people with a stoma, some learning has taken place. As interviewees report, airport managers and the association of stoma patients have agreed a solution that is acceptable to both. They together arrived at the agreement that people carrying a stoma may identify themselves to security officers, upon which they are treated in what is argued to be a less criminalizing way. While stoma patients are not exempted from airport security and while their stoma still works as an anomaly in the sense just described, they have been promised that the consequent examination will take place in a secluded examination room, and not simply in front of the waiting line as had been the case before. Importantly, the Association of Stoma Patients has not argued for an exemption from safety measures; they are not contesting the need for security.[28]

While this solution is endorsed by both airport management and the stoma patients' association, this is not to say that it is neutral. It is still a very specific implementation of the privacy of stoma patients. True enough, they are no longer required to explain or even show what is under their shirt in public. But still they have to reveal themselves as stoma patients, an issue for which they may have good reasons to keep it private. Also, they have to come to the examination room, which still renders them suspicious in front of others in the waiting line. Even though the patients' association endorsed the solution, it may also have been the best they could get when confronted with the *fait accompli* that these particular scanners were installed. It does not take away that it is still, at least potentially, highly uncomfortable for individual stoma patients.

7.5.2 The body eliminated

A second thing that the security scanner does when taken at face value, is representing the body in an abstract way on a screen. Leaving out anatomical and other details, it seems that the scanner pays a great respect to privacy. However, again, a second glance reveals that things are in fact a bit more complicated, and that the abstract representation of the scanned body does not unequivocally correspond with a respect for privacy – leaving unanswered the question of which idea of privacy exactly is respected, in the first place.

[28] Source: Interview.

First, it differs between exact types of scanners how this abstract picture is created. The AMS currently under development at Rohde and Schwartz detects anomalies – with all the difficulties spelled out above – directly from the reflected waves. The reflected waves and the way they are detected do not contain information that is sufficiently detailed to create a visual picture that contains anatomical details of the scanned body. However, even though no photo is created in this straightforward sense, the system still creates a representation in a more generic sense (indeed referred to, by system developers, as an 'image', as opposed to the term 'photo' they use when they refer to a representation that does visually convey details, including anatomical ones). It is not quite the case that no private data at all are contained in the representation, if only through the very ability to transform a stoma into a suspect anomaly as described above.

Second, one difference between the Rohde and Schwarz and the L3 scanner becomes relevant here. The latter first creates a photo-like image, upon which object recognition is applied. To begin with, one interviewee explains that on pictures produced by this system, it is almost impossible to tell a bomb belt from a stoma. A hard lower boundary is set to the minimal sizes of details that can be made visible by waves in the millimetre spectrum (see below), which in turn sets limits to the accuracy of visual object detection. Thus, the body is still present in all the ambiguous anomalousness that the scanner imposes on it.

However, perhaps more important, even if the human operator is not shown the photo-like image by the L3 system, such an image is still there, latent in the device. To prevent leakage, such devices are provided with different modes: operation modes in which data cannot be stored, and development modes in which data can be stored and used for debugging purposes. As interviewees from Rohde and Schwarz claim, not only is such a photographic image absent in their system, it is also impossible to store any of the information without additional hardware. Only the vendor has access to such diagnostic hardware. The certification process for these scanners includes assessment of these modes and technical possibilities.

However, certification agencies are not the ones operating the device in practice. In the end, operating parties, no matter how well-organized and democratically governed they are, are susceptible to failure. It has indeed been reported that scanners in operation at airports were actually set (and apparently able to be set) to the 'development mode', thus allowing for the retention of data.[29] While the possibility of storage has always been denied in official communications by the US Transportation Security Administration,[30] it has also been confirmed by other official bodies.[31] Ultimately, whether the images are really safe depends on the reliability of the party operating the device.

All in all, the various types of AMS scanners do not just 'eliminate' the representation of the human body while maintaining or even increasing the level of security. Rather, they displace particular operations on the human body – photo-like representations from earlier x-ray

[29] Bosker, Bianca, "Body Scan Images From Security Checkpoints Were Saved By Feds", 2010. http://www.huffingtonpost.com/2010/08/04/body-scan-images-from-sec_n_670170.html. (Accessed: 2012.11.02)

[30] Rossides, Gale D., "Letter to Bennie J. Thompson, chairman of the Committee on Homeland Security, U.S. House of Representatives", U.S. Department of Homeland Security, Transportation Security Administration, Arlington, VA, 2010. http://epic.org/privacy/airtravel/backscatter/TSA_Reply_House.pdf.

[31] Bordley, William E., "Letter to John Verdi, EPIC concerning Freedom of Information / Privacy Act Request no. 2009USMS13697, subject: Images", U.S. Department of Justice, United States Marshals Service, Alexandria, VA, 2010. http://epic.org/privacy/body_scanners/Disclosure_letter_Aug_2_2010.pdf.

backscatter scanners, inspection by walk-through metal detectors, and randomly selected full body searches – by other operations – classifying anomalies and positioning them on a mannequin, thus pre-structuring targeted searches.

One important effect of such displacements is that they engender a vocabulary of respect for privacy. Strictly speaking, no nude picture is created. Indeed the privacy issue of nude pictures has been resolved by eliminating the nude picture. Yet, this does not take away the fact that these new representations have consequences for the persons involved, and that these persons may take issue with some of these consequences. Against the backdrop of a vocabulary that emphasizes the elimination of pictures, such issues are harder to voice. Thus, de facto, this configuration contributes to its own justification.

7.5.3 Harnessing radiation

The wavelength has been chosen in the millimetre spectrum for various reasons. Many properties of electromagnetic waves vary with the wavelength. For one thing, the scanner's resolution varies directly with the chosen wavelength. That is to say that shorter waves (which equals a higher frequency) are able to detect smaller objects and/or produce pictures at a higher resolution. However, with shorter wavelengths also the relative energy of waves increases, up to a point where they become harmful for the human body. From a perspective of resolution, the very short waves of X-rays would be preferable, as they could detect or image even the smallest detail. However, because of their high energy, these waves are ionizing, which is associated with harmful effects. Peculiarly, the low dose at which X-rays are typically used prevents them from doing any measurable harm. The millimetre-wave spectrum strikes a particular balance between short and long waves: the waves are short enough to scan the human body at sufficient detail, and long enough to stay clear of inducing potentially harmful effects in the scanned body, or so it is argued by producers of this technology. Also, if the waves were slightly shorter, they would have increasing difficulty penetrating garments, making them unusable for body scanning.[32] Another consequence of the plain fact that millimetre waves do not penetrate the skin is the fact that objects hidden under the skin remain undetected.

Yet, some remarks are to be made at this point. First, in the earlier backscatter scanners, indeed ionizing X-ray radiation was used. However, this radiation was used at a very low intensity, at which it was still considered harmless. In fact, when an airplane flies high in the atmosphere, it is less protected against cosmic radiation by that same atmosphere, which entails that passengers are exposed to an amount of radiation, including X rays, at an intensity that is much greater than the intensity used in the backscatter scanners. The cosmic radiation during a flight is argued to cause 150 times more carcinogenic damage than the scanner does.[33] In fact, an advice solicited by the European Commission itself assesses the risks of

[32] May, Torsten, "Body Scanner Technologies: a review", Paper presented at: International Conference "Security, Ethics, and Justice: Towards a More Inclusive Security Design", 21-23 June 2012, Tübingen, Germany, 2012. http://www.uni-tuebingen.de/en/facilities/international-centre-for-ethics-in-the-sciences-and-humanities/research/ethics-and-culture-security-ethics/focus-of-research-security-ethics/kreta/internationale-tagung.html

[33] Mehta, Praktik, and Rebecca Smith-Bindman, "Airport full-body screening: What is the risk?", *Archives of Internal Medicine*, Vol. 171, No. 12, 2011, pp. 1112-1115. http://dx.doi.org/10.1001/archinternmed.2011.105.

this particular application of X-rays in much the same way.[34] Nonetheless, the latter advice stresses that even if no effect is present, justification is still needed as to why particular individuals are to undergo the (even if negligible) burden of X-rays, while the perceived benefits accrue to society at large.

Thus, there is something peculiar about the millimetre-wave radiation being proposed as harmless *in contrast to* x-ray radiation. Apparently, policy makers adopt what could be called a popular frame of X rays, that does not entirely coincide with the frame of radiology scientists such as Mehta and Smith-Bindman.[35] This popular frame has been used strategically (perhaps even unknowingly so) in staging the active millimetre-wave scanner as a device without any health risks.

A second point regarding the choice of wavelength concerns a more natural-scientific and technological source of contingency. Selecting a wavelength is not simply a matter of picking an arbitrary working range that suits best. It hinges on a lot of technological contingencies whether a particular wavelength can be handled in the first place. As developers from Rohde and Schwarz explain, working with this frequency range was only possible because appropriate analogue-to-digital converters were available. Also the amount of computing power needed has not always simply been there, but it could be made available at the right moment. This adds to the desirability of millimetre waves, relative to other wavelength bands.

7.5.4 Displacement of labour

Security scanners, both in general and the AMS in particular, are often legitimized by their contribution to efficiency: less time per passenger would be needed and the number of manual body examinations would be reduced.[36] Also, scanners such as the AMS, that automatically detect anomalies, are argued in interviews by both vendors and security managers to reduce the human effort needed to judge the representations, as they are less susceptible to the fluctuations that are natural to human performance.[37] Both the reduction of body searches and the fact that security officers no longer need to spend time on judging the suspiciousness of pictures would free them for other tasks: offering service to passengers, dealing with exceptional situations, etc.[38]

However, some objections arise here. First, the inference so far seems to neglect the fact that conventionally, full body searches were mostly performed on a random basis. In the new situation, everybody is screened by the scanner, and potentially subject to a body search. Other than the full body examination, this search is pre-structured and only requires inspection of part of the body. While the search itself thereby becomes less time-consuming, the probability of being subject to a search increases – mind again the business card that potentially causes a 'false positive' alert.

[34] Scientific Committee on Emerging and Newly Identified Health Risks, Anssi Auvinen, Thomas Jung et al., "Health effects of security scanners for passenger screening (based on X-ray technology)", European Commission, Brussels, 2012. http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_036.pdf.
[35] Mehta, Praktik, and Rebecca Smith-Bindman, "Airport full-body screening: What is the risk?", *Archives of Internal Medicine*, Vol. 171, No. 12, 2011, pp. 1112-1115. http://dx.doi.org/10.1001/archinternmed.2011.105.
[36] Source: Interview.
[37] Source: Interview.
[38] Source: Interview.

One interviewee argues that this new configuration indeed requires learning among the general public. Thus, travellers are disciplined and forced into learning to store everything in their bags and jacket and then take off the jacket. These are then to be scanned by the hand-luggage scanner. Yet, the same interviewee explains that current hand-luggage scanners, which work with X rays much the same way as the x-ray photographs made in the hospital, are unable to look through the batteries of laptops. This is problematic, as, apparently, security seems to demand a kind of material transparency, which laptop batteries do not comply with. Therefore, laptops are always to be taken out of the passenger's bag or briefcase, for otherwise the inspecting security officer cannot see whether something is hidden under the laptop battery. Thus, the learning goal that passengers are confronted with is actually ambiguous: put everything in the bag to ensure your own privacy, but take some things out of the bag, because otherwise the system that serves your privacy, will fail.

The claimed increase in efficiency thus at least depends on what is taken into account. The burden of this process of complex learning is placed to considerable extent at the passenger. Also, even though interviewees generally claim that the AMSs and similar scanners contribute to efficiency, one interviewee also argues that currently, the number of (partial) body searches is still too high. However, this is ascribed to the learning process accompanying the introduction of any new technology, rather than seeing it as a necessary consequence of the whole configuration.

Additionally, research has shown that it is an immensely complex task to assess whether security scanners pay for themselves. For the US situation, which cannot be translated straightforwardly to the European situation but which might still serve as an indication, it has been calculated that a terrorist attack must be intercepted every two years by the security scanners for them to pay back in mere financial terms. The broader social costs have however remained under-researched, and in the European situation, research has even been narrower and focused on the local costs and benefits at the airport level only.[39]

7.6 CONCLUSION

At face value, active millimetre-wave scanners just seem to offer a helping hand to security officers, when it comes to selecting people for a more extensive security check. This is indeed the typical perspective that is invoked in defence of the idea that security scanners are indispensable in the practice of airport security, and a necessary development if we want to keep airport security manageable.

However, this case study has revealed that below this simple picture, a wealth of ambiguities, contingencies and negotiations are present. We have seen that identifying anomalies is not as straightforward as it sounds, and its consequences are moreover far from neutral. Also, even though rendering the body as an abstract mannequin takes away some privacy concerns, it immediately raises others, and thus amounts more to a *displacement* of privacy issues than to their *elimination*. Additionally, the kind of waves being used is not just a matter of selecting the best wave spectrum from a safety perspective, but rather a complex discursive game that trades one kind of radiation for another. Finally, while it is widely argued that security

[39] Hallinan, Dara, and Michael Friedewald, "Economic costs of surveillance technologies", in David Wright (ed.), *IRISS Deliverable D1.1: Surveillance, fighting crime and violence*, 2012, pp. 233-246. http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf.

scanners contribute to a reduction of effort to be made in the security process, it strongly depends on what one looks at and what is taken into account, and also in this case it is more appropriate to speak of displacement of work rather than the elimination of work.

To this light, it can be confirmed once more that privacy and security are not mutually exclusive. Rather, changes in security arrangements lead to changes in privacy and its issues, but this rather takes the form of displacement and alteration, than of elimination or deterioration in a 'more versus less' interdependency. It is not that security is incompatible with privacy, but rather that particular arrangements of security correlate to particular forms of privacy. This depends on the ideas underlying specific designs, the natural, social and technical contingencies that feed into the design process, and on further transformations that are made on technical and operational arrangements once the technology is put in place.

8 AUTOMATIC NUMBER PLATE RECOGNITION

Noor Huijboom

This case study examines two specific ANPR (automatic number plate recognition) configurations; the application of ANPR for average speed control and ANPR application for interception and investigation of offences. In both configurations, cameras take photos of vehicles and software extracts the licence plate numbers from the photos. However, the subsequent processing and usage of ANPR data differs between the two configurations. In case of average speed control, the number plate data is used to calculate average speed and fine owners of vehicles that exceeded the speed limit. In case of ANPR for interception and investigation, the number plates and in some cases photos (referred to as raw data) are used to intercept offenders or to solve a crime case.

At face value, these ANPR systems seem to simply support law enforcement agencies in carrying out their tasks. However, when comparing the characteristics and the use of these systems with their predecessors (e.g., the spot speed camera for speed enforcement) it seems that ANPR systems make law enforcement agencies extremely powerful in the detection and interception of offenders. As regards speed enforcement, the behaviour of drivers is continuously monitored over a greater distance, which enables police forces to more structurally and generally observe behaviour. And, as regards interception and criminal investigation, police forces can intercept and track considerably more offenders than they could with conventional means.

This case study shows that ANPR systems enact specific ideas of security and privacy. Police forces perceive ANPR to be a crucial tool in support of various security tasks, ranging from fining of speed offenders to the detection of human trafficking. In addition, ANPR is understood to support various phases of the law enforcement process, from prevention (e.g., deterrence of offences) to investigation (e.g., tracking of offenders) and arrest. Privacy seems to be chiefly a data protection issue for law enforcement authorities. Questions which are frequently posed concern the lawfulness of data gathering, storage and/or usage. Issues which police forces recurrently relate to privacy are retention dates, access control and accuracy of data. Privacy experts raise more fundamental questions to ANPR deployment, such as: is ANPR a proportionate means to its goals? And: could other – less intrusive means – be applied to achieve a similar degree of security? For developers, ANPR systems seem to be an important business case. However, several of them also pose fundamental privacy questions to the current and future use of ANPR technologies.

Questions remain about how citizens perceive ANPR systems, their relation to specific goals (e.g., road safety, investigation in crime cases), the characteristics of the systems and privacy implications. Moreover, some studies indicate that citizens are not always aware or knowledgeable on how ANPR works. In particular, in cases of covert ANPR application, it might be unclear to citizens which institution is watching what. This makes it difficult for them to assess the advantages and disadvantages of the system, to oppose to it if they see any reason to, and to hold the justice system accountable for adhering to rules. In addition, they are not always able to create reasonable expectations as to the future use of ANPR data. It seems that their influence on the development of ANPR systems is limited.

8.1 CURRENT TECHNOLOGY

In most European countries, ANPR systems are used for two key purposes, namely (a) for average speed enforcement and/or (b) for enforcement of other offences and criminal investigation. The design and operation of these ANPR systems differ. ANPR systems for speed enforcement consist of multiple cameras which allow the calculation of the average speed of vehicles as they travel between multiple points. The cameras – mostly fixed above the lanes – record images of all vehicles entering and exiting the speed camera corridor and store them locally for a predetermined period of time. Pattern recognition software identifies the licence plate number and subsequently matches the plates of vehicles which enter and exit the ANPR zones. Based on the identified number plates at the several locations, software calculates the average speed of the vehicles. The average speed is generally determined by dividing the total distance between the camera points by the time taken to travel between the points. In case an identified vehicle exceeds the speed limit, information about the vehicle and the offence is send to the police infringement bureau which issues a fine to the owner of the vehicle (the retention dates of the data differ for each country – this will be discussed in sections 1.3 and 1.4 of this chapter).

ANPR technologies used for the enforcement of other offences and criminal investigation consist of camera systems designed to photograph and compare license plate numbers against a database of "known numbers" to allow the police to identify whether there is something untoward about any vehicle coming into the range of the ANPR camera[40]. The lists of "known plates" (often referred to as "hot lists") are updated periodically with information from law enforcement agencies and other government authorities (e.g., Driver and Vehicle Licensing Agency). If a license plate photographed by the camera matches a plate from the database, it is considered a "hit". At this point, the system emits an alarm alerting the police to the hit and providing information about the nature of the hit, such as the hit corresponding to a stolen vehicle or an uninsured vehicle or driver[41].

In addition to this primary use of ANPR technology, the systems may also be used to support more elaborate criminal investigations.[42] In this case, the previously captured numbers or 'non hits' (also called secondary data) are used to collect evidence in a crime case (as stated before, the retention dates of the data differ between countries which will be discussed in sections 1.3 and 1.4). An example of secondary use would be when a witness of a crime has only seen part of a license plate and an officer involved manually enters this information into a database of previously captured license plates in order to see if there is a match. Examples of solutions of crimes in which ANPR based data is being used (in various countries) include burglaries, possession and distribution of narcotics, firearm violations, homicides, kidnapping, sexual-based offences, terrorism related offences, robberies, and child abduction cases.

40 Armstrong, J., J. Czeck, M. Franklin and D. Plecas, "Automated License Plate Recognition (ALPR), How long should the data retention period be?", 2010.
41 Cohen, I. M., D. Plecas and A.V. McCormick, "A report on the utility of the automatied license plate recognition system in British Columbia", School of Criminology and Criminal Justice, Center for Criminal Justice Research, University of the Fraser Valley, Abbotsford, Canada, 2007.
42 Armstrong, J., J. Czeck, M. Franklin and D. Plecas, "Automated License Plate Recognition (ALPR), How long should the data retention period be?", 2010.

8.2 BACKGROUND

Automatic Number Plate Recognition (ANPR) was first developed in the United Kingdom in 1976 at the Police Scientific Development Branch (today known as the Home Office Scientific Development Branch). The ANPR system was initially invented to combat the use of car bombs in mainland Britain by the Irish Republican Army[43]. In 1996, provisional IRA bombings in the City of London resulted in a major application of ANPR: the establishment of the 'ring of steel' – a surveillance and security cordon using CCTV cameras. All vehicles entering the City of London were identified by the installed cameras and had their number plates checked against police databases. Any suspected vehicle could be real-time located and apprehended instantaneously.

Following this, several other European countries implemented ANPR technologies for a variety of purposes. Early applications of the technology were for instance in the Netherlands, where the Dutch government introduced an ANPR pilot on highway A13 in 2002. The purpose of this ANPR measure was to improve the air quality in parts of Rotterdam. The Dutch government argued that by limiting the maximum speed to 80km per hour, the pollution caused by the highway would decrease. Also in France, ANPR technologies have been introduced around 2002. Here, the key goal was to increase road safety. In 1999, the French Interdepartmental Road Safety Committee (Commission de la sécurité routière) set out to enhance the effectiveness of speed checks by providing the police with ANPR systems.[44] Tests with ANPR systems began in 2002, with the first devices being officially put into use by the Minister of Transport and the Minister of the Interior in November 2003.

Today, ANPR technology is commonplace in the majority of European countries. In most countries, the development and application of ANPR technologies were given a strong impetus by the events of 9/11 and the London and Madrid attacks. In the wake of these events, there was a general call of politicians throughout Europe for far reaching security measures, including the application of ANPR technologies. In particular in the UK, the application of ANPR technologies is relatively widespread. In 2011 the UK police force had between 6,000 and 10,000 (mobile and fixed) ANPR systems in use by which around 50 million number plates 'reads' per day could be stored.[45] For comparison, in 2009 the Australian government had between 300 and 400 ANPR systems in place and the Dutch government around 210 in 2011.[46]

In the next sections, two specific applications of ANPR systems will be explored from a social-constructivist's viewpoint, namely (a) the application of ANPR for average speed enforcement and (b) the application of ANPR for the interception or detection of other offences and crimes.

8.3 SPEED ENFORCEMENT BY ANPR

43 Ibid.

44 Carnis, Laurent, "A Public Policy in Evolution:Speed Enforcement in France (2000-2010)", Paper presented at: Australasian Road Safety Research, Policing and Education Conference, Perth, Western Australia, 2011. http://arsrpe.acrs.org.au/pdf/A%20Public%20Policy%20in%20EvolutionSpeed%20Enforcement%20in%20France%20%282000-2010%29.pdf

45 Flight, Sander, and Paul van Egmond, "Hits en hints: De mogelijke meerwaarde van ANPR voor de opsporing", DSP Groep, Amsterdam, 2011. http://wodc.nl/images/volledige-tekst_tcm44-418513.pdf.

46 Clarke, Roger, "The Covert Implementation of Mass Vehicle Surveillance in Australia", Paper presented at: Fourth Workshop on the Social Implications of National Security: Covert Policing, 7 April 2009, Canberra, 2009. http://www.rogerclarke.com/DV/ANPR-Surv.html

8.3.1 The sledgehammer and the nut

At first sight, fixed ANPR systems used for average speed enforcement seem to be installed to detect people who exceed speed limits. However, when looking more closely at how the ANPR systems precisely work, it appears that they not only detect road safety offences but that they pro-actively affect the behaviour of drivers. By making an explicit design choice for overt, highly visible systems and announcing average speed enforcement zones through road signals, police forces try to increase law-abiding behaviour among drivers. Our desk research and interviews revealed that police forces use ANPR systems as a 'communication tool'; to convey the presence of law enforcement[47]. The line of reasoning behind this stems from 'deterrence theory' which assumes that law violation decreases when people perceive that there is a strong likelihood of detection, arrest and eventual penalty[48]. ANPR systems for speed control are thus not only intended to trace speed limit offenders, but to deter all drivers in a certain area from speeding. In this sense the police forces which apply these ANPR systems have a broad interpretation of their security task – they not only react upon actual law violations as but also act as a deterrent to the commission of crime.

A closer look into ANPR systems also reveals that whereas other speed control measures (e.g. the traditional spot-speed cameras and police speed guns) only photograph vehicles which exceed the speed limit (a radar is mostly being used here to measure the speed of vehicles), ANPR systems photograph *all* passing vehicles. In other words, while the more traditional traffic enforcement tools are restricted to the assessment of the *speed* of all passing vehicles, ANPR systems take a *picture* of all vehicles containing information about the speed, type, condition, route and (in some cases) the driver of the vehicle. Although the ANPR pictures of vehicles which did not exceed the speed limits are normally removed from the database (after a predetermined period of time), significantly more data is collected by ANPR systems compared to other speed control tools. In most countries this data is only being used in the road safety domain to detect speed offences; yet several police forces have identified other potential road safety offences which could be detected. The pictures (also referred to as 'raw camera data') can reveal far more information than needed for the fining of people who exceed speed limits. The photo can also contain information about the compliance by the driver or passengers to rules concerning for instance using mobile phones in a vehicle, allowed number of passengers, wearing of seat belts, use of child seats, carrying of (unpermitted) large items, severe damage to the vehicle, missing mirrors, functioning of headlamps, unpermitted use of front or rear fog lamps, etc.

Other significant characteristics of ANPR in comparison with conventional speed control systems concern the dimensions of space and time. Whereas traditional speed enforcement measures (e.g., spot-speed cameras) take a picture at one location, ANPR systems take pictures at several locations along a certain route – also called 'average speed zone.' Herewith, police forces are able to structurally and generally (instead of randomly and locally) monitor the behaviour of drivers. In addition, while conventional systems function during a limited period of time (e.g., speed guns, but also spot-speed cameras that often needed to have rolls of camera film replaced), ANPR systems are able to monitor traffic 24/7.

47 Watson, Barry C., and Karen M. Walsh, "The road safety implication of automatic number plate recognition technology (ANPR)", Center for Accident Research & Road Safety Queensland, Brisbane, 2008. http://eprints.qut.edu.au/13222/1/13222.pdf.
48 Ibid.

As regards both the continuous monitoring capacity of ANPR systems and the monitoring over a longer distance, police forces promote ANPR systems as a fairer means than speed guns and spot-speed cameras. Police argue that the ANPR system is designed to penalize those drivers who continue to exceed the speed limit rather than the accidental lapse that can occur at spot-speed camera sites[49]. Moreover, in some countries (e.g. Australia) average speed offences are being considered as more serious than spot speeding due to the presumed deliberate nature of exceeding the speed limit over a prolonged period rather than a single point.

While fairness is put forward as an unproblematic value by defenders of ANPR systems, it is not at all straightforward what it means in this specific context. The first assumption is that the speed-limit infringement by the driver in case of the spot-speed camera can be an accident, while a similar infringement in an ANPR zone would be deliberate. Particularly as regards ANPR systems in complex road networks with varying speed limits, experts state that people can by accident (because of complexity) exceed speed limits. In addition, some road safety experts argue that drivers who more frequently exceed speed limits, also more frequently are flashed by random speed guns or spot-speed cameras (as they more frequently exceed speed limits, the chance that they are detected by a random camera is higher). Thus, the claimed fairness is in fact a very specific idea of fairness, and it can even be questioned whether this particular form of fairness indeed helps justifying the ubiquity of an ANPR system.

8.3.2 Shifting translations

Strategic reports and press releases by police forces indicate that speed enforcement ANPR systems are also legitimized by their contribution to efficiency; as they automate the detection and fining process, less manpower would be needed for traffic enforcement. These documents state that ANPR systems can read far more license plates per time unit (up to 90,000 vehicles per day) than conventional systems, and that consequently, ANPR systems contribute to an increased issuing of fines on a yearly basis. This latter would further stimulate law-abiding behaviour as the chance that one is caught increases. This, in turn, would support the most important reason to apply ANPR technology put forward by policy forces; namely to decrease the number of speed related crashes. In line with this, several suppliers of ANPR systems claim substantial reductions in annual fatal or serious-injury crash rates. For instance, VYSIONICS, supplier of an ANPR system in Nottinghamshire UK, stated the ANPR system to have contributed to a reduction of 65% of serious crashes at the ANPR site. Here, the effects of the ANPR system seem to actually contribute to underlying reason of speed enforcement, namely road safety.

However, research reports on this matter show ambiguous results. Whereas several studies show that the number of accidents decreased after the implementation of an ANPR system, some reports point out that – in particular in case of complex road networks - accidents may increase due to a higher ‘task load’ for the driver. While driving at complex road networks, drivers have to carry out several tasks at the same time, such as watching speed, navigating and anticipating on movements of others, which makes the driving more difficult and may lead to more accidents.

49 Lynch, M., M. White and R. Napier, "Investigation into the use of point-to-point speed cameras", Transport Agency research report no. 465, NZ Transport Agency, Wellington, 2011. http://www.nzta.govt.nz/resources/research/reports/465/docs/465.pdf.

One important question in the design and implementation of ANPR systems is where will the 'monitoring line' be drawn? Several police forces identified other road safety rules which can be enforced by ANPR systems, such as compliance with rules concerning mobile phoning, carrying of passengers and load, safety condition of the car, etc. In addition, several (new versions of) ANPR systems are not only capable of identifying the vehicle by its number plate, but also of identifying the driver by facial characteristics. This provides all kinds of new possibilities for law enforcement agencies to enforce road safety. Potential applications which have been identified by police forces are, for instance, the targeting of unlicensed driving and fatigue offences among heavy vehicle drivers. Importantly, in this latter case it is not the vehicle which is subject of the observation of police forces, but the individual or individuals in the vehicle. This incurs a radical change in how privacy is translated in the ANPR system: from a configuration that stores vehicle data, to a configuration that stores person data. Reports and interviews reveal that some police forces are currently considering a further extension of the ANPR data use for road safety purposes. ANPR seems to be perceived by police forces as a solution to many road safety problems.

In addition, evaluation reports on ANPR average speed enforcement demonstrate that police forces see an important limitation of the ANPR system in the fact that people are still able to exceed speed limits outside the ANPR zone[50]. In several instances this led to the expansion of average speed zones and/or the identification of new ANPR sites. Overall, the length of average speed zones in several European countries seems to have considerably increased over the years. Tutor, the Italian version of average speed enforcement, is for instance currently being used to monitor 2093 kilometres of the *Autostrade per Italia*'s motorway network, including one zone with a length of 243 kilometres.

The extension of ANPR zones also touches upon the more fundamental question about the boundaries of monitoring. Theoretically, ANPR systems could cover the whole road network of a nation, but various actors question the desirability of such a development. Whereas some policemen emphasize the possibilities of ANPR systems to catch criminals ("How could we justify not catching criminals when the technology is there to catch them"), some policy makers seem to point to proportionality. They argue that in every decision to extend the use of ANPR, one should evaluate whether the means (specific use of ANPR) is proportionate to the specific goal one wants to achieve. Some road safety experts, in turn, point to the self-responsibility of drivers and the ability to make one's own estimation of a situation (e.g., what speed limit would match with a certain weather condition). According to privacy experts, ubiquitous application of ANPR systems could have a chilling effect on drivers' behaviour in the sense that drivers would uncritically obey rules for the sake of obeying rules, rather than critically reflecting on how to achieve road safety.

8.3.3 When do privacy and 'subjects' come into play?

When specifically looking at the framing of the notion 'privacy' maintained by police forces in relation to ANPR systems, the concept seems to be predominantly defined as the right of protection and accuracy of personal data. The term privacy is most frequently mentioned in cases of incorrect infringements and unauthorized access to databases by third parties. This specific view of privacy can also be found in design choices which are often focused on

50 See e.g. the 'halo-effect' in Lynch et al. 2011.

ensuring privacy by data security and data quality measures. In line with this, suppliers promote their ANPR systems by emphasizing the accuracy of the technical elements (e.g., camera and software) and the available 'high tech' security software for databases. This specific view of privacy seems to be mainly based on the principle of 'fairness' and less on the principle of 'diminishing intrusion'. Fairness is by police forces taken to mean that people who do not exceed a speed limit should not be fined and that unauthorized entities should not have access. Privacy can however also be approached by focusing on the right of citizens to be 'left alone'; in other words 'not being watched'. This implies a discussion, not about the consequences of mistakes (incorrect fining) but on the extent to which people are being watched. And, not about unauthorized access by third parties but on the question of who has access (who are first parties?).

Another important question concerns the influence of 'subjected users'; to what extent do they influence ANPR constructions? In other words, do they – and if so in what way do they – shape ANPR technology? As for the application of ANPR technology they do not have much say – other than through general and regional elections. As political views of parties on this subject are not always clear and this subject seems not to be crucial for a political choice in elections, influence here is almost negligible. There are some rare cases of referenda on the application of speed cameras (e.g., in Ohio, US, in 2006), but generally speaking the systems are imposed by governments. And also in the design phase, the influence of subjected users is insignificant. The specific characteristics of the systems are highly determined by police forces and suppliers that advise police forces. Citizens, thus, do not have much choice in the presence or the operation of the systems. The only rightful choice they have in relation to ANPR speed enforcement is to take another route.

In several countries, however, a means of avoiding ANPR detection, called license plate cloning, has emerged[51]. License plate cloning is defined as the illegal purchasing or copying of a number plate of a law-abiding person and attaching it to the own vehicle (often similar model and age). For instance, in 2005, 1 in 1,000 vehicles in the UK had a stolen number plate[52]. Yet, this was not correlated to any broader public revolt against ANPR speed enforcement. An analysis in the UrbanEye project (2004) revealed that in Norway the majority of citizens seems to accept ANPR systems at motorway sites (67% of the respondents of the study)[53]. However, the study does not clarify what Norwegian citizens exactly accept and for what reasons and if other countries may show other acceptance levels. Interestingly, in some cases, government communication on ANPR predominantly seems to aim at acquiring public acceptance. In several policy documents, police forces state that ANPR success stories should be communicated to the media in order to stimulate public acceptance.[54]. In media, both critical and positive reports on ANPR can be found. Criticism on ANPR speed enforcement typically concerns increased fining – e.g. ANPR is mentioned as a 'revenue-generating' measure of police forces.

51 Mathieson, S. A., "Worried about being watched? You already are", *The Guardian*, 15 February 2007. http://www.guardian.co.uk/technology/2007/feb/15/epublic.guardianweeklytechnologysection.

52 Webb, Barry, and Bronny Raykos, "Theft of vehicle number plates: a problem analysis", University College London, Jill Dando Institute of Crime Science, London, 2006. http://www.ucl.ac.uk/scs/downloads/research-reports/numberplate-theft-report.

53 Sætnan, Ann Rudinow, Johanne Yttri Dahl and Heidi Mork Lomell, "Views from under surveillance. Public opinion in a closely watched area in Oslo", Urban Eye Working Paper No. 12, Trondheim/Oslo, 2004. http://www.urbaneye.net/results/ue_wp12.pdf.

54 e.g. NPIA, "Practice Advice on the Management and Use of ANPR", National Policing Improvement Agency, London 2009. http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf.

8.4 ANPR TO IDENTIFY AND INTERCEPT OFFENCES

8.4.1 The unverifiable gaze

Contrary to ANPR used for speed control, the design of systems applied to intercept vehicles or persons involved in existing offences and crimes is often camouflaged or covert. Whereas in the case of speed control one of the goals of applying the system is to pro-actively affect drivers behaviour at the ANPR site, the key goal of interception ANPR is to act upon offences and crimes already committed in the past (unpaid taxes, stolen vehicles, etc.). In this latter case, the ANPR system makes use of databases (hot lists) of licence plate numbers which are associated with specific offences and crimes. It is argued by some police forces that covert systems contribute to the 'hit rate' as people who have been involved in an offence or crime are less able to avoid the systems. A design choice made by several police forces to further increase the hit rate is to integrate or mount ANPR cameras onto (unmarked) police cars. During their patrol, policein these ANPR equipped cars not only watch neighbourhoods but can also act upon existing offence or crime cases (e.g., collect fines, arrest suspects). According to some police forces, these mobile, covert applications have another important advantage in comparison to fixed applications: the 'eye' of the police could be anywhere, which would more generally stimulate law-abiding behaviour. Additionally, it would minimize offenders' implementation of countermeasures and reduce intentionally inflicted damage[55].

In some cases, stored ANPR data (mostly from fixed sites, covert as well as overt) are used for criminal investigation purposes. This is not based on a real-time 'hit' of a number plate with a 'hot list'. Instead, 'non-hit' data are used to find certain mobility patterns in vehicles and persons, which can be used in solving a crime case. For instance, there are multiple examples in which police forces matched stored ANPR data from fixed sites with crimes at several locations (e.g., burglary, robbery) in order to assess whether vehicles and/or the occupant(s) appeared at the various crime scenes. In this case, the goal of the data usage is not to intercept vehicles or persons involved in an offence (with a tangible sentence and perpetrator), but to investigate a crime (to find evidence and identify suspects). Here, bulk data (databases of non-hits) are used earlier in the law enforcement process. Moreover, several police forces are considering the use of non-hit data for targeted crime prevention. A police force for instance stated that data mining software has been developed which can identify criminal lifestyle patterns in vast amounts of ANPR data. With this software, police forces aim at pro-actively identifying (groups of) people who have the risk profile to commit a crime. In other words, while at first glance ANPR systems seem to only intercept vehicles to effectuate concrete penalties, a closer look reveals that in practice ANPR data is used far more extensively – of anyone passing the ANPR and for interception, crime investigation and (sometimes) prediction purposes.

55 The police of Wassenaar, the Netherlands in this respect published the following message on their website: "Saturday, the Wassenaar police carried out a patrol with an ANPR equipped vehicle. Due to the ANPR several drivers were intercepted which had unpaid fines. […] Pay in time! The Wassenaar police will increase the number of patrols with an ANPR equipped vehicle. If you have unpaid fines and want to avoid unexpected arrests, then pay your fine at the police station. […]" Dutch Police, "Inzet ANPR in Wassenaar succesvol", 2011. http://www.politie.nl/mobile/nieuws/2012/oktober/28/06-inzet-anp-in-wassenaar-succesvol.html. (Accessed: 25 March 2013)

ANPR systems are used to solve a wide variety of offences and crimes, ranging from collecting unpaid taxes to human trafficking. In interviews and documents, extensive lists of offences and crimes have been put forward, only to mention a few: burglaries, possession and distribution narcotics, firearm violations, homicides, kidnapping, sexual based offences, terrorism, robberies, child abduction.

Many hot lists are compiled or administered by entities other than law enforcement agencies, including tax authorities, social security agencies, airport authorities, departments of transportation and customs. From a citizen perspective however, it is not always apparent which parties are involved. In other words, it is not clear who is watching what. Moreover, in the more exhaustive use of ANPR for the identification of potential offenders, it is not clear for citizens what criteria make that a person or group is potentially threatening. When are you perceived to be a potential offender? Does the fact that you frequently visit a certain place make you a potential suspect? These questions may particularly result in ANPR systems being experienced by citizens as an unverifiable gaze; knowing that you are being watched, while it remains vague by whom, for which purposes and with what consequences. Moreover, in cases in which people are not aware of the existence and/or operation of ANPR systems, they are not able to hold the justice system accountable for adhering to rules. In this sense, the covert application of ANPR for interception and/or investigation seems to be substantially more intrusive than the application of ANPR for speed control.

8.4.2 The utopia of the crime-free society

The use of ANPR for interception and investigation is often legitimized by police forces by pointing to increased crime solving rates. The Metropolitan Police in the UK for instance stated: *"[…] More than 110 ANPR vehicles currently patrol the city's streets but this is due to be doubled by the end of the financial year. Last year the Met [Metropolitan Police] made around 1,500 arrests using ANPR, which included arrests for robbery and firearm offences, drug trafficking and serious sexual offences."*[56] According to several police forces ANPR is a powerful tool in combatting crime. In interviews, policeemphasized the great potential of this technology in diminishing crime. Several interviewees state that police forces would even be more effective in crime solving if the potential of technology would be further exploited. Theoretically, by applying ubiquitous monitoring, almost all offenders and criminals who make use of the road can be followed and eventually caught. Involved actors (police, policy makers, but also politicians) seem to struggle with the question to which extent ANPR systems should be applied.

It seems that in the past, the increased application of ANPR often has been at the expense of less privacy. One could, however, also imagine a system in which data capture and storage is minimized, further anonymized and the processing automated. As regards speed control for instance, the information the police needs is time, location, speed, vehicle and vehicle owner. Systems which directly scan the number plate (without taking a picture) would gather substantially less privacy sensitive information. Several developers have identified other technologies to directly read number plates, for instance through the use of RFID tags. However, they perceive disadvantages of these alternative technologies, such as that these tags would require batteries which must be replaced.

56 Metropolitan Police Service, "New approach to ANPR launched", London, 2012. http://content.met.police.uk/News/New-approach-to-ANPR-launched/1400012148405/1257246741786.

According to some interviewees, the fact that these more 'privacy friendly' systems (as yet) have not been (extensively) developed and deployed may be partly explained by the misleading term ANPR, which emphasizes the number plate as data source, whereas far more other data is revealed. Moreover, interviewees do not always perceive ANPR data to be personally identifying information and therefore contend that privacy interests are limited. It has been stated that ANPR does not concern personal data as a number plate identifies a specific vehicle and not a specific person. However, two important counter-arguments can be made here. First, as interviews and documents reveal, ANPR pictures may include images of the vehicle's driver and passengers (and thus personally identifying information), which information in some instances has been used for investigation purposes. Second, in almost all cases ANPR data is used to trace (and thus identify) offenders (who e.g., exceeded speed limits or committed other offences) through the matching of ANPR data with other sources (linking of databases). In other words, in most types of usage of ANPR, persons are identified.

8.4.3 Watching the watchers?

Yet, there are several examples in which developers and police forces have incorporated privacy protection principles into ANPR systems. One of these examples is the use of audit logs, which are built into ANPR systems and record specific queries to an ANPR system (often including the identity of the user initiating the query, the license plate number or other data elements used to query the ANPR system, the date and time of the query and the response to the user's query). The audit logs are subsequently checked for inconsistencies that raise a suspicion of abuse. In most cases abuse is defined in this respect as the 'unauthorized' access to data – access to (specific parts of) the ANPR data by someone who is not entitled to that specific access. The rationale behind the audit logs is that law enforcement officers may be discouraged from requesting ANPR data if they know that their access to that data is being monitored and recorded. It is perceived to be an effective means to discourage unnecessary or inappropriate use of ANPR data and trace any improper uses to the offending party. However, what determines to what extent individuals' privacy is protected depends on the 'rules of access' – who is entitled to access which information? The extent to which parties have access to ANPR greatly varies between countries and even within countries between regions. There are examples in which several ANPR data are provide to third (non-governmental or private) parties and there are examples in which ANPR data usage is more restricted.

Another means applied by law enforcement agencies to protect individuals' privacy is to set specific retention dates. Although retention periods were once necessitated by physical storage constraints, these increasingly have become a matter of privacy policy. In several countries the secondary usage of ANPR databases raised privacy discussions and has been regulated. In the Netherlands for instance, the Dutch privacy watchdog CBP concluded after an inquiry into the retention of "no hit" data by the police force Rotterdam-Rijnmond (which retained no-hit data for a period of 120 days) that there was no legal basis for this retention of "no-hit" ANPR data. In Germany, the Bundesverfassungsgericht concluded that the retention of number plates through ANPR is in violation of the right to "Informationelle Selbstbestimmung" and therefore not allowed. In Germany, ANPR is only allowed in a very limited number of cases (i.e., cases of a concrete suspicion). However, in other countries no-hit ANPR data can be retained, for instance in Belgium for 30 days and in the UK for 5 years. In the Netherlands legislation has been drafted to retain no-hit ANPR data for four weeks. In several countries the discussion about retention dates seems to be dominated by justice

practitioners and privacy watchdogs. Justice practitioners argue that seemingly irrelevant or untimely information may acquire new significance as an investigation brings new details to light. Deleting or destroying information, justice practitioners argue, would impede investigations and potentially result in fewer cases being solved[57]. However, as privacy watchdogs and advocacy groups argue, the question should be posed whether the measure (retaining vast amounts of personal data) is proportionate to its goals. Moreover, according to privacy advocates the discussion should not only concern retention dates but also the type of data that is collected.

Just like in the case of ANPR systems used for speed control, citizens do not have much say in the design, implementation and usage of ANPR systems for interception and investigation. Moreover, as ANPR systems for interception and investigation are mostly camouflaged, citizens often are not aware of the systems. In addition, some studies indicate that citizens do not fully understand how ANPR systems work[58]. The lack of awareness and knowledge about the operation of systems makes it difficult for subjected individuals to assess the implications of the systems, oppose to it, to hold the justice system accountable for adhering to rules or to create reasonable expectations as to the future use of the information about individuals. It may also contribute to the lack of public debate about ANPR systems and the translation of broader societal values into the system. The information citizens receive about ANPR systems through media often concern stories in which police forces succeeded in solving a (high profile) crime case, without much information about the actual working of the systems and possible implications. All in all there seems a large distance to between the observer and the observed.

8.5 CONCLUSIONS

The case study shows that whereas law enforcement authorities play a dominant role in the shaping of ANPR technology, other actors – e.g., subjected users – only have limited influence. The evolution of and the values incorporated into the systems mainly represent the specific security and privacy ideas upheld by law enforcement agencies. Security is interpreted very broadly, involving many issues (ranging from road safety to human trafficking) and covering the whole security process (from prevention to crime solving). This broad understanding of security in relation to ANPR may explain the substantial expansion of ANPR usage over the past decade. Privacy values incorporated into ANPR systems predominantly yield from legal discussions on for instance retention dates (e.g., data storage), access control (e.g., encryption) and accuracy of data (e.g., camera quality). Influence of subjected users on the shape of ANPR systems seems to be very limited. Several studies indicate that citizens are not always aware of and/or do not fully understand how ANPR works. In particular in cases of camouflaged ANPR application, it might not be apparent for citizens which actor is watching what. This makes it difficult for subjected users to form a thorough opinion on ANPR systems and to influence the evolution of the technology.

57 Tracy, Meghann, Heather Ruzbasan Cotter and William Nagel, "Privacy impact assessment report for the utilization of license plate readers", International Association of Chiefs of Police, Alexandria, VA, 2009. http://www.theiacp.org/LinkClick.aspx?fileticket=N%2bE2wvY%2f1QU%3d&tabid=87.

58 E.g. Deisman, Wade, Patrick Derby, Aaron Doyle et al., *A Report on Camera Surveillance in Canada - Part One*, Surveillance Camera Awareness Network (SCAN), The Surveillance Project, Queen's University, Kingston, 2009. http://www.sscqueens.org/sites/default/files/SCAN_Report_Phase1_Final_Jan_30_2009.pdf.

9 SMART GRIDS, SMART METERS, AND CRITICAL INFRASTRUCTURES

Govert Valkenburg

9.1 INTRODUCTION

The term *smart grid* refers to the next generation of electrical power networks, in which information technologies become indispensable for their operation. By deploying information technologies, it becomes possible to make more efficient use of energy resources. Also, the network becomes more responsive and adaptive, so as to enable the use of varying, distributed and intermittent sources. Unlike the conventional power network in which large central power plants provide energy to a large group of consumers, the smart grid facilitates fine-tuning between production and consumption of electrical power.

With the development of smart electricity grids, the distribution of electrical power becomes gradually intertwined with the realm of information. Part of the informational need concerns the power consumption at the consumer level. To this end, so-called *smart meters* are increasingly installed at the household level. Unlike the classical power meters that just cumulatively count how much power is used over a longer period, these smart meters can provide information about consumption on a real-time basis.

As the development of smart grids draws ever stronger ties between the energy sphere and the information sphere, the provision of energy increasingly becomes a matter of cyber security. Cyber attacks have already been reported on power facilities causing power blackouts in Brazil,[59] even though it has also already been objected that the blackouts were actually the result of poor network maintenance, not cyber attacks.[60] Also, security breaches in US utility networks by Russian and Chinese spies have been reported.[61] Breaches have been reported as recent as late 2012 in Germany and the USA.[62]

This case study on smart grids and the smart meters through which consumers connect to the grid highlights particular versions of privacy and security, and how they are related. The security issues of smart grids are largely discussed in terms of cyber security, at the level of integrity of whole infrastructures. Privacy issues, in contrast, chiefly concern the protection of consumption data, i.e., how often smart meters are remotely read by utility companies, etc.

---

[59] Allan, Sharon, Eric Trapp and Anthony David Scott, "Critical infrastructure protection for the smart grid", Accenture, 2010. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Cyber_Security_Smart_Grid.pdf. Kroft, Steve, and Graham Messick, "Cyber War: Sabotaging the System", *CBSNews, 60 minutes*, 06 November 2011. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

[60] Harris, Shane, "Brazil To "60 Minutes: It Wasn't a Hacker", *The Atlantic*, 10 November 2009. http://www.theatlantic.com/politics/archive/2009/11/brazil-to-60-minutes-it-wasnt-a-hacker/29934/. Krebs, Brian, *Cable: No Cyber Attack in Brazilian '09 Blackout*, 2010. http://krebsonsecurity.com/2010/12/cable-no-cyber-attack-in-brazilian-09-blackout/. WikiLeaks, *09BRASILIA1383, BRAZIL: BLACKOUT - CAUSES AND IMPLICATIONS*, 2011. http://www.wikileaks.org/cable/2009/12/09BRASILIA1383.html.

[61] Gorman, Siobhan, "Electricity Grid in U.S. Penetrated By Spies", *The Wall Street Journal*, 08 April 2009. http://online.wsj.com/article/SB123914805204099085.html.

[62] Bakker, Jasper, "Malware op usb-sleutels besmet energiecentrales VS", *Webwereld*, 04 February 2013. http://webwereld.nl/nieuws/113052/malware-op-usb-sleutels-besmet-energiecentrales-vs.html. EurActiv, "European renewable power grid rocked by cyber-attack", Brussels, 2012. http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541. (Accessed: 15. December 2012)

These turn out to be two largely separate domains, which entails that privacy and security are hardly ever positioned in the mutually-exclusive relation of a trade-off. By this disconnection, this case differs from the other cases presented in this deliverable.

9.2 METHODOLOGY

The empirical base of this case study is provided on the one hand by 5 interviews, including technology experts from both academics and corporate backgrounds, and experts on the technology-society boundary and technology assessment. On the other hand, empirical material is provided by academic literature, press coverage, corporate communication and websites, material from watchdog and other societal organisations, and so on. The selection of material was not limited to one specific site, but includes material from a coherent range of technologies and situations. Thereby, the analysis earns more generalising power than if the empirical base had been confined strictly to one site of operation. From this base, a 'snapshot' is composed of the practice of energy systems comprised of smart grids and smart meters, which should make clear how privacy and security are 'done' or enacted in practice.

9.3 CURRENT TECHNOLOGY

One sense in which today's energy infrastructure differs from other technical domains engendering privacy and security issues, is the fact that it comprises many system elements of which the life span is several decades: investments made in the electrical power infrastructure often have a time horizon between 40 and 80 years.[63] This offers a sharp contrast with the domain of ICTs, where lifecycles of a few years are more typical and ones of a few months not exceptional. As will be explained in the next section, this leads to a clash of different technological cultures.

Different levels of the power system are currently in different stages of development. On the one hand, the much-discussed smart meter, sometimes called the 'intelligent terminal' that connects the consumer household to the power grid, is currently rolled out in large numbers throughout Italy, Sweden, Canada, US, Turkey, Australia, New Zealand and the Netherlands. Italy and the Nordic countries are leading the race.[64] Germany is lagging behind, but meter rollout is expected to increase there shortly.[65] On the other hand, approaches to integrating these meters into sophisticated approaches to domestic energy management are mostly found in pilot projects. The smart appliances connecting to smart meters are equally exceptional. Key standards have been established, but innovative technologies have not quite proliferated yet.

At the system level, developments are slower, but European operators have a track record of using the newest technologies in their systems. European power utilities rank among the most

[63] Netbeheer Nederland, "Net voor de toekomst: een verkenning", Netbeheer Nederland, Arnhem, 2011. http://www.netbeheernederland.nl/Content/Files/373_320008-Rapport%20Net%20voor%20de%20Toekomst.pdf.

[64] Foster, Pete, "Smart Meter Rollout in Europe - More Talk than Action", 2012. http://www.thegreenitreview.com/2012/03/smart-meter-rollout-in-europe-more-talk.html. (Accessed: 19 March 2013)

[65] Navigant Research, "Smart Meters in Europe", 2012. http://www.navigantresearch.com/research/smart-meters-in-europe. (Accessed: 19 March 2013)

reliable in the world. As one interviewee indicates, average power outages typically remain below half an hour per year. This suggests that aiming at a further reduction of blackouts would incur disproportionate costs. At the same time, making the power network ready for envisioned future demands by merely expanding its capacity would also require huge investments. Therefore, seeking technologies that enable a more efficient use of existing infrastructures, with their life spans of decades, is argued to be a much more efficient investment by several interviewees from the sphere of technological development. However, others have calculated that smart meters can at best improve the efficiency of the networks between 3,7 – in case consumers are only provided with informational feedback – and 9,5 per cent – in case consumers are provided with information, and variable energy rates are established. Also, the savings are overcompensated by the necessary investments.[66]

Intelligent control and approaches, such as self-diagnostics and self-repair, aim to make the power network more resilient and robust. According to one interviewee from the technology development sphere, this is a process that has already been going on for decades. The impression fed by discussions on smart meters, as if the smart grid would be something that has been emerging only in recent years, is thus skewed, to say the least.

Current developments at the micro level mostly take place as pilot projects. This means that they are relatively self-contained and not deeply entwined with other system parts, and that they are relatively singular in their aims. For example, one smart meter project explained by an interviewee that was aimed at influencing consumers' power use,[67] pays relatively little attention to privacy friendly approaches such as *privacy by design*.[68] Rather, it caters for basic privacy needs by deploying post-hoc data protection on stored information. Conversely, a project[69] explained by another interviewee that explicitly pursued privacy by design by deploying role division and data minimisation etc., was not so much concerned with new targets in efficiency and demand-side management (DSM, see also 9.5.4).

9.4 BACKGROUND OF EMERGENCE

Towards the end of the twentieth century, power grids had mainly developed as interconnected systems, to which bulk generators were connected, and which uni-directionally provided power to end users. The amount of power generated was, and to a large extent still is, determined by predictions of power need at a particular moment. In consequence, a certain surplus of power is always needed to accommodate for fluctuations. Also, such a system is poorly able to incorporate power sources that are less deterministic, such as solar plants and wind turbines. Therefore, sophisticated control technologies are envisioned and developed to make the system more flexible.[70]

[66] Fraunhofer ISI, "The project Intelliekon presents first results on saving electricity via smart metering: Timely information enables up to 3.7 per cent reduction in consumption", 2011. http://www.isi.fraunhofer.de/isi-en/service/presseinfos/2011/pri11-13.php?WSESSIONID=50b6ba2a8ec56aa4fda421890f4e4b5f (Accessed: 18 March 2013)

[67] *Jouw Energiemoment* ('your energy moment'), developed by Dutch distribution system operator Enexis.

[68] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner of Ontario, Toronto, 2011. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

[69] *Smart Charging*, a project developed by Dutch distribution system operator Enexis, aimed at electric mobility.

[70] Netbeheer Nederland, "Net voor de toekomst: een verkenning", Netbeheer Nederland, Arnhem, 2011. http://www.netbeheernederland.nl/Content/Files/373_320008-

Thus, the primary challenges that the power system faces include a transition from centralised bulk generation to more distributed and intermittent generation as a consequence of the use of renewable sources, and a more efficient and flexible use of existing power infrastructures. This in turn entails the need to collect use-data in a more granular way, which is impossible with conventional meters that just cumulatively record power consumption. An additional challenge is posed by EU targets for increasing energy efficiency and reducing energy consumption.[71]

When a system becomes more complex, it also becomes more vulnerable. This means that disruption of power supply as a result of systemic failure becomes more difficult to manage.[72] The security and continuity of energy supply is considered essential within security agendas, both at the national and the European level.[73] The increasing complexity of the system entails increasing vulnerability, which lowers security, which in turn is thus ironically connected to the on-going evolution of the energy system and the extent to which we depend on it.

A consequential challenge appears in that the power system becomes essentially also an information system. Thus, it becomes part of cyberspace, inheriting from the cyber sphere a vulnerability to cyberterrorism and cyber crime. Cyber attacks have indeed been reported.[74] These attacks have hitherto been aimed at core system components such as power plants and distribution systems, not at consumer-level elements such as smart meters and smart appliances. However, attacks on the latter will only be a matter of time.

Practices of smart grids can be understood as three domains coming together. First, there is the domain of operational technology. The name ‘operational technology’ refers to those technologies that facilitate the core processes of energy production and distribution: generators, power lines, transformers, and the switches that connect and disconnect them. Conventionally, these switches were operated by hand: a human operator locally monitored processes and switched system elements on or off, and communication took the shape of a phone call. Since the 1950s, such monitoring and switching processes has become increasingly remotely operated. This then became known as SCADA: supervisory control and data acquisition systems. This falls under the greater domain of ICS, industrial control systems.[75]

Rapport%20Net%20voor%20de%20Toekomst.pdf. van Voorthuizen, Joris, and Han Slootweg, *Smart Grids*, Position Paper, Enexis DSO, 2011. https://www.enexis.nl/Documents/position-paper-smart-grids-2011-06.pdf.

[71] Directive 2006/32/EC, "Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC", *Official Journal of the European Union*, L 114, pp. 64-85. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:114:0064:0064:en:pdf.

[72] McDaniel, Patrick, and Stephen McLaughlin, "Security and privacy challenges in the smart grid", *Security & Privacy, IEEE*, Vol. 7, No. 3, 2009, pp. 75-77.

[73] European Commission, "Energy Infrastructure: Critical Infrastructure Protection", 2013. http://ec.europa.eu/energy/infrastructure/critical_en.htm. (Accessed: 18 March 2013)

[74] Gorman, Siobhan, "Electricity Grid in U.S. Penetrated By Spies", *The Wall Street Journal*, 08 April 2009. http://online.wsj.com/article/SB123914805204099085.html. Harris, Shane, "Brazil To "60 Minutes: It Wasn't a Hacker", *The Atlantic*, 10 November 2009. http://www.theatlantic.com/politics/archive/2009/11/brazil-to-60-minutes-it-wasnt-a-hacker/29934/. WikiLeaks, *09BRASILIA1383, BRAZIL: BLACKOUT - CAUSES AND IMPLICATIONS*, 2011. http://www.wikileaks.org/cable/2009/12/09BRASILIA1383.html.

[75] Allan, Sharon, Eric Trapp and Anthony David Scott, "Critical infrastructure protection for the smart grid", Accenture, 2010. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Cyber_Security_Smart_Grid.pdf.

Second, there is the domain of information and communication technologies. These technologies take data and information as their resource of operation. This is exactly what makes the connection between ICTs and SCADA processes non-trivial. Focusing on primary processes of energy provision and focusing on processes of information processing are radically different stances leading to different consequences, and they build on different histories and engineering cultures. As one interviewee illustrates, at some point the operation of a SCADA system was assigned to an ICT-oriented operational unit. Aware as they were of threats from cyber space, they rolled out a virus-protection system throughout the plant. As a consequence of the rollout process, energy-related processes were left unmonitored for some 15 minutes. Doing this with high-energy installations is extremely dangerous, and it is also against all paradigms in SCADA. Another difference is that in operational technology (OT), i.e. those systems that actually transport the electrical power, investments typically have a life cycle of decades, whereas in IT this is typically years and sometimes even only months.[76]

Third, there is the domain of home automation, domotics, ambient intelligence, and consumer convenience. To this domain, the smart meter and the home energy computer are central. The smart meter allows for very detailed registration of power consumption in a household. This may be used for flexible pricing, load balancing and demand side management, or innovative services that use data and which are currently unforeseen. This domain of domotics could be largely disconnected from both OT and IT domains, though connecting them would probably open up new avenues for innovation. Also, it is in this field of domotics that new services might be important to create consumer acceptance. The added convenience might be an additional stronghold in case energy savings remain below expectation, or in case technologies raise the suspicion of privacy invasiveness.

9.5 SOCIOTECHNICAL ANALYSIS

9.5.1 The future is green and informational

The three main historical strands elaborated in the previous section each pursue different aims in partly overlapping discourses, through which developments towards smarter energy systems are legitimated and given direction. For example, smart meters are presented to the general audience as an 'obligatory passage point' towards an electrical power grid that embraces sustainable energy. Smart grids and smart meters are often legitimated with an explicit appeal to the so-called 20-20-20 targets, or a 20 per cent reduction in emissions, a 20 per cent increase in renewable generation, and a 20 per cent improvement in energy efficiency by 2020.[77] *Demand side management*, i.e. influencing people's power consumption behaviour through the provision of information or even through the active control of their appliances, becomes possible when people have disposal of more granular use-data than they had with the conventional power meter.[78] Power savings of up to 10% have been reported through demand

[76] Cisco, "Securing the Smart Grid", White paper, Cisco Systems Inc, San Jose, CA, 2009. http://www.cisco.com/web/strategy/docs/energy/SmartGridSecurity_wp.pdf.

[77] Cavoukian, Ann, *Smart Meters in Europe: Privacy by Design at its Best*, Information and Privacy Commissioner, Ontario, Canada, 2012.

[78] Capgemini, "Smart Metering: The holy grail of demandside energy management?", 2013. http://www.in.capgemini.com/m/in/tl/tl_Smart_Metering__The_holy_grail_of_demand-side_energy_management_.pdf. (Accessed: 15 March 2013)

side management.[79] Also, the yearly power balance could be established with greater reliability and accuracy. By corollary, the smart meter would help in tracing and preventing electricity theft. Delicately, it has also been argued that manipulating the data flows from the meters themselves open up new opportunities for energy theft.[80]

Part of this rhetoric merits critical attention. For example, as several interviewees indicate, the stability of the energy system under the use of intermittent sources does in fact *not* depend on smart meters. Also, many discussions are conducted as if the energy system is soon to become one big internet-like data system, that could collapse if 'scriptkiddies' hack their neighbour's smart meter. However, today, and probably even in the distant future, the informational structures that make up the energy system are very much segmented, such that it will probably be easier to demolish the power supply by brute force than by logging into your smart meter. Also, in order to give the consumer full control over the use of their use-data, it is left to them to decide how often the meter readings will be collected, which in principle abates some privacy issues. This in turn raises the issue of consumer education, as consumers may lack knowledge to make such decisions, in particular about where the data is stored, who has control over it an access to it, and what the consequences of such arrangements are. At a more abstract level, complications may arise because consumers potentially hold knowledge frames that are different from the frames held by technology experts, operators, and utility provides.

From this first birds-eye overview, already some peculiar privacies and securities can be identified. On the one hand, the individual consumer is rendered more and more as an active part of the system, rather than a passive recipient of energy. This means that part of their actions become to some extent public in a way they were not before. At the same time, new options become available for the end user in their ways of sharing usage information. The fact that they can make new choices is in a way an increase of decisional privacy, even though before, there was simply no need to make these decisions.

9.5.2 Securing power supply

Obviously, electrical power is of immeasurable importance to modern daily life. Economic loss upon power outage is huge, and even human lives may depend directly upon electrical power – although hospitals and air traffic control centres, etc. of course have extensive backup facilities. Additionally, the term critical refers to the interconnectedness of various infrastructures, and the possibility of problems in one section invading into another. This concerns infrastructures of the same kind, e.g. power infrastructures in adjacent countries, as well as different infrastructures, such as the interdependency of communication networks and power networks in the same area. Indeed, problems with a high-voltage power line in Germany have already been reported to cause power outages in a handful of European countries and even Morocco in 2006.[81]

[79] van Voorthuizen, Joris, and Han Slootweg, *Smart Grids*, Position Paper, Enexis DSO, 2011. https://www.enexis.nl/Documents/position-paper-smart-grids-2011-06.pdf.

[80] McLaughlin, Stephen, Dmitry Podkuiko and Patrick McDaniel, "Energy Theft in the Advanced Metering Infrastructure", in Erich Rome, and Robin Bloomfield (eds.), *Critical Information Infrastructures Security*, Springer, Berlin, Heidelberg, 2010, pp. 176-187.

[81] Hämmerli, Bernhard, and Andrea Renda, "Protecting Critical Infrastructure in the EU - CEPS Task Force Report", Centre for European Policy Studies, Brussels, 2010. http://www.ceps.eu/ceps/dld/4061/pdf.

By connecting different national power systems, the continuity of power supply has become a national as well as an international concern. For this reason the European Commission has designated the power infrastructure as a critical infrastructure. Critical infrastructures are "… those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health safety, security or economic well-being of citizens or effective functioning of governments."[82] Not only does it refer to the power system, but also other infrastructures such as banking systems and air and sea ports.

Importantly, critical infrastructures have important *cultural* meanings, never only economical. Their cultural meaning is in the fact that they symbolise the stability of society, the dependability of government, or in short: civilization. This is what makes them interesting targets for terrorists. To them, not the infrastructural disruption itself is valuable, but the fact that an entire culture loses confidence in the particular infrastructure and by consequence in society at large.[83] This engenders particular framings of security, which in turn entails particular definitions of security problems. In the case of energy security, security is mostly framed either in the context of a war, in the context of human subsistence, or in a discourse of 'total security'.[84] Also, a German report has identified difficulties deriving from the fact that important parts of energy utilities are in corporate hands, making security a particularly hybrid public-private affair.[85]

The increasing dependency of the power system on the use of information entails at least a number of theoretical vulnerabilities. These include at least the following:[86]

1. Bidirectional communication can in principle be intercepted and spoofed.
2. Systems become more distributed and interconnected. While this basically increases resilience and decreases vulnerability, it also increases the exposure of systems to disturbance, whether intentional or, for example, as the consequence of natural disaster.
3. There is the intrinsic vulnerability to abuse that is the consequence of the very act of collecting user data.
4. The more smart metering devices become capable of, the greater the need to subject them to extensive security measures.
5. From the prior situation of low data-intensity, a weak approach to authentication and access control has been inherited.

[82] Burgess, J. Peter, "Social values and material threat: the European Programme for Critical Infrastructure Protection", *International Journal of Critical Infrastructures*, Vol. 3, No. 3/4, 2007, pp. 471-487. European Commission, "Critical Infrastructure Protection in the fight against terrorism", COM (2004) 702 final, Brussels, 2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF. Hämmerli, Bernhard, and Andrea Renda, "Protecting Critical Infrastructure in the EU - CEPS Task Force Report", Centre for European Policy Studies, Brussels, 2010. http://www.ceps.eu/ceps/dld/4061/pdf.

[83] Burgess, J. Peter, "Social values and material threat: the European Programme for Critical Infrastructure Protection", *International Journal of Critical Infrastructures*, Vol. 3, No. 3/4, 2007, pp. 471-487.

[84] Ciută, Felix, "Conceptual Notes on Energy Security: Total or Banal Security?", *Security Dialogue*, Vol. 41, No. 2, 2010, pp. 123-144. http://sdi.sagepub.com/content/41/2/123.abstract.

[85] Petermann, Thomas, Harald Bradke, Arne Lüllmann et al., "What happens during a blackout: consequences of a prolonged and wide-ranging power outage", Office of Techonlogy Assessment at the German Bundestag, 2011. http://www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf.

[86] Allan, Sharon, Eric Trapp and Anthony David Scott, "Critical infrastructure protection for the smart grid", Accenture, 2010. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Cyber_Security_Smart_Grid.pdf.

6. People may not be sufficiently equipped in terms of education and training to deal with the new complexities of the power infrastructure.
7. It seems that standardization and interoperability still have a long way to go, which entails that currently, it is relatively difficult to subject systems to security and privacy audits.

As explained before, smart grids must be seen as the conflation of at least three domains. One of them, the domain of operational technology (OT), ICS and SCADA, hitherto translated security mainly as physical security. Basically, security meant that physical keys were needed to open physical doors. This is radically different from security as understood in the ICT domain. At the same time, increasing use of ICT in the operational technology domain does not mean that also the security culture of ICT can be as easily transferred to that domain. For example, it is even beyond discussion in ICT that people should always identify themselves with some account, if only by a basic username and password. However, this is not as straightforward in a field station, where access should be immediately granted in cases of emergency. If a technician passes by unmanned stations on a very irregular basis, and if it is more important *that* a particular action is performed than by *whom* it is performed, it is easy to see that account-based access is not easy or naturally embedded in operational routines, and even poses difficulties to keeping OT processes in the air.

Opinions differ on how a security threat should be assessed when so many devices are located 'in the field'. Some argue that this is the primordial vulnerability of today's power infrastructure.[87] At the same time, one interviewee points out that this is the same reason that some other threats become irrelevant. For example, it will be very difficult for 'scriptkiddies' to gain access to these systems in the field, because they cannot get access to 'model devices' to even start practicing their hacking skills, though this might change if those technologies become less expensive. However, another interviewee argues that smart meters are a fundamental risk for the continuity of power provision, because they are an exposed part of the great information system that the power system is about to become. Contrarily, several interviewees explain that there is no data link between the smart meter and the systems that are to keep the greater system stable, making the previous vulnerability somewhat academic.

Indeed, gaining access to high-level systems to, for example, shut off electricity in entire areas, if not impossible, would at least be considerably harder than 'simply' hacking into the IT systems of the transmission system operator (TSO) through the Internet and see what trouble can be made there. Thus, while security concerns are cherished from the very beginning, their consequences in the OT domain are sometimes surprising from an IT perspective.

Nonetheless, one interviewee explains an interesting vulnerability: In order to secure maximum versatility, smart meters have been equipped with a switching functionality. First, this introduces a vulnerability to hacking, and enabling others than the utility companies to take a household off the power grid. Second and more intricate, if such a hack was performed with large numbers of households at the same time, then the total power consumption would drop from normal levels to something much lower in a very short period of time. The network is not adapted to such fluctuation, simply because power generation cannot be taken offline

[87] Cisco, "Securing the Smart Grid", White paper, Cisco Systems Inc, San Jose, CA, 2009. http://www.cisco.com/web/strategy/docs/energy/SmartGridSecurity_wp.pdf.

that quickly. This will lead to a great surplus of power to which the network cannot adapt. Considerable damage might be the consequence.

Also experts are divided as to whether security concerns should be handled proactively or reactively. On the one hand, one interviewee argues that a proactive security policy is not feasible. As the system is open and complex, each and every part of its behaviour cannot be predicted in advance. Broken smart meters will inevitably occur, and it would be of little use to call off alerts if some unexpected (data) behaviour is observed. On the other hand, Cisco argues[88] that security approaches should be proactive, and potential targets for cyberterrorists be charted. While these are not necessarily mutually exclusive, they entail different approaches and different framings of security issues, appropriate for different primary security threats.

9.5.3 Data integrity and privacy as data protection

Smart meters, introduced as part of the facilitation of the transition towards smart energy grids and renewable sources, offer a boon of consumer data. They potentially record our power use in a very detailed way, which obviously falls under the category of personal data, as it is uniquely connected to an individual person. One intricacy is in the fact that such data pertains to a household, not a strictly person, a situation that might be anomalous in face of privacy regulations. This information can exploited in numerous new – beneficial as well as harmful – ways. For example, home appliances have typical 'power consumption fingerprints', which at least theoretically opens up the possibility of establishing profiles of a household. This could reveal when people typically do their laundry, or whether a new cohabitation seems to have started. Also, if this consumption is monitored real-time, it is possible to draw conclusions as to whether a family has been away for a few days, suggesting that they might be on vacation and rendering their home a good candidate for burglary.[89] Even if these concerns seem far-fetched or academic, people may still object to a company gathering this data about them.

Several interviewees explain that it is therefore vital to protect consumers' data and prevent its unnecessary collection, as well as paying due attention to communicating to consumers what their data are needed and used for. As one interviewee explain, experience tells that if consumers can sufficiently recognise the added value of using a smart meter, they are willing to provide their use-data for this purpose. Importantly, this added value need not be monetary. For example, benefits for the environment and for future generations by seeking alternatives to depleting fossil reserves constitute commonly accepted aims. Similarly, one interviewee presents the convenience of allowing for remote fault analysis in case of disruption as a promising possibility.

Nonetheless, people are keen on privacy. Two basic mechanisms are deployed to offer the best possible data privacy: aggregation and segmentation. The former stands out in

[88] Ibid.

[89] Krebs, Brian, "Experts: Smart grid poses privacy risks", *The Washington Post*, 18 November 2009. http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_priva.html. Munkittrick, David, "Smart Grid Technology Implicates New Privacy Concerns", 2012. http://privacylaw.proskauer.com/2012/03/articles/data-privacy-laws/smart-grid-technology-implicates-new-privacy-concerns/. (Accessed: 19 March 2013). My Secure Cyberspace, "Smart Grid and Privacy Concerns", 2013. http://www.mysecurecyberspace.com/articles/features/smart-grid-and-privacy-concerns.html. (Accessed: 19 March 2013)

comparison to many other areas in which data protection is an issue. If your use-data are taken together with those of your neighbours, the data are rendered less personal, while still usable for most purposes. If data are aggregated at street or block level, they are still useful for analysing the demand, while practically no individual personal data can be extracted from it. For example, Kursawe et al.[90] have devised an algorithm that first encrypts user data, and then allows for the addition of those data in the encryption space without the need to first decrypt them. A simpler approach is the addition to user data of random data that over a large number of accounts add up to zero.[91]

The second mechanism, segmentation, comprises the idea that data are not stored in one database, but at different places and dedicated to specific purposes, such that at each place only those data are available that are actually needed. As a matter of fact, segmentation coincides well with the liberalisation of the energy market. First, power supply has already been split up over the last decades into production, transport, distribution and retail companies. This disentanglement has mainly been pursued to open up the energy market for competition. Second, developments in the ever smarter grid open up opportunities for new and inventive services. For example, a service could be developed that offers a very specific analysis of your energy consumption. Alternatively, a retailer could offer you electrical energy at an extremely low price, under the condition that you can be taken offline for a limited number of times per year, such that your consumption can be supplied by the excess of available energy. (Depending on the exact consequences of switching off, this raises of course ethical issues: people might be seduced to endanger themselves in return for some small financial gain.) As all these different uses need different information, and a lot of effort is being made to show to consumers that indeed only those segments of data are stored and made available that are needed for a particular purpose by a particular party.[92]

However, currently, consumer data, in whatever segmented or aggregated form, is not needed for things such as load balancing, but it might offer interesting opportunities in the future. Importantly, this data sphere of consumer power use is completely detached from the SCADA systems that maintain the stability of the macro power grid. This entails, *inter alia*, that smart meters offer no gateway to the high-level control systems. According to several interviewees, even if one meter is hacked, it will not offer any exposure of the system at large to malevolent actions. An average energy meter will have a life span of about 15 years from introduction to deprecation. It is presumed that during this life span, a meter will in some sense be compromised. However, the system is arranged such that this should not pose any significant threat.

Remarkably, this focus on information and its integrity plays out differently in Europe than it does in the US. In Europe, the focus is on the added value in terms of new services, greater efficiency and greater reliability. In the US, in contrast, focus seems to be more on the

[90] Kursawe, Klaus, George Danezis and Markulf Kohlweiss, "Privacy-friendly Aggregation for the Smart-grid", in Simone Fischer-Hübner, and Nicholas Hopper (eds.), *Privacy Enhancing Technologies*, Springer, Waterloo, ON, Canada, 2011, pp. 175-191. http://research.microsoft.com/pubs/146092/main.pdf.

[91] Cavoukian, Ann, *Smart Meters in Europe: Privacy by Design at its Best*, Information and Privacy Commissioner, Ontario, Canada, 2012.

[92] Source: Two interviews with technology experts from distribution system operators.

integrity of data.[93] Also, smart meters are presented as a solution against the theft of electrical energy, though this argument is mostly used in the US.[94]

9.5.4 Redefining self-determination

One new application made possible by smart grids is *demand side management*. In conventional power grid configurations, electrical power would be generated in bulk, based on an estimated load profile. First, this means that a considerable overhead is needed, since the prediction of demand is only known statistically and hence loaded with error. Second, this means that conventional sources cannot easily be replaced by renewable sources such as photovoltaic plants and wind farms, as these are much more intermittent and dependent on daylight and weather conditions. Against these two challenges, it would be of great help if the demand for electrical energy could be better attuned to supply.

Controlling the energy consumption at the consumer level comes in two basic forms. First, it can be used to avoid hitting the limits of supply. Second, it can be used to spread energy consumption over time and make more efficient use of available resources.[95] This so-called peak-load shaving[96] decreases the need for surplus supply, and thus reduces the overall cost of electrical energy. Remarkably, this benefit also accrues to those who do not take part in the innovation.

Reduction of the overhead needed and the adoption of intermittent sources require that demand becomes better structured than a mere stochastic process. One option would be the introduction of flexible pricing, and make electrical power more or less expensive, depending on availability. This flexible pricing should then seduce people into adjusting their power use to availability. This may for example mean that their laundry should be done not at a fixed time during the week, but whenever power is cheap. Washing machines able to handle such pricing information already exist, and they sometimes are among the perks that people enjoy when participating in smart energy pilots. It should be born in mind, that demand side management is foremost beneficial for network operators because it increases the overall efficiency of their network; benefits only marginally accrue to the customers.

Privacy of behaviour and action is one of the conceptual versions of privacy.[97] By the mechanism described above, the decision on when to do the laundry is reconfigured, and public and private elements are arranged differently in that decision. This is not to say that it is a grave encroachment of privacy and an interference with essentially private decisions. Yet it is to say that some of the determination of our lives is connected in a different way than

[93] Allan, Sharon, Eric Trapp and Anthony David Scott, "Critical infrastructure protection for the smart grid", Accenture, 2010. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Cyber_Security_Smart_Grid.pdf.

[94] Cavoukian, Ann, *Smart Meters in Europe: Privacy by Design at its Best*, Information and Privacy Commissioner, Ontario, Canada, 2012. Also various interviewees confirm this point.

[95] Clastres, Cédric, "Smart grids: Another step towards competition, energy security and climate change objectives", *Energy Policy*, Vol. 39, No. 9, 2011, pp. 5399-5408.

[96] Giordano, Vincenzo, Flavia Gangale, Gianluca Fulli et al., "Smart Grid projects in Europe: lessons learned and current developments", EUR 24856 EN, Publications Office of the European Union, Luxembourg, 2011. http://ses.jrc.ec.europa.eu/sites/ses/files/documents/smart_grid_projects_in_europe_lessons_learned_and_current_developments.pdf.

[97] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.

before to the world outside our front door. A cornerstone of privacy in modern societies is the recognition of home as a sanctuary,[98] and this rearrangement at least conceptually presents interference of some sort with this home.

9.6 CONCLUSIONS

In the case of smart grids and smart meters, security is constructed rather differently at the level of individual consumers than it is at the network level. At the consumer level, it takes the shape of relatively 'mainstream' approaches such as data protection, data segmentation, and role separation. At the network level, it quite often takes the shape of physical access control. This can be traced back to different histories and path dependencies, and especially to different problems that are to be solved: while security in the form of access control is very important at the network level, it is also very important that actions can be taken immediately, entailing that the security paradigm of a user account with a password might not be the best solution. In contrast, at the consumer level, the paradigm of user accounts and passwords is appropriate, although it is clearly only a baseline, and many privacy and security ensuring measures are placed on top of it. At these two levels, the problem of security is defined very differently, leading to different translations in terms of how technological solutions are arranged.

Because of the watershed between the two levels, the issue of privacy does not really exist at the higher level of network devices. Network devices do not convey personal information, nor do changes in the network architecture seem to open up new privacy threats – that is, from an *operational technology* perspective. Obviously, the ICT infrastructures over which consumer devices such as smart meters are connected, does entail such hazards. However, these are more akin to classical information protection problems, although they show some unique properties that require unique approaches such as the segmentation and aggregation techniques explained above.

[98] Cavoukian, Ann, *Smart Meters in Europe: Privacy by Design at its Best*, Information and Privacy Commissioner, Ontario, Canada, 2012.

10 DEEP PACKET INSPECTION AND INTERNET MONITORING AND SURVEILLANCE

Arnold Roosendaal and Anne Fleur van Veenstra

10.1 INTRODUCTION

The Internet is an enormous source of information for users, but it also offers opportunities for close monitoring of users' activities. Due to the fact that Internet use implies a constant interaction between a computer (or other device) and most of the time one or more web servers, all types of use leave digital trails. Traditionally, if something unlawful or illegal is done in an offline context, forensics can help discover who did what, at what time and what location. By analogy, in an online environment, the digital trails can be subjected to digital investigation. These digital forensics can, similar to the offline situation, help to answer questions related to a crime.

Solving a crime is an important achievement. An even greater achievement is made when crimes are prevented, since harm and damage are pre-empted. For this reason, police authorities have several competences and means which help to identify preparations of crime. In order to prevent crimes, suspicious activities have to be identified and analysed. On the Internet, this can be done by means of monitoring and surveilling online activities, either with a focus on specific users, or targeted at groups, communities, or specific activities. In the former case, a legal basis may be needed and the monitored individual has to be a legal suspect.

There are several means and technologies to monitor Internet activities. It depends on the type of activity that is sought and on the level of focus – either individuals or groups, activities, etc. – which surveillance technology is most suitable. Additionally, monitoring can be started from one or more specific websites and their visitors, or from the users themselves. An example of monitoring at the level of a website can be found in the context of copyrighted materials that may be offered for unlicensed download. For instance, in copyright infringement cases, the users who were illegally uploading materials were monitored, therewith making these available for other users. The uploading (making public) of these materials is unlawful/illegal[99] and individual uploaders were sued by copyright holders.

The other type of monitoring, starting at a specific user, comprises of following the activities of this user. The computer of the user is identified or the user is recognised when using other computers (for instance, based on login credentials). Once the user or the computer that is used is identified, activity can be monitored. Usually, the monitoring takes place by the Internet Service Provider (ISP) on request of law enforcement authorities. This includes inspecting the websites visited, as well as registering with whom interactions have taken place, for instance, via e-mail or on a social networking site.

As described above, Internet surveillance means that authorities are 'looking around' on the Internet in a comparable manner as they do when surveying the street in a city. Both online and offline, surveillance is automated. Offline, automation has taken place with the introduction of surveillance cameras and ANPR technologies. Online, surveillance can be

[99] Depending on whether a civil law or a criminal law approach is taken in a legal procedure specific terminology is used.

carried out by individuals searching for Internet activities of others, but it can also take place automatically, for instance, based on keywords or specific types or pieces of content that are searched for. For the past decades technologies have been developed that can monitor more online activity, more intensively.

Internet monitoring is used for different forms of surveillance. Some forms of monitoring applied by commercial network providers focus on network management to ensure efficiency and stable performance of the network. In other cases, Internet monitoring goes beyond a focus on technical performance of the network and extends to law enforcement and commercial purposes. For example, network providers may apply surveillance technologies to monitor packet content in order to identify illegal or unlawful material that is distributed over the web.

Several technologies allow for Internet monitoring and surveillance. The choice for a technology depends on the specific purpose the user of the technology wants to achieve. Some distinctions can be made. First, the application of monitoring technologies can be related to commercial purposes or to purposes of criminal and other governmental investigation (intelligence). In relation to commercial purposes, the application may relate to the search for unlawful content or for the management of network capacity. In the context of intelligence, the use can be focused on the general use of the Internet, on specific content, or focused on specific individuals that have been identified as potential criminal suspects. In particular, the prevention of terrorist attacks by means of Internet monitoring has gained attention.

Well known technologies for Internet surveillance are 'packet sniffing' and 'deep packet inspection' (DPI). Packets are small quantities of data into which all information transported over the Internet is subdivided. Just before the content is shown to a user or otherwise meaningfully processed by a computer, the packets are recombined to recreate the original content, such as an e-mail message or a web page. The packets contain the IP addresses of both the sender and the receiver. A packet sniffer can inspect this routing information and check it against a blacklist. DPI systems can be used to inspect entire packets travelling the network, looking not only at packet headers like legacy systems do, but also at the packet's payload.[100][101]

DPI is a prominent example of a technology used for Internet surveillance and will be the specific technology focused on in this case study.

10.2 METHODOLOGY

This case study utilised desk research to give an initial description of DPI technology and its use. Documents studied included policy documents, statements made by activists, scientific studies and academic articles. Furthermore, three semi-structured interviews were conducted

[100] TNO, *BIAR-Deelrapport: Technieken om online-radicalisering te signaleren*, TNO-DV, Vol. 2010 C 439, 2010.
[101] Mochalski, K., and H. Schulze, "Deep Packet Inspection: Technology, Applications & Net Neutrality", White Paper, Ipoque, Leipzig, 2009. http://www.ipoque.com/sites/default/files/mediafiles/documents/ipoque_WP_Deep_Packet_Inspection_2009_DPI.pdf.

to fill the gaps and to verify the findings, as well as to complement the case study with practical insights and interpretations of the people that develop and apply DPI technology. The interviewees included a representative of the Dutch supervisor for the telecom market, an academic expert on DPI, and a privacy activist, representing several international public rights associations. The researchers aimed to include a representative of an ISP (Internet service provider) into the study, but these organisations did not want to be interviewed on the matter of DPI, since it is a sensitive issue in the Netherlands.

10.3 TECHNOLOGY

One specific surveillance technology is Deep Packet Inspection (DPI). "DPI is the process of inspecting network packets by a third party (i.e., not the party sending or receiving the packets) to reveal the *content* of the communication between two end-points for analysis and other purposes, such as automated differentiation. 'Deep' in DPI refers to the fact that all available information is extracted from the communication stream."[102] DPI has several applications. It is commonly used to detect viruses or spyware when deployed in firewalls or virus scanners. Other applications relate to network management by network providers. Commercially, DPI can be used for targeted injection of advertisements. Finally, in a law enforcement context, DPI can be used for interception of communications. There is also a an open source version of the DPI technology that was initiated by the commercial provider, Ipoque. [103]

The application of DPI is by nature a risk for the privacy of communication as DPI is used for monitoring online activity. The potential impact of the use of DPI technology on privacy of Internet users depends, next to the type of application, on the level of inspection. Internet communication takes place over several layers (e.g. network layer, protocol layer, application layer, and content layer) and the layer that is inspected determines whether the actual content (payload) of a communication is seen or not. If not, the technology may be suitable for identifying the type of content, such as video, Voice over IP (VoIP), or the Skype protocol. In the design phase, some choices can be made here, including levels of difficulty to change the algorithm for the DPI tool later on. In cases where an algorithm can be easily adjusted, it is easier to use the technology for additional analyses after implementation. This may harm privacy more than when these algorithms cannot be altered after the technology has been implemented.

While the technology almost by nature presents a risk to privacy, since it is being used to look into Internet traffic at different levels, its application in a specific environment and bound by specific rules determines its actual level of privacy infringement.

10.4 APPLICATION OF TECHNOLOGY

As described before, DPI technology is used by public authorities for purposes of the prevention of crime and terrorism (intelligence), as well as by private parties, for purposes of network management.

[102] Meulenhoff, P., and M. Van der Werff, "Deep Packet Inspection", TNO Report 35134, TNO, Groningen, 2010.
[103] NTOP, "nDPI: Open and Extensible GPLv3 Deep Packet Inspection Library", 2013. http://www.ntop.org/products/ndpi/.

The use of surveillance technologies such as DPI, by public authorities is based on the need to prevent terrorism in the information society. It appears that important parts of terrorist networks and communications were facilitated by the Internet. The reasons for terrorists to use the Internet include propaganda, financing, training, planning, execution, and cyber attacks.[104] Except for the latter, all applications relate to organisational and practical issues concerning terrorist purposes in the offline environment. Cyber attacks are a category in itself and will not be discussed here in detail. In terms of intelligence, the monitoring and identification of terrorist networks and activities is of utmost importance in order to prevent attacks. Taking this into consideration, the 9/11 attacks have sped up the passing of several legislative documents, which empower authorities to strictly monitor Internet activities for prevention purposes. Thus, these technologies are approached as *security* technologies by state authorities. They can be of help in targeting suspicious materials or actions on the Internet. "Surveillance computers do not just surveil: they direct the attention of police and other authorities to 'targets' identified by algorithms."[105]

In a commercial context, DPI is often used for network management and differentiation of Internet traffic. In this case, the technology can be labelled as either a privacy or a security technology. Besides as a security technology for identifying malware or network malfunctioning, DPI can be seen as a privacy technology in case it is used for identification of spyware or malware aimed to steal personal data. As DPI is primarily intended to look into the payload of Internet traffic, users have mainly labelled the technology as a risk to privacy. It should be noted, though, that for DPI not to be privacy invasive, additional measures need to be taken.

In the Netherlands, independent research by supervisory authorities shows no evidence of unlawful or illegal intrusion of web contents or illegal differentiation in practice.[106] In 2011, several ISPs were subjected to investigations in their DPI applications by the Dutch Telecommunications Supervisory Authority. Even though this authority found no unlawful practices, public outrage forced companies to revise their use of DPI. Moreover, the Dutch Data Protection Authority started its own research afterwards with a specific focus on data protection issues related to the use of DPI by ISPs. The findings of this research are expected to be presented in 2013. Generally, the use of DPI for purposes of network (performance) management does not enable identification of the web users. Identification can only be based on IP addresses, which are linked to the user by means of a traffic accounting system (assuming the customer or subscriber to be the actual user). Another possibility is to look at the payload or 'actual content' of network packets, which is likely to reveal additional information. This may include information such as cookies or usernames, which can be used to identify a user.[107]

[104] UNODC (United Nations Office on Drugs and Crime), *The Use of the Internet for Terrorist Purposes*, United Nations, Vienna, 2012. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[105] Brown, Ian, and Douwe Korff, "Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime.", Information Commissioner's Office, Wilmslow, 2004.

[106] OPTA, "Voorlopige bevindingen OPTA over gebruik van Deep Packet Inspection door aanbieders van mobiele telefonienetwerken", OPTA/ACNB/2011/201469, Den Haag, 2011. http://www.opta.nl/nl/download/publicatie/?id=3439.

[107] Meulenhoff, P., and M. Van der Werff, "Deep Packet Inspection", TNO Report 35134, TNO, Groningen, 2010.

10.5 SOCIO-TECHNICAL PRACTICE

When looking at the prevention of terrorist attacks, several foci of attention can be distinguished in Internet surveillance and monitoring. These include:

- Looking for distribution via email etc. of specific content/user guides, such as manuals or training guides, that can be used for terrorist attacks (content)
- Looking for suspicious behaviour (behaviour)
- Monitoring a suspicious group of people (behaviour)
- Monitoring a suspicious individual (behaviour)
- Monitoring and tracking suspicious content (content)

Thus, surveillance can be focussed either on content or on behaviour. In both cases, an indication is needed that the specific type of content or behaviour relates to (potential) criminal activities. However, from a privacy perspective, the monitoring of content types may be less intrusive than the monitoring of behavioural types, since only the latter is directly connected to an individual or a group of individuals. A type of behaviour is personal and is a specific characteristic of an individual's identity. Content is not directly linked to an individual. Only when an individual accesses a piece of content can the content be linked to this individual and become part of an individual profile.

In industrialised countries, the use of DPI technology was deemed to be very intrusive by the general public, even though its actual setup was not found to harm the privacy of Internet users in any way. Concerning the use of DPI by state authorities, privacy concerns as well as the fear of function creep and surveillance states have influenced industrialised countries' decisions to avoid using the technology for monitoring individuals' online activities at a large scale. Nevertheless, it appears that several companies are developing the technology and selling it to questionable regimes elsewhere, for example to read e-mails of citizens and track down political activists.[108] In industrialised countries, the use of the technology by state authorities seems to be limited to prevention of terrorist crimes. However, developers of DPI technology were not willing to share any information concerning their clients (including state authorities) nor the specific applications of DPI. It is, thus, not possible to present a solid claim here.

Applications have been developed to allow for law enforcement authorities to automatically monitor Internet content and map (cor)relations. Pieces of content and Internet traffic can be combined with metadata and are subsequently categorised. For instance, systems can recognise whether some specific content concerns a person, a location, or an organisation. Subsequently, combining pieces of information can reveal potential threats, because a specific person is named in relation to a specific location several times, combined with a reference to a weapon or an attack. Pieces of content can be tagged and recorded by relevant authorities.[109]

Also in a commercial context, the use of DPI is limited, even though there are several purposes for which ISPs can use the technology. DPI can be used to "ensure network security,

[108] Fuchs, Christian, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", Privacy & Security Research Paper #1, PACT Project, Uppsala, 2012.
[109] See, for instance, the Dutch iColumbo project by the Dutch National Coordinator Terrorist Prevention and Security.

perform network management, and to achieve price discrimination, behavioural advertising or content filtering."[110] Similar to what is described in the previous paragraph, monitoring network performance can take place by recognising which type of applications are more likely to congest the network.

In 2012, it became known by the general public that the Dutch telecom provider KPN was using DPI as part of its network management. Some other telecom providers admitted the use of DPI as well. Public outrage resulted[111] and the public prosecutor started investigations concerning the use of the technology. It appeared, however, that there was no integral storage of the packets or contents. This meant that the way the technology was implemented by the ISPs, did not infringe privacy as the actual content was not shown to anyone. Therefore, the public prosecutor stated that there was no possibility to start a criminal procedure, since there was no criminal act.[112]

When being interviewed, vendors of DPI technology emphasise that the technology is neutral. They argue that the exact meaning the technology in practice depends on the way it is applied and the purposes for which application is taking place. For instance, DPI has been used in firewalls and virus scanners for years without any problems. Applying the same technology for purposes of network or bandwidth management has raised concerns amongst citizens, however, since they assumed that the exact contents of their web traffic were monitored and analysed. While no evidence was found in practice that this monitoring takes place, it should also be noted, as stated before, that the technology may, in fact, not be neutral as DPI is designed to look into the payload of Internet traffic. To overcome any risks to privacy, additional measures need to be taken. Examples of these additional measures include the installation of storage terms or the aggregation of information at group level.

Also supervisory authorities and public rights associations indicate that the technology can be used in a neutral manner, but can most clearly be indicated as a security technology due to its application in practice. The application of DPI to detect malware or spyware aims to protect privacy of the Internet user and may, thus, have the function of a privacy technology in this setting. However, also in this case, the direct application concerns differentiation and detection of content in order to keep the computer of the Internet user secure. This means that it is in fact more appropriate to regard DPI as a security technology, which may also protect privacy. According to public rights associations, this is, however, ambiguous as this seems to suggest that privacy can only be protected when it is first breached.

Some academics and policy makers stress that the purpose of DPI is to look into the contents of Internet traffic. Hence, they see a potential for the technology to be privacy intrusive. Overall, amongst interviewees from different groups of actors involved, the threat to privacy is more prevalent than the benefits for privacy resulting from the detection of malware. The way in which DPI is applied determines the (perceived?) degree of intrusiveness most. Every DPI technology allows for reading Internet traffic and it is thereby naturally a risk to privacy. However, as DPI can also be implemented in such a way that it does not harm privacy, the

[110] Sluijs, Jasper P., *Network Neutrality and European Law*, Wolf Legal Publishers, Nijmegen, 2012. http://arno.uvt.nl/show.cgi?fid=128367.
[111] de Haes, Andreas Udo, "KPN luistert abonnees af met Deep Packet Inspection", *Webwereld*, 12 May 2011. http://webwereld.nl/nieuws/106656/kpn-luistert-abonnees-af-met-deep-packet-inspection.html.
[112] Vermeer, Reinier, "'DPI-gebruik van KPN geen strafbaar feit'"ibid., 3 August 2011. http://webwereld.nl/nieuws/107507/-dpi-gebruik-van-kpn-geen-strafbaar-feit--.html.

factor determining the risk for privacy most is what the user of the technology is planning to do with it.

In response to the use of Internet surveillance technologies in general, an important initiative was taken to protect the privacy of users in the 'Tor project'.[113] Tor (the onion routing) is a network that reroutes Internet traffic and therewith allows for shielding information about the sender and receiver of content over the web. Traffic can be rerouted over several network nodes within the network. As a result, surveillance based on traffic analysis is no longer possible. In relation to DPI this would mean that even inspecting packets at the header level is made difficult by Tor, due to the obfuscation of senders and receivers of packages. Tor is, thus, presented as a privacy technology which counterparts traffic analysis surveillance technologies. The Tor project indicates that this facility is highly necessary for, for instance, journalists who want to communicate with their secret sources, whistle blowers, dissidents, but also ordinary users who do not want to be tracked and monitored. In light of the technical possibilities offered by DPI and the different functions that can be integrated in the technology, keeping an eye on the function of the Internet as an open information source is deemed important as well. DPI can become a disruptive technology when applied on a large scale and has the potential of changing the basic nature of the Internet as an open infrastructure.[114]

10.6 CONCLUSION: MUTUAL SHAPING OF THE TECHNOLOGY

A first occurrence of shaping took place when the technology was developed. DPI was designed to monitor Internet traffic and increase security. It was thus shaped as a technology that may be used for increasing security, at the price of an increased risk to privacy. Firstly, security may be increased by allowing for detection of malicious or harmful communications, for example between terrorists. Secondly, security may be increased by detecting network problems, malware or spyware. In this second application, it may also function as a privacy technology when malicious software aimed to breach the privacy of Internet users is detected. The shaping of technology took place by developers of DPI wanting to create technology that can look into the payload of Internet traffic. While in offline communications (such as letters) it is much more cumbersome to have to open all envelopes rather than only reading the addresses, with DPI reading the content of a packet is only a step away from reading the address.

A second occurrence of shaping is the application of the technology. The most common practice of the application of DPI in the Netherlands, for example, is its use for network management. In this case, users of the technology may ignore or not store any information that can be traced back to individuals. Thereby, data protection can be guaranteed. However, DPI is known to be used for different applications, such as the US government tracing terrorists by monitoring Internet activity at network hubs, or Internet censorship in Turkey. In the first case, the attacks on the World Trade Center have been highly influential in shaping the application of the technology.

[113] TOR Project, "Tor Project: Anonymity Online", 2013. https://www.torproject.org/index.html.en. (Accessed: 1 March 2013)
[114] Bendrath, R., "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection", Paper presented at: International Studies Annual Convention, New York City, 2009.

As a result of the attention that has been drawn by the use of DPI by ISP's, a countermovement or form of 'countershaping' is currently taking place. Firstly, this is taking place by digital rights groups developing a framework of principles of use that governments should adhere to. They argue that states are obliged to inform citizens when they were subjected to online surveillance in order to act in conformity with the requirements derived from human rights protection. They do this because they observe a trend in the EU's security programmes towards allowing states more interference with fundamental rights for security reasons. They consider the development and use of surveillance technologies, in particular DPI, as a striking example. Secondly, also legal action was undertaken, for example in the Netherlands. Specific applications of DPI are prohibited because of the legal requirement of net neutrality. Using DPI to differentiate between types of content or traffic is not allowed, because this infringes upon net neutrality.

11 BIOMETRIC ACCESS CONTROL

Govert Valkenburg

11.1 INTRODUCTION

This case study concerns biometric technologies for access control. By measuring or recording properties of the human body, these technologies aim to confirm in some way a person's identity, or rather a *particular* identity of the person. The verification of an identity informs the process of granting or denying a person access to a particular site, or to particular services, etc. At face value, biometric technologies seem to simply enable or promote access control. However, as this case study will show, they also enact multiple and particular ideas of identity, security and privacy. A range of enacted realities are hidden behind the generic purposes for which biometric solutions are presented.

Biometric access control technologies potentially hide a great deal of socially relevant issues. Biometric data are principally *personal data* as they are uniquely connected to one single person.[115] Thus, these technologies introduce many potential problems: identity theft and other fraud, exclusion of people whose biometric properties fall outside the range that was presumed when designing the system, or the unanticipated connection of databases by means of unique biometric keys. Therefore, numerous methods are developed by vendors, scientists and operators to handle biometric data carefully: revocability of biometric templates, purpose binding that allows a biometric template to be used for only one specific purpose, and encryption that renders data useless when stolen.

One of the primary aims of the PRISMS project is to analyse privacy and security beyond the idea that they would be irreconcilable or mutually exclusive. In such an idea, increasing security would lead to deterioration of privacy, and vice versa.[116] However, the field of biometrics shows in fact a range of forms of identity, security and privacy that emerge in different practices. If privacy, security and identity are complex, heterogeneous and multiple concepts, then it is at least highly unlikely for their interrelation to be one of simple mutual exclusion. This case study will articulate, based on empirical research, the range of issues and problems that fall under the names of security and privacy. It then becomes clear that the relation between privacy and security is not actually a trade-off, but much more intricate than that. In fact, many measures that are taken to improve privacy, are also beneficial for security, and vice versa.

11.2 METHODOLOGICAL ACCOUNT

This case study is empirically underpinned by eight interviews (some of them by telephone, but mostly in person) with vendors, policy makers, operators and representatives from interest groups, as well as a review of academic literature, press coverage, corporate communication and websites, material from watchdog and other societal organizations, and so on. Selected material comes from various technologies and situations, ranging from relatively simple

[115] Koorn, Ronald, Herman van Gils, Joris ter Hart et al., "Privacy-Enhancing Technologies - White Paper for Decision-Makers", Ministry of the Interior and Kingdom Relations, The Hague, 2004. http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

[116] See PRISMS Deliverable 1.1

access control systems in a sports facility, to configurations with complex informational and security needs. Thereby, the analysis earns more generalizing power than if the empirical base had been confined strictly to one site of operation. From this base, the case study composes a 'snapshot' of the practice of biometric access systems, which should make clear how privacy and security are 'done' or enacted in practice.

11.3 CURRENT TECHNOLOGIES AND CHALLENGES

The term 'biometric technologies' refers to a collection of identification technologies making use of properties of the human body that can be measured and that are in many cases unique to the individual. The uniqueness of certain body properties is used to determine the likelihood that two recordings originate from the same person. The state of the art in biometric technologies comprises a wide range of techniques, such as fingerprint recording, iris scans and facial recognition. It varies between authors what they exactly count as biometrics. In the Dutch legal context, the term 'biometrics' explicitly refers to technologies that establish or check a person's identity.[117] Alternatively, the definition given in the position paper of the Netherlands Biometrics Forum[118] regards automation and information processing on sensor data as quintessential to biometrics. This would logically exclude visual comparison of photographs by human agents. In contrast, Cavoukian et al.[119] regard such manual comparison as 'the most common form of biometrics'.[120] In yet another perspective, EU guidelines specify that storage of data must be regarded as processing,[121] thus rendering the distinction of 'automatic processing' somewhat superfluous.

An important development is the emergence of a so-called 'second generation' of biometric technologies. In these new technologies, less unique biometric modalities such as gait, handwriting characteristics, voice and body weight are used, the inaccuracy of which is compensated for by using multiple biometric modes together. Also, the technologies are characterized by a 'retreat' from clearly identifiable interfaces into the background of ambient intelligence, and for example incorporation into consumer mobile devices.[122] This constructs convenience as the subjected user is bothered less with the issue of biometrics, but it also constructs further opacity and decreasing awareness among subjected users.

[117] Willemsen, Clemens, *Biometrics: how it works*, Progis; Ministry of Justice, The Hague, 2009.
[118] van Kleef, Frans, "Position paper: Betrouwbaar en veilig gebruik van biometrie", Nederlands Biometrie Forum, Tilburg, 2012. www.biometrieforum.nl.
[119] Cavoukian, Ann, M. Chibba and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment", *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61.
[120] The watershed is on the agent of comparison: human versus computer. The fact that today, access to photographs virtually always mediated by information technology, is itself irrelevant to this distinction.
[121] Directive 95/46/EC, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data", *Official Journal of the European Communities*, L 281, 23 November 1995, pp. 31-50. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[122] Finn, Rachel L., David Wright, Michael Friedewald et al., "Privacy, data protection and ethical issues in new and emerging technologies: Five case studies", Deliverable 2, PRESCIENT Project, 2011. http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf.. See also van der Ploeg, Irma "Security in the Danger Zone: Normative Issues of Next Generation Biometrics", in Emilio Mordini, and Dimitros Tzovaras (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, Dordrecht, 2012, pp. 287-303.. The point of mobile devices is mentioned by several interviewees.

Biometric technologies are typically used for two basic purposes: identification and verification.[123] Verification is the process of determining whether (or at least at which likelihood) two measurements derive from the same person. This is also referred to as "1:1 comparison". Identification, in contrast, is the process of determining which measurement from a large set is closest (or equal) to a particular reference measurement. This is also referred to as "1:n comparison". Both processes will generally be used to obtain certainty – or rather: provide strategies to *construct* certainty – regarding a person's identity. Of course, the difference between them will engender different ways in which the technologies are exactly used and arranged. In general, processes of identification are more prone to error than are processes of verification.[124]

Biometric technologies pose a number of challenges that need to be addressed in practice. For example, biometric data could in principle be stolen and used to counterfeit a person's identity ("spoofing"). In prevention of such identity theft, as well as in abatement of the intrinsic statistical uncertainty, configurations of biometric access technologies typically comprise various security measures, both technically and socially/procedurally. These measures include irreversible coding ("hashing") of biometric data, minimization of the data recorded of one person, and ensuring that unrelated processes are allocated to different systems with different system designs, such that they cannot be linked. Also the use of multiple biometric modes together ("multi-modality", e.g. fingerprints combined with the vein pattern in the finger skin) offers an additional (technical) solution to such problems, a solution that some interviewees find promising.[125]

Biometric technologies are also essentially loaded with margins of error and statistical uncertainty. The multimodality just mentioned offers some solace to specific errors. Also basic checks can be performed whether the biometric data originate from a live body part, rather than a dead one or a silicone reproduction. But even such "liveness detection" approaches have been reported to be spoofed.[126] Additionally, errors may result from the fact that one's biometric characteristics might actually change over time.[127] Finally, people might have body properties that fall outside the range considered as "normal". They will then fail to 'fit' into the biometric system, even if this exclusion itself is neither legitimate nor justifiable. These issues demonstrate that anomalies and unexpected system behaviour will occur, for which fall-back procedures and workarounds will have to be created.

[123] Cavoukian, Ann, M. Chibba and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment", *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61. Grijpink, J.H.A.M., "Checklist biometrische persoonsherkenning (NL-versie)", *Checklisten Informatiemanagement (update 34)*, SDU, Den Haag, 2009.

[124] Cavoukian, Ann, M. Chibba and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment", *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61.

[125] van Kleef, Frans, "Position paper: Betrouwbaar en veilig gebruik van biometrie", Nederlands Biometrie Forum, Tilburg, 2012. www.biometrieforum.nl.

[126] Boult, Terrance E., Walter J. Scheirer and Robert Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis", in T. Kanade, G. Medioni et al. (eds.), *IEEE Conference on Computer Vision and Pattern Recognition (CVPR '07)*, IEEE Computer Society, Minneapolis, Minn., 2007, pp. . Snijder, Max, "Het Biometrisch paspoort in Nederland: Crash of zachte landing", Webpublicatie Nr. 51, Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag, 2010. http://www.wrr.nl/fileadmin/nl/publicaties/PDF-webpublicaties/Het_biometrisch_paspoort_in_Nederland.pdf.

[127] Willemsen, Clemens, *Biometrics: how it works*, Progis; Ministry of Justice, The Hague, 2009.

11.4 BACKGROUND

The recognition that body properties differ between people in a measurable way has been used for identification and verification purposes for over hundred years: in 1892 the first criminal fingerprint identification was conducted.[128] This criminological perspective remained the dominant frame for a long time in discussions of biometrics. For example, much of the standardisation of biometric technologies in the 19th and 20th centuries was aimed at using the technologies in policing.[129] It is observed that this criminalizing frame and the underlying pursuit of control by the state still determine part of today's state-operated biometric technologies, e.g. in border control and welfare administration.[130] Also, it is argued that much of the use of biometrics in border control – whether deliberately or unintendedly – serves the construction of persons as falling outside the legal order.[131]

Since its earliest use, numerous developments have taken place in the field of biometric technologies. Shifts include, but are not limited to: from criminal to civil purposes, from the closed group of criminals to the open group of general citizens, from compulsory to voluntary enrolment, and from manual, analogue to digital, automated processing.[132] Importantly, the digitization of biometric comparison has enabled the comparison of large numbers of biometric samples, instead of having to compare samples manually one by one.

From the early days of biometrics, it has been subject to contestation whether fingerprints are fully unique or not, and whether it is possible for a human investigator to estimate with full certainty whether a latent fingerprint – i.e. a fingerprint that is for example left at a crime scene – belongs to a particular person. The prevailing opinion today is that, regardless of whether fingerprints are unique, their comparison is always human work, even if technologically mediated, and therefore ultimately inconclusive.[133] This also holds for other biometric modalities such as DNA, iris, retina or vein patterns, etc.

Given this history of contested and constructed 'biometric certainty', it is remarkable that still today, biometric technologies are often presented as the ultimate proof of an undisputable and unique identity.[134] In general, biometric technologies are presented as adding safety by

[128] German, Ed, "The history of finger prints", 2013. http://onin.com/fp/fphistory.html. (Accessed: 08 January 2013)

[129] Becker, Peter, "Networked technologies: new identification technologies at the turn of the century", in Efi Avdela, Shani D'Cruze et al. (eds.), *Problems of Crime and Violence in Europe, 1780-2000. Essays in Criminal Justice*, The Edwin Mellen Press, Lewiston, Queenston, Lampeter, 2010, pp. 119-152.

[130] Kruger, Erin, Shoshana Magnet and Joost Van Loon, "Biometric Revisions of the `Body' in Airports and US Welfare Reform", *Body & Society*, Vol. 14, No. 2, 2008, pp. 99-121. http://bod.sagepub.com/content/14/2/99.short.

[131] Bewley-Taylor, DavidR, "US concept wars, civil liberties and the technologies of fortification", *Crime, Law and Social Change*, Vol. 43, No. 1, 2005, pp. 81-111. http://dx.doi.org/10.1007/s10611-005-4054-z. van der Ploeg, Irma, and Isolde Sprenkels, "Migration and the Machine-Readable Body: Identification and Biometrics", in Huub Dijstelbloem, and Albert Meijer (eds.), *Migration and the new technological borders of Europe*, Palgrave Macmillan, London, 2011, pp. 68-104.

[132] Snijder, Max, "Het Biometrisch paspoort in Nederland: Crash of zachte landing", Webpublicatie Nr. 51, Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag, 2010. http://www.wrr.nl/fileadmin/nl/publicaties/PDF-webpublicaties/Het_biometrisch_paspoort_in_Nederland.pdf.

[133] Cole, Simon A., "More than zero: Accounting for error in latent fingerprint identification ", *The Journal of Criminal Law and Criminology*, Vol. 95, No. 3, 2005, pp. 985-1078. Cole, Simon A., "The 'Opinionization' of Fingerprint Evidence", *BioSocieties*, Vol. 3, No. 1, 2008, pp. 105-113.

[134] Ball, Kirstie, "Organization, Surveillance and the Body: Towards a Politics of Resistance", *Organization*, Vol. 12, No. 1, 2005, pp. 89-108. http://org.sagepub.com/content/12/1/89.abstract. Cavoukian, Ann, M. Chibba

increasing the likelihood that persons are actually the persons they claim to be. Even though experts agree that full certainty is impossible to attain in practice, the fiction of absolute certainty is prominent, and it is also through this pretention of certainty that biometric systems are justified in their use.

Currently, several broad developments can be observed in the field of biometrics. First, applications of biometric technologies are increasing in numbers, thus potentially increasing security as well as efficiency and convenience. For example, in ever more situations, a single fingerprint scan potentially displaces several minutes of administrative work, and the problem initially solved by the paperwork is now translated into a fingerprint scan with all its statistical boundary conditions. Second, developers and policy makers focus on improving the safety of the biometric data themselves. As will be shown onwards, biometric data is protected in numerous ways against theft, fraud, leakage and unjust exercise of power. Thus, effort is made to feed confidence and ensure that people are willing to enrol their biometrics. Third, effort is continuously dedicated to improving biometric technologies so as to better perform their envisioned primary task, namely providing certainty regarding somebody's identity, with ever smaller margins of error. Improvements are also sought in the development of three-dimensional measurements.[135] Thus, further certainty is constructed.

11.5 BIOMETRIC CONSTRUCTIONS

Biometric technologies are presented as an aid in confirming a person's identity. However, neither identity nor the process of biometric authentication are as unambiguous and straightforward as they may sound. On the one hand, numerous measures are taken to render our biometric properties in some sense irrelevant: they are processed in a way that nothing else can be done with it than the mere purpose for which they were obtained. On the other hand, the same biometric properties are of utmost relevance: they provide the ultimate touchstone of our identity, or even its token, and as such, they have important consequences.

In a similar sense, biometrics are ambiguous with respect to uniqueness. On the one hand, uniqueness is the essence of biometric access control: it proves that a specific person, and no other person, is present. This presumes that that persons' biometrics 'fit' into the system, that they remain stable over time, and that they can be made available to the system, presumptions that are at least questionable.[136] On the other hand, practices of biometric access control are always entrenched by false acceptances and false rejections, which are to be coped with by fall-back procedures. Also, even if people's biometric properties are analysed correctly, their identities are still only established with a degree of certainty, not absolute certainty. Ultimately, no biometric technology is able to make persons fully unique.

and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment", *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61.

[135] Willemsen, Clemens, *Biometrics: how it works*, Progis; Ministry of Justice, The Hague, 2009. This point was also mentioned by one of the interviewees.

[136] van der Ploeg, Irma, "Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications", in S. van der Hof, and M .M. Groothuis (eds.), *Innovating Government*, T. M. C. Asser, Den Haag, 2011, pp. 29-40.

11.5.1 Biometrics without consequences

11.5.1.1 "Biometrics are naturally void of consequences"

From a particular perspective, there is something utterly irrelevant about biometrics. That is to say: the information that biometric data contain, thus argue several interviewees, will generally not be found commercially interesting, or privacy-sensitive. Your fingerprint is just a fingerprint like any other. It may reveal that you have done a lot of handwork, but that's it. My iris scan only reveals that I have blue eyes, which correlates mostly with a white skin, but that's it. Biometrics do typically not reveal any diseases[137], nor other elements of one's identity such as street address or income. Needless to say, this absence of consequences only lasts as long as the context in which the biometrics are used does not put the biometrics to use in a way that constructs such relevance. Thus, the freedom of consequences is itself a contingent construction.

Nevertheless, this freedom of consequences is put forward in defence of some biometric access control systems. For example, the sports facility of one Dutch university uses finger print scanners as its primary token for access. It uses hash coding (to be discussed later) to encode the scanned finger prints irretrievably, and hence render it uninteresting for theft. On top of that, one interviewee from an operational position argues that people understand, maybe after some explanation, that even if a fingerprint were stolen, it would incur far less vulnerability to maleficent use than for example a lost paper note with one's name and phone number on it.

Regarding this freedom of consequences, or more specifically the 'absence of consequences in a particular context', things differ between different modes of biometrics. For example, as one interviewee explains, fingerprints have the characteristic that we 'drop' them on everything we touch. Contrastingly, the exact shape of our irises are never left in any place, let alone a crime scene, or it must be at least very coincidental that the eye is caught on a high-definition camera. With finger vein patterns and retina vein patterns, it is even less probable that they are taken without permission or without the person noticing it.

Additionally, even within one biometrical mode, the personal nature of the biometrics, their privacy-sensitivity and their relevance are subject to contestation. Literature and interviewees generally agree that biometric data are principally personal data. Indeed, the whole idea is that they are connected to one person and not to another. However, this is not to say that biometric data are always agreed upon to be privacy-sensitive. As several interviewees argue, a fingerprint is just a fingerprint, and it does not reveal anything about the person. Even the fact that we leave it on anything we touch, by which a complete trace over our lives could in theory be reconstructed, is placed in perspective by some: simply too many fingerprints are dropped to make sense of them. Yet the meaning of a fingerprint in a particular context depends on the socio-technical configuration: how it is sampled and at what accuracy, to which end it is used, and how it is further connected to other information.

An example of the contested consequences of fingerprints is reflected by an episode in German public affairs. A German group of hackers captured and reproduced a fingerprint of the German federal minister of the Interior, Wolfgang Schäuble. This was done in response to

[137] This is different with e.g., DNA sampling, but that is considered beyond the scope of this study, even though it can in a particular perspective be seen as a form of biometrics.

his proposal to add fingerprints to passports, so as to add an extra layer of security.[138] The minister declined the issue as being insignificant and indeed it seemed to have no further consequences.

Whereas the German minister upheld the position that the stolen fingerprint was meaningless and without any consequences, such indifference could not be maintained after a failed experiment with fingerprint-facilitated payments. A leading Dutch chain of super markets, Albert Heijn, terminated a pilot project in which fingerprints were used for identification and payment purposes.[139] The pilot clearly showed a security exploit, as one hacker proved to be able to use (and have payments made using) the account of someone else. Even though the fingerprint was 'stolen' from someone who co-operated in the hack and the hack was consequently argued to be unrepresentative for real life, it does cast quite some doubt on the claim that fingerprints are by themselves not so relevant. Such relevance ultimately depends on how the world at large is organized qua biometrics; not just on the arrangement of a single system. As several interviewees agree, much of the practical meaning of biometrics depends on how technologies and sociotechnical practices are arranged.

What we see here is a discursive construction of biometrics as being without consequences. Importantly, little technological intervention is involved, and fairly little technological translation is visible of considerations of privacy and security in the realm of biometrics. The following section shows a rather different picture.

11.5.1.2 "We try hard to eliminate biometrics' consequences"

While biometrics potentially hides many consequences, this is exactly what owners of biometric access control systems in most cases want to prevent. Even if biometric data themselves do not contain so much interesting information, it turns out that still quite some effort is being made to make sure that the potential of biometrics to be uniquely linked to other sets of data, or serve as a key or index that facilitates the connection between different sets of data, is not realized. This potential for 'profiling' casts suspicion on biometrics. This suspicion is counteracted, both through sociotechnical arrangements and through the deployment of vocabularies of trust, confidentiality, and a general take on biometric information as *irrelevant*.

Hashing is the most widely-used mechanism through which consequences are eliminated. Hashing usually refers to an operation of transforming information in an irreversible way. From the hashed data, the original information (regardless whether it is an iris scan, finger prints or any other modality) cannot be retrieved. It can only be verified against biometric information that has undergone the same process of hashing. Thus, a hash from a fingerprint recorded at an access gate can be compared with a hash that has been enrolled from a trusted person at an earlier point, without making a comparison between the fingerprints themselves – and without the need to keep any record of the original fingerprints. This form of encoding provides the baseline above which current biometric systems typically stay. However, even

[138] Kleinz, Torsten, *CCC publiziert die Fingerabdrücke von Wolfgang Schäuble* 2008. http://www.heise.de/security/meldung/CCC-publiziert-die-Fingerabdruecke-von-Wolfgang-Schaeuble-Update-193732.html. Zetter, Kim, "Hackers Publish German Minister's Fingerprint", *Wired*, 31 March 2008. http://www.wired.com/threatlevel/2008/03/hackers-publish/.

[139] Haes, Andreas Udo de, "Albert Heijn zet betalen met vingerafdruk in de koelkast", *Webwereld*, 17 March 2009. http://webwereld.nl/nieuws/56479/albert-heijn-zet-betalen-met-vingerafdruk-in-de-koelkast.html.

though it is the kind of golden standard, two problems connect to it. First, researchers have argued that methods of irreversible coding are not always as irreversible as their makers want us to believe.[140] Second, as one interviewee explains, comparing transformations of fingerprints is less accurate than comparing untransformed fingerprints.

More sophisticated constructions of eliminated consequences in biometric technologies include various forms of biometric encryption. For example, some forms of encryption allow a biometric template to be revoked, such that it becomes worthless if it is lost, leaked or stolen. Alternatively, key and biometrics could be interchanged: instead of scrambling biometric data using a secret key, a secret key could be scrambled using biometric data. Thus, there is no need to store biometric data. It is only used at several points – chiefly at enrolment and during verification at the access gate – to derive some code from it, which is then used to access and verify the key.[141] Yet another alternative, biometric templates can be encrypted such that they are only usable for one specific purpose.[142] In some cases, this 'purpose binding'[143] consists of including into the encoded template itself some information about the purpose for which the template was created (and hence where it has been leaked, once it is found in an improper context).

These transformations of biometric information into arguably secure forms of data depend on techniques, which always have specific consequences. For example, revocability in biometrics first depends on developing encodings that can produce more than one transformation, which in turn depends on some form of helper data to indicate which particular transformation should be made for either enrolment or verification. Revoking the biometric sample thus requires either supplying new helper data, or even the need to re-enrol all samples if the same helper data are used for all samples. ('Helper data' is to be understood in a broad meaning here, and 'new helper data' may de facto consist of selecting whole new transformations.) Similarly, purpose binding depends on encryptions that are themselves vulnerable as any other encryption.

The pursuit of irrelevance need not take such a technical shape. In different vein, the irrelevance of biometric information can be constructed through organizational arrangements. This could for example consist of articulating clearly how the information is processed, and especially what is *not* done with it and how it is *not* distributed. In a general sense, this entails segmentation – i.e. restricting the use and distribution of information to a well-specified context – and role separation – i.e. an articulation of the purposes for which an office needs a particular piece of information. For example, as one interviewee explains, an envisioned biometrics-based trusted traveller programme at Amsterdam Schiphol Airport creates trust through exactly this mechanism: at each operational point, the stored data are minimized, and only those pieces of information are shared between organizational segments that are absolutely essential. Remarkably, this minimization of data is *facilitated by* biometrics, which offers a reliable primary key through which relevant data can be retrieved from segmented data sources.

[140] Jain, Anil K., Arun Ross and Umut Uludag, "Biometric template security: Challenges and Solutions", Paper presented at: Proceedings of the 13th European Signal Processing Conference (EUSIPCO), Antalya, Turkey, 2005.

[141] Cavoukian, Ann, M. Chibba and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment", *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61.

[142] Ibd.

[143] van Kleef, Frans, "Position paper: Betrouwbaar en veilig gebruik van biometrie", Nederlands Biometrie Forum, Tilburg, 2012. www.biometrieforum.nl.

An alternative approach arranging data storage in a trustable way, in line with the principles of *privacy by design*,[144] is the strategy of decentralization of storage. For example, in the Rotterdam harbour area, a biometric authentication system has been successfully in use for over ten years. The system enjoys great support among users, primarily owing to the fact that biometric data, in this case a hand-geometry scan, are stored on a smart card, not in a central database. The data are encrypted by an algorithm that according to one interviewee is the most secure one currently available on the market. Moreover, in case a smart card is lost, it will be blacklisted and no longer be accepted at access gates. Also, its content will remain unusable because of the thorough encryption. Additionally, trust is created through the fact that no record is kept of the whereabouts of a card holder. Finally, an ISO-9001 certification and the fact that the organization is not profit-oriented are supposed to help positioning the organization as a trusted party. Thus, even if biometrics feeds the suspicion of 'traceability' and potentially offers a boon to e.g., criminal investigations, this system is deliberately 'un-geared' to support this.

Thus, considerations of privacy are translated in to chiefly technical solutions, which in turn reflect particular versions of those ideas. In these situations, ideas of privacy as particular 'impossibilities' are inscribed.

11.5.1.3 "Even if biometrics has some consequences, you should still want it!"

Even if biometrics are indeed embedded in a practice that eliminates some important potential consequences of the use of biometrics, this elimination is still always bound to context, and relative to existing alternatives. The challenges of dealing with particular consequences of biometrics are translated into different solutions in different practices. In the case of the access system for truck drivers in the Rotterdam harbour area, the alternative consists of going through up to 45 minutes of administrative paper work. Accepting the biometric alternative and reducing this processing time to less than 6 minutes means vastly increasing convenience as well as efficiency and turnover. This alternative is made less burdensome on purpose in order to place pressure on people to accept biometrics that also responds to the increased need to process information in the cargo transport sector over the past decades. Even though this is not a 'natural necessity', it is at least a 'historical contingency', and compelling at that. While the biometric technologies were not forced onto truck drivers in a strict sense, their *comparative* attractiveness must be seen as a further momentum in getting the biometrics accepted as irrelevant.

Remarkably, an interviewee closely connected to the harbour access system also argues that part of the acceptance of the system had been implicitly created before the introduction of biometric technologies. Some decades ago, a truck driver would just enter a compound and leave with the container he claimed he was to take. Ever since, freight documentation has been added and extended, identification and legitimation has been introduced, and track records of cargo operations have been installed. In a sense, it has become fully normal that each operation is logged and checked. As this administration in general had long been accepted, it proved to be only a small step towards facilitating this identification by biometric means, certainly if it saves so much time.

[144] Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner of Ontario, Toronto, 2011. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

The same kind of comparative convenience is elucidated by one interviewee involved in the use of fingerprints for the identification and verification of asylum seekers in the Netherlands. Along similar lines as explained above, he argues that the biometrics themselves are not sensitive personal data. Additionally, he positions the Dutch system as attractive in comparison to alternatives: if a system without biometrics were designed, it would be necessitated to record a host of intimate details about asylum seekers. He argues that this is the only way to achieve deduplication, i.e. the detection and removal of multiple entries belonging to the same physical person. Alternatively, this task is now largely fulfilled by comparing fingerprints.

11.5.2 Constructed securities

As was stated in the beginning, biometric technologies are virtually never capable of offering 100% certainty. There is always some likelihood that a person is incorrectly assessed. In case of a *false rejection*, a system concludes a person is not the person they claim to be, whereas in fact they are. In case of a *false acceptance*, the opposite happens: a system concludes that a person is the person they claim to be, whereas in fact they are not. And finally, there is the *doppelganger* problem: even if a person makes no explicit claim about their identity – but for example only shows a fingerprint which on its own should suffice to acquire access – it may still happen that the system concludes from the biometrics that person A is granted access, whereas in fact person B walks in. These are natural consequences of biometric processes being statistical in nature, instead of fully deterministic.

The problems of false acceptance and false rejection are not symmetrical. In case a biometric system is arranged to keep ‘good’ people in and ‘bad’ people out, a false rejection will make the falsely rejected person protest and trigger a fall-back procedure. A false acceptance on the contrary will not raise any alert. (This asymmetry is of course reversed if the objective of the system is to identify ‘bad’ people, for example when facial recognition is used to enforce restraining orders in shopping areas.) This false acceptance is a peculiar example of when biometrics becomes irrelevant. They become irrelevant in a way that was not desired by system designers.

Which fall-back procedures are available strongly depends on the further sociotechnical arrangements surrounding the actual use case. For example, if biometric data are irreversibly coded, no original data are available for manual inspection. It is exactly for this reason that the immigration service and the operational service of the Ministry of Justice use unencrypted storage. Ultimately, a human fingerprint examiner must be able to give a conclusive assessment. This additionally makes the process transparent and checkable, ultimately by the legal court. The fact that unencrypted storage is generally found unacceptable in the context of biometric data is compensated for by the fact that the IT systems of the Ministry of Justice are subject to the same strict security regimes that also control the IT systems of other police, defence and intelligence services. Additionally, even though fingerprints are not hash-coded, they are pseudonimized in the sense that they are connected to a criminal or immigration file number, not to a personal record, though of course this personal record is only one step away.

Constructions in this perspective are delicate. On the one hand, the statistical uncertainties remain. On the other hand, security translated into particular definitions of identification problems, seem to ask for a certainty that is not possible to give along technical lines. This then flows over into the social domain, where such security is more discursively constructed.

11.5.3 (Non)biometric identities

Biometrics are associated with, and connected to, identities. These identities include identity in a cultural sense as the person I am, identity in an administrative sense as the data that tell where I live and how much I make, and many other conceptions of 'who I am' that may be relevant at some point. In other words, identities are plural, not singular. Practices of biometric technologies always contain a *particular* construction of identity.[145] The request of 'show me your fingerprint' always displaces some particular guise of the question 'tell me who you are'. Consequently, each different arrangement of a biometrically secured identity in a specific practice entails different opportunities, problems, and challenges. They also entail particular take on how this identity operates as a representation of the private individual in the public context.[146]

In the case of the Rotterdam harbour access card, the biometrically secured identity largely coincides with the set of safety certificates the driver holds: numerous safety trainings are required for dealing with specific goods or conducting specific operations, and certificates of these trainings are stored on the card. Additionally, the information contained on the card includes basic identity data and data about the employer of the truck driver. Remarkably, the card can also contain a medical statement that exempts the card holder from being subject to biometric technologies (e.g. rheumatic hands, which are problematic in hand geometry scanning systems). Finally, the card of course contains an encrypted template of the driver's hand print, by which the driver's formal identity can be ascertained. The question of 'tell me who you are' in this case translates into the particular question of 'tell me your name and show me your safety certificates'. Remarkably, as an interviewee indicates, a person's criminal record is thought to be irrelevant for the issuance of the card, and hence for this particular understanding of security. This altogether shows that the load of paperwork that predated the biometric verification system is not just a plain form of bureaucracy, but a bureaucracy for the purpose of a very specific understanding of safety and security – though it might still be regarded bureaucracy.

An entirely different identity is constructed in the biometrics-facilitated trusted traveller programmes. There the identity largely coincides with the traditional boarding pass, which in turn is a token for a whole array of processes including screening and vetting, financial transactions, consenting to exchange of very specific information between countries, etc. Again a lot of paperwork (or its digital equivalent) is displaced by a single biometric identification. However, contrary to the harbour access system, all data are stored centrally (if only because a 'tokenless trajectory' also means that no token is available on which the data could be stored locally). While these data are segmented and strictly separated in such a way that only very specific parts of it are available at very specific places, these collections of data together construct, literally, the identity of the 'trusted traveller'.

[145] See also e.g. van der Ploeg, Irma, and Isolde Sprenkels, "Migration and the Machine-Readable Body: Identification and Biometrics", in Huub Dijstelbloem, and Albert Meijer (eds.), *Migration and the new technological borders of Europe*, Palgrave Macmillan, London, 2011, pp. 68-104.

[146] See e.g. van der Ploeg, Irma "Machine-Readable Bodies, Biometrics, Informatization and Surveillance", in Emilio Mordini, and M. Green (eds.), *Identity, Security and Democracy*, IOS Press, Amsterdam, 2009, pp. 85-94.

If only one thing, these two examples show that the identity that is constructed through a biometric identification technology is far from neutral. Not only does a technology offer a very specific answer to the question who somebody is, it also, in constructing this answer, take on board a range of presumptions and transformations that work in a discriminating or otherwise socially or politically relevant way.

11.5.4 Constructions of privacy

The ambiguity between biometrics with and without consequences becomes even more intricate in cases where biometrics are explicitly harnessed in service of privacy. The terms *privacy by design* and *privacy enhancing technologies* in general refer to design philosophies that aim at incorporating privacy and security from the early design phases on, instead of first designing a technology and then starting to think about how it can be made secure and privacy-respecting. This becomes even more delicate if the object that needs protection, namely the biometric data, is harnessed itself to serve privacy.

Returning to the Rotterdam harbour authentication infrastructure, it is clear that the biometric authentication replaces a lot of paperwork. In addition, it prevents these data from being read when the cardholder is not present. Also, it ensures that the data can only be read in locations where use of the data is actually appropriate. The hand print forms the key to the data, and the hand print itself cannot be leaked because of the encryption. This thus facilitates decentralization.

A similar kind of 'concealment through biometrics' is visible in biometric *trusted traveller programmes* at international airports, be it in a rather different configuration. On the one hand such programmes require the disclosure of a lot of sensitive personal information during the enrolment process. On the other hand, they eliminate the need to disclose this information to any customs official. In this case, biometrics are used as a primary key of identification at various phases in the flow of a passenger through the airport. Thus, a biometric technology facilitates role separation and data segmentation, which are particular constructions of privacy. This construction of privacy is obtained by accepting that another form, namely keeping biometric data secret, is taken to count less.

As is argued by one interviewee, the success of such trusted traveller programmes indicates that people apparently have little difficulty trusting the corporate players operating such programmes. He estimates that commercial players that collect biometric data for very specific purposes are more likely to be trusted than governmental bodies that for example collect fingerprints for less clear purposes, as was done in an unfortunate way by, e.g. the Dutch government [147] – if only because the former have a strong commercial interest in protecting their clients' biometric data.

11.5.5 Constructions of convenience

Clearly, privacy and security are not the only values that are constructed in practices of biometric access control. Convenience is perhaps just as important. In the Rotterdam port area

[147] This has been argued to be highly disproportionate and a violation of fundamental human rights Mom, Peter, "'Paspoortbiometrie is mensenrechtenschending'", *Binnenlands Bestuur*, 29 October 2010. http://www.binnenlandsbestuur.nl/digitaal/nieuws/paspoortbiometrie-is-mensenrechtenschending.381106.lynkx.. Two interviewees refer to this same episode of storing fingerprints as something that defied a lot of public trust.

case, the biometric technology displaces a considerable effort of paperwork. Also in the case of the trusted traveller program, it provides a considerably faster alternative to lining up for passport checks.

In this respect, not all biometric modalities are equal. With iris scans, one interviewee explains that it requires some practicing before the user handles the system well. As another interviewee involved in the trusted traveller program explains, it is interesting to see how a community emerges of users of the program, who amongst themselves help others to master the system properly. Hand geometry scans in contrast are much more robust to disturbances, and people turn out to require little or no training to operate it.

11.6 CONCLUSION

Through biometrics, many different problems can, at least ideally, be solved. Biometrics can be used to reveal private data when needed, for example in the criminal system. It can be used to conceal private data, for example in trusted traveller programs. It can be used to speed up processes, which is one of the aims in the Rotterdam harbour case.

Privacy and security are *translated* into different sociotechnical configurations in each case. Privacy might consist of hash coding or any other informational operation that prevents potential consequences of the use of biometric data from realization. Alternatively, it might consist of using the biometric data as a key to lock and unlock (potentially sensitive) personal data. For security, the same holds, *mutatis mutandis*. With each of these translations, different routines of use emerge, and different *inscriptions* follow.

Something that occurs in this case study and not in most others is the appearance of particular translations of *identity* as a corollary to the constructions of privacy and security. Identity might be translated into a pack of safety certificates, or just a as subscription at the gym.

REFERENCES

Akrich, Madeleine, "The description of technical objects", in Wiebe Bijker, and John Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, Mass, 1992, pp. 205-224.

Akrich, Madeleine, and Bruno Latour, "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies", in W. E. Bijker, and J. Law (eds.), *Shaping Technology, Building Society: Studies in Sociotechnical Change*, MIT Press, Cambridge, MA, 1992, pp. 259-264.

Allan, Sharon, Eric Trapp and Anthony David Scott, "Critical infrastructure protection for the smart grid", Accenture, 2010. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Cyber_Security_Smart_Grid.pdf.

Armstrong, J., J. Czeck, M. Franklin and D. Plecas, "Automated License Plate Recognition (ALPR), How long should the data retention period be?", 2010.

Bakker, Jasper, "Malware op usb-sleutels besmet energiecentrales VS", *Webwereld*, 04 February 2013. http://webwereld.nl/nieuws/113052/malware-op-usb-sleutels-besmet-energiecentrales-vs.html.

Ball, Kirstie, "Organization, Surveillance and the Body: Towards a Politics of Resistance", *Organization*, Vol. 12, No. 1, 2005, pp. 89-108. http://org.sagepub.com/content/12/1/89.abstract.

Becker, Peter, "Networked technologies: new identification technologies at the turn of the century", in Efi Avdela, Shani D'Cruze et al. (eds.), *Problems of Crime and Violence in Europe, 1780-2000. Essays in Criminal Justice*, The Edwin Mellen Press, Lewiston, Queenston, Lampeter, 2010, pp. 119-152.

Bendrath, R., "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection", Paper presented at: International Studies Annual Convention, New York City, 2009.

Bewley-Taylor, DavidR, "US concept wars, civil liberties and the technologies of fortification", *Crime, Law and Social Change*, Vol. 43, No. 1, 2005, pp. 81-111. http://dx.doi.org/10.1007/s10611-005-4054-z.

Bordley, William E., "Letter to John Verdi, EPIC concerning Freedom of Information / Privacy Act Request no. 2009USMS13697, subject: Images", U.S. Department of Justice, United States Marshals Service, Alexandria, VA, 2010. http://epic.org/privacy/body_scanners/Disclosure_letter_Aug_2_2010.pdf.

Bosker, Bianca, "Body Scan Images From Security Checkpoints Were Saved By Feds", 2010. http://www.huffingtonpost.com/2010/08/04/body-scan-images-from-sec_n_670170.html. (Accessed: 2012.11.02)

Boult, Terrance E., Walter J. Scheirer and Robert Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis", in T. Kanade, G. Medioni et al. (eds.), *IEEE Conference on Computer Vision and Pattern Recognition (CVPR '07)*, IEEE Computer Society, Minneapolis, Minn., 2007, pp.

Brown, Ian, and Douwe Korff, "Striking the Right Balance: Respecting the Privacy of Individuals and Protecting the Public from Crime.", Information Commissioner's Office, Wilmslow, 2004.

Burgess, J. Peter, "Social values and material threat: the European Programme for Critical Infrastructure Protection", *International Journal of Critical Infrastructures*, Vol. 3, No. 3/4, 2007, pp. 471-487.

Callon, Michel, Pierre Lascoumes and Yannick Barthe, *Acting in an uncertain world: an essay on technical democracy*, The MIT Press, Cambridge MA, 2009.

Capgemini, "Smart Metering: The holy grail of demandside energy management?", 2013. http://www.in.capgemini.com/m/in/tl/tl_Smart_Metering__The_holy_grail_of_demand-side_energy_management_.pdf. (Accessed: 15 March 2013)

Carnis, Laurent, "A Public Policy in Evolution:Speed Enforcement in France (2000-2010)", Paper presented at: Australasian Road Safety Research, Policing and Education Conference, Perth, Western Australia, 2011. http://arsrpe.acrs.org.au/pdf/A%20Public%20Policy%20in%20EvolutionSpeed%20Enforcement%20in%20France%20%282000-2010%29.pdf

Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner of Ontario, Toronto, 2011. http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

Cavoukian, Ann, and Dix Alexander, *Smart Meters in Europe: Privacy by Design at its Best*, Information and Privacy Commissioner, Ontario, Canada, 2012.

Cavoukian, Ann, M. Chibba and A. Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment", *Review of Policy Research*, Vol. 29, No. 1, 2012, pp. 37-61.

Cisco, "Securing the Smart Grid", White paper, Cisco Systems Inc, San Jose, CA, 2009. http://www.cisco.com/web/strategy/docs/energy/SmartGridSecurity_wp.pdf.

Ciută, Felix, "Conceptual Notes on Energy Security: Total or Banal Security?", *Security Dialogue*, Vol. 41, No. 2, 2010, pp. 123-144. http://sdi.sagepub.com/content/41/2/123.abstract.

Clarke, Roger, "The Covert Implementation of Mass Vehicle Surveillance in Australia", Paper presented at: Fourth Workshop on the Social Implications of National Security: Covert Policing, 7 April 2009, Canberra, 2009. http://www.rogerclarke.com/DV/ANPR-Surv.html

Clastres, Cédric, "Smart grids: Another step towards competition, energy security and climate change objectives", *Energy Policy*, Vol. 39, No. 9, 2011, pp. 5399-5408.

Cohen, I. M., D. Plecas and A.V. McCormick, "A report on the utility of the automatied license plate recognition system in British Columbia", School of Criminology and Criminal Justice, Center for Criminal Justice Research, University of the Fraser Valley, Abbotsford, Canada, 2007.

Cole, Simon A., "More than zero: Accounting for error in latent fingerprint identification ", *The Journal of Criminal Law and Criminology*, Vol. 95, No. 3, 2005, pp. 985-1078.

Cole, Simon A., "The 'Opinionization' of Fingerprint Evidence", *BioSocieties*, Vol. 3, No. 1, 2008, pp. 105-113.

de Haes, Andreas Udo, "KPN luistert abonnees af met Deep Packet Inspection", *Webwereld*, 12 May 2011. http://webwereld.nl/nieuws/106656/kpn-luistert-abonnees-af-met-deep-packet-inspection.html.

Deisman, Wade, Patrick Derby, Aaron Doyle et al., *A Report on Camera Surveillance in Canada - Part One*, Surveillance Camera Awareness Network (SCAN), The Surveillance Project, Queen's University, Kingston, 2009. http://www.sscqueens.org/sites/default/files/SCAN_Report_Phase1_Final_Jan_30_2009.pdf.

Directive 95/46/EC, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data", *Official Journal of the European Communities*, L 281, 23 November 1995, pp. 31-50. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Directive 2006/32/EC, "Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing

Council Directive 93/76/EEC", *Official Journal of the European Union*, L 114, pp. 64-85. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:114:0064:0064:en:pdf.

Dutch Police, "Inzet ANPR in Wassenaar succesvol", 2011. http://www.politie.nl/mobile/nieuws/2012/oktober/28/06-inzet-anp-in-wassenaar-succesvol.html. (Accessed: 25 March 2013)

EurActiv, "European renewable power grid rocked by cyber-attack", Brussels, 2012. http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541. (Accessed: 15. December 2012)

European Commission, "Critical Infrastructure Protection in the fight against terrorism", COM (2004) 702 final, Brussels, 2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF.

European Commission, "On the use of security scanners at EU airports", European Commission, Brussels, 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0311:FIN:EN:PDF.

European Commission, "Commission Implementing Regulation (EU) No 1147/2011 of 11 November 2011, amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports", *Official Journal of the European Union*, L294, 12 November 2011, pp. 7-11.

European Commission, "Energy Infrastructure: Critical Infrastructure Protection", 2013. http://ec.europa.eu/energy/infrastructure/critical_en.htm. (Accessed: 18 March 2013)

European Smart Metering Industry Group, "Position Paper on Smart Metering in the energy efficiency directive (COM 2011/370)", 2012. http://www.esmig.eu/press/filestor/eed_pp. (Accessed: 12 March 2013)

Finn, Rachel L., David Wright, Michael Friedewald et al., "Privacy, data protection and ethical issues in new and emerging technologies: Five case studies", Deliverable 2, PRESCIENT Project, 2011. http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf.

Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.

Flight, Sander, and Paul van Egmond, "Hits en hints: De mogelijke meerwaarde van ANPR voor de opsporing", DSP Groep, Amsterdam, 2011. http://wodc.nl/images/volledige-tekst_tcm44-418513.pdf.

Foster, Pete, "Smart Meter Rollout in Europe - More Talk than Action", 2012. http://www.thegreenitreview.com/2012/03/smart-meter-rollout-in-europe-more-talk.html. (Accessed: 19 March 2013)

Fraunhofer ISI, "The project Intelliekon presents first results on saving electricity via smart metering: Timely information enables up to 3.7 per cent reduction in consumption", 2011. http://www.isi.fraunhofer.de/isi-en/service/presseinfos/2011/pri11-13.php?WSESSIONID=50b6ba2a8ec56aa4fda421890f4e4b5f (Accessed: 18 March 2013)

Friedewald, Michael, David Wright, Kush Wadhwa et al., "Central Concepts and Implementation Plan", PRISMS Deliverable 1.1, 2012.

Fuchs, Christian, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", Privacy & Security Research Paper #1, PACT Project, Uppsala, 2012.

German, Ed, "The history of finger prints", 2013. http://onin.com/fp/fphistory.html. (Accessed: 08 January 2013)

Giordano, Vincenzo, Flavia Gangale, Gianluca Fulli et al., "Smart Grid projects in Europe: lessons learned and current developments", EUR 24856 EN, Publications Office of the

European Union, Luxembourg, 2011. http://ses.jrc.ec.europa.eu/sites/ses/files/documents/smart_grid_projects_in_europe_lessons_learned_and_current_developments.pdf.

Gonzalez Fuster, Gloria, and Rocco Bellanova, "Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices", *International Political Sociology*, Vol. 7, 2013, p. Forthcoming.

Gorman, Siobhan, "Electricity Grid in U.S. Penetrated By Spies", *The Wall Street Journal*, 08 April 2009. http://online.wsj.com/article/SB123914805204099085.html.

Government of the Netherlands, "Privacy", Dutch Government, The Hague, 2013. http://www.government.nl/privacy. (Accessed: 2013.01.31)

Greening, Justine, "Airport security scanners. Written statement of the Secretary of State for Transport.", Department for Transport, London, 2011. https://www.gov.uk/government/speeches/airport-security-scanners.

Grijpink, J.H.A.M., "Checklist biometrische persoonsherkenning (NL-versie)", *Checklisten Informatiemanagement (update 34)*, SDU, Den Haag, 2009.

Haes, Andreas Udo de, "Albert Heijn zet betalen met vingerafdruk in de koelkast", *Webwereld*, 17 March 2009. http://webwereld.nl/nieuws/56479/albert-heijn-zet-betalen-met-vingerafdruk-in-de-koelkast.html.

Hallinan, Dara, and Michael Friedewald, "Economic costs of surveillance technologies", in David Wright (ed.), *IRISS Deliverable D1.1: Surveillance, fighting crime and violence*, 2012, pp. 233-246. http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf.

Hämmerli, Bernhard, and Andrea Renda, "Protecting Critical Infrastructure in the EU - CEPS Task Force Report", Centre for European Policy Studies, Brussels, 2010. http://www.ceps.eu/ceps/dld/4061/pdf.

Harris, Shane, "Brazil To "60 Minutes: It Wasn't a Hacker", *The Atlantic*, 10 November 2009. http://www.theatlantic.com/politics/archive/2009/11/brazil-to-60-minutes-it-wasnt-a-hacker/29934/.

Jain, Anil K., Arun Ross and Umut Uludag, "Biometric template security: Challenges and Solutions", Paper presented at: Proceedings of the 13th European Signal Processing Conference (EUSIPCO), Antalya, Turkey, 2005.

Kleinz, Torsten, *CCC publiziert die Fingerabdrücke von Wolfgang Schäuble* 2008. http://www.heise.de/security/meldung/CCC-publiziert-die-Fingerabdruecke-von-Wolfgang-Schaeuble-Update-193732.html.

Koorn, Ronald, Herman van Gils, Joris ter Hart et al., "Privacy-Enhancing Technologies - White Paper for Decision-Makers", Ministry of the Interior and Kingdom Relations, The Hague, 2004. http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

Krebs, Brian, "Experts: Smart grid poses privacy risks", *The Washington Post*, 18 November 2009. http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_priva.html.

Krebs, Brian, *Cable: No Cyber Attack in Brazilian '09 Blackout*, 2010. http://krebsonsecurity.com/2010/12/cable-no-cyber-attack-in-brazilian-09-blackout/.

Kroft, Steve, and Graham Messick, "Cyber War: Sabotaging the System", *CBSNews, 60 minutes*, 06 November 2011. http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

Kruger, Erin, Shoshana Magnet and Joost Van Loon, "Biometric Revisions of the `Body' in Airports and US Welfare Reform", *Body & Society*, Vol. 14, No. 2, 2008, pp. 99-121. http://bod.sagepub.com/content/14/2/99.short.

Kursawe, Klaus, George Danezis and Markulf Kohlweiss, "Privacy-friendly Aggregation for the Smart-grid", in Simone Fischer-Hübner, and Nicholas Hopper (eds.), *Privacy Enhancing Technologies*, Springer, Waterloo, ON, Canada, 2011, pp. 175-191. http://research.microsoft.com/pubs/146092/main.pdf.

L3 Communications, "Security and Detection Systems", 2013. http://www.sds.l-3com.com/advancedimaging/provision-at.htm. (Accessed: 13 March 2013)

Latour, Bruno, *Science in Action: How to Follow Scientists and Engineers Through Society*, Harvard University Press, Cambridge, Mass., 1987.

Latour, Bruno, *La clef de Berlin et autres leçons d'un amateur de sciences*, Éditions la Découverte, Paris, 1993.

Law, John, "Enacting Naturecultures: a Note from STS", Centre for Science Studies, Lancaster University, Lancaster, 2004. http://www.lancs.ac.uk/fass/sociology/papers/law-enacting-naturecultures.pdf.

Lynch, M., M. White and R. Napier, "Investigation into the use of point-to-point speed cameras", Transport Agency research report no. 465, NZ Transport Agency, Wellington, 2011. http://www.nzta.govt.nz/resources/research/reports/465/docs/465.pdf.

Mathieson, S. A., "Worried about being watched? You already are", *The Guardian*, 15 February 2007. http://www.guardian.co.uk/technology/2007/feb/15/epublic.guardianweeklytechnologysection.

May, Torsten, "Body Scanner Technologies: a review", Paper presented at: International Conference "Security, Ethics, and Justice: Towards a More Inclusive Security Design", 21-23 June 2012, Tübingen, Germany, 2012. http://www.uni-tuebingen.de/en/facilities/international-centre-for-ethics-in-the-sciences-and-humanities/research/ethics-and-culture-security-ethics/focus-of-research-security-ethics/kreta/internationale-tagung.html

McDaniel, Patrick, and Stephen McLaughlin, "Security and privacy challenges in the smart grid", *Security & Privacy, IEEE*, Vol. 7, No. 3, 2009, pp. 75-77.

McLaughlin, Stephen, Dmitry Podkuiko and Patrick McDaniel, "Energy Theft in the Advanced Metering Infrastructure", in Erich Rome, and Robin Bloomfield (eds.), *Critical Information Infrastructures Security*, Springer, Berlin, Heidelberg, 2010, pp. 176-187.

Mehta, Praktik, and Rebecca Smith-Bindman, "Airport full-body screening: What is the risk?", *Archives of Internal Medicine*, Vol. 171, No. 12, 2011, pp. 1112-1115. http://dx.doi.org/10.1001/archinternmed.2011.105.

Metropolitan Police Service, "New approach to ANPR launched", London, 2012. http://content.met.police.uk/News/New-approach-to-ANPR-launched/1400012148405/1257246741786.

Meulenhoff, P., and M. Van der Werff, "Deep Packet Inspection", TNO Report 35134, TNO, Groningen, 2010.

Mochalski, K., and H. Schulze, "Deep Packet Inspection: Technology, Applications & Net Neutrality", White Paper, Ipoque, Leipzig, 2009. http://www.ipoque.com/sites/default/files/mediafiles/documents/ipoque_WP_Deep_Packet_Inspection_2009_DPI.pdf.

Mom, Peter, "'Paspoortbiometrie is mensenrechtenschending'", *Binnenlands Bestuur*, 29 October 2010. http://www.binnenlandsbestuur.nl/digitaal/nieuws/paspoortbiometrie-is-mensenrechtenschending.381106.lynkx.

Munkittrick, David, "Smart Grid Technology Implicates New Privacy Concerns", 2012. http://privacylaw.proskauer.com/2012/03/articles/data-privacy-laws/smart-grid-technology-implicates-new-privacy-concerns/. (Accessed: 19 March 2013)

My Secure Cyberspace, "Smart Grid and Privacy Concerns", 2013. http://www.mysecurecyberspace.com/articles/features/smart-grid-and-privacy-concerns.html. (Accessed: 19 March 2013)

Navigant Research, "Smart Meters in Europe", 2012. http://www.navigantresearch.com/research/smart-meters-in-europe. (Accessed: 19 March 2013)

NCTb, "NCTb Q&A Security Scan", 2010. http://english.nctb.nl/Images/Factsheet%20security%20scan%20UK_tcm92-246192.pdf. (Accessed: 14 March 2013)

Netbeheer Nederland, "Net voor de toekomst: een verkenning", Netbeheer Nederland, Arnhem, 2011. http://www.netbeheernederland.nl/Content/Files/373_320008-Rapport%20Net%20voor%20de%20Toekomst.pdf.

NPIA, "Practice Advice on the Management and Use of ANPR", National Policing Improvement Agency, London 2009. http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf.

NTOP, "nDPI: Open and Extensible GPLv3 Deep Packet Inspection Library", 2013. http://www.ntop.org/products/ndpi/.

OPTA, "Voorlopige bevindingen OPTA over gebruik van Deep Packet Inspection door aanbieders van mobiele telefonienetwerken", OPTA/ACNB/2011/201469, Den Haag, 2011. http://www.opta.nl/nl/download/publicatie/?id=3439.

Petermann, Thomas, Harald Bradke, Arne Lüllmann et al., "What happens during a blackout: consequences of a prolonged and wide-ranging power outage", TAB, Office of Techonlogy Assessment at the German Bundestag, 2011. http://www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf.

Rossides, Gale D., "Letter to Bennie J. Thompson, chairman of the Committee on Homeland Security, U.S. House of Representatives", U.S. Department of Homeland Security, Transportation Security Administration, Arlington, VA, 2010. http://epic.org/privacy/airtravel/backscatter/TSA_Reply_House.pdf.

Sætnan, Ann Rudinow, Johanne Yttri Dahl and Heidi Mork Lomell, "Views from under surveillance. Public opinion in a closely watched area in Oslo", Urban Eye Working Paper No. 12, Trondheim/Oslo, 2004. http://www.urbaneye.net/results/ue_wp12.pdf.

Schiphol, "Airport secuity: Security scan", 2013. http://www.schiphol.nl/web/file?uuid=2a47b6ff-3a71-4054-a603-6e68aae51cfa&owner=fc5889a9-e049-442a-b208-b416f05e180d. (Accessed: 13 March 2013)

Scientific Committee on Emerging and Newly Identified Health Risks, Anssi Auvinen, Thomas Jung et al., "Health effects of security scanners for passenger screening (based on X-ray technology)", European Commission, Brussels, 2012. http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_036.pdf.

Sluijs, Jasper P., *Network Neutrality and European Law*, Wolf Legal Publishers, Nijmegen, 2012. http://arno.uvt.nl/show.cgi?fid=128367.

Snijder, Max, "Het Biometrisch paspoort in Nederland: Crash of zachte landing", Webpublicatie Nr. 51, Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag, 2010. http://www.wrr.nl/fileadmin/nl/publicaties/PDF-webpublicaties/Het_biometrisch_paspoort_in_Nederland.pdf.

TNO, *BIAR-Deelrapport: Technieken om online-radicalisering te signaleren*, TNO-DV, Vol. 2010 C 439, 2010.

TOR Project, "Tor Project: Anonymity Online", 2013. https://www.torproject.org/index.html.en. (Accessed: 1 March 2013)

Tracy, Meghann, Heather Ruzbasan Cotter and William Nagel, "Privacy impact assessment report for the utilization of license plate readers", International Association of Chiefs of Police, Alexandria, VA, 2009. http://www.theiacp.org/LinkClick.aspx?fileticket=N%2bE2wvY%2f1QU%3d&tabid=87.

TSA (USA Transportation Security Administration), "AIT: how it works", 2013. http://www.tsa.gov/ait-how-it-works. (Accessed: 13 March 2013)

UNODC (United Nations Office on Drugs and Crime), *The Use of the Internet for Terrorist Purposes*, United Nations, Vienna, 2012. http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

van der Ploeg, Irma, "Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications", in S. van der Hof, and M .M. Groothuis (eds.), *Innovating Government*, T. M. C. Asser, Den Haag, 2011, pp. 29-40.

van der Ploeg, Irma, and Isolde Sprenkels, "Migration and the Machine-Readable Body: Identification and Biometrics", in Huub Dijstelbloem, and Albert Meijer (eds.), *Migration and the new technological borders of Europe*, Palgrave Macmillan, London, 2011, pp. 68-104.

van der Ploeg, Irma "Machine-Readable Bodies, Biometrics, Informatization and Surveillance", in Emilio Mordini, and M. Green (eds.), *Identity, Security and Democracy*, IOS Press, Amsterdam, 2009, pp. 85-94.

van der Ploeg, Irma "Security in the Danger Zone: Normative Issues of Next Generation Biometrics", in Emilio Mordini, and Dimitros Tzovaras (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, Dordrecht, 2012, pp. 287-303.

van Kleef, Frans, "Position paper: Betrouwbaar en veilig gebruik van biometrie", Nederlands Biometrie Forum, Tilburg, 2012. www.biometrieforum.nl.

van Lieshout, Marc, Michael Friedewald, David Wright and Serge Gutwirth, "Reconciling privacy and security", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1-2, 2013.

van Voorthuizen, Joris, and Han Slootweg, *Smart Grids*, Position Paper, Enexis DSO, 2011. https://www.enexis.nl/Documents/position-paper-smart-grids-2011-06.pdf.

Vermeer, Reinier, "'DPI-gebruik van KPN geen strafbaar feit'", *Webwereld*, 3 August 2011. http://webwereld.nl/nieuws/107507/-dpi-gebruik-van-kpn-geen-strafbaar-feit--.html.

Watson, Barry C., and Karen M. Walsh, "The road safety implication of automatic number plate recognition technology (ANPR)", Center for Accident Research & Road Safety Queensland, Brisbane, 2008. http://eprints.qut.edu.au/13222/1/13222.pdf.

Webb, Barry, and Bronny Raykos, "Theft of vehicle number plates: a problem analysis", University College London, Jill Dando Institute of Crime Science, London, 2006. http://www.ucl.ac.uk/scs/downloads/research-reports/numberplate-theft-report.

Weimarer Verfassung, "Die Verfassung des Deutschen Reichs vom 11. August 1919", Reichsgesetzblatt, Jg. 119, Nr. 152 vom 14. August 1919, S. 1383-418. http://www.dhm.de/lemo/html/dokumente/verfassung/index.html. (Accessed: 12 March 2013)

WikiLeaks, *09BRASILIA1383, BRAZIL: BLACKOUT - CAUSES AND IMPLICATIONS*, 2011. http://www.wikileaks.org/cable/2009/12/09BRASILIA1383.html.

WikiPedia, "Richard Reid", 2013. http://en.wikipedia.org/wiki/Richard_Reid. (Accessed: 20 March 2013)

Willemsen, Clemens, *Biometrics: how it works*, Progis; Ministry of Justice, The Hague, 2009.
Wittgenstein, Ludwig, *Philosophical Investigations/Philosophische Untersuchungen*, Blackwell, Oxford, 1953.
Zetter, Kim, "Hackers Publish German Minister's Fingerprint", *Wired*, 31 March 2008. http://www.wired.com/threatlevel/2008/03/hackers-publish/.