Chapter 5
Theorizing technologically mediated policing in smart cities
An ethnographic approach to sensing infrastructures in security practices

Vlad Niculescu-Dincă

Abstract Smart digital infrastructures predicated on myriads of sensors distributed in the environment are often rendered as key to contemporary urban security governance to detect risky or suspicious entities before or during a criminal event takes place. At the same time, they often involve surveillance of urban environments, and thus not only criminals but also large groups of people and entities unrelated to criminal phenomena can end up under close inspection.

This chapter makes its contribution on two levels. For one, it offers a theoretical framework to the research and conceptualization of the role of sensing infrastructures in urban security practices. It shows how insights from Philosophy of Technology and Science and Technology Studies can produce a nuanced understanding of the role of digital technologies in security practices, beyond standard conceptualizations of technology. Moreover, the chapter proposes a geological approach to enrich our repertoire of imagining and researching smart urban ecosystems.

Secondly, the chapter contributes to a higher level of transparency of these practices by presenting the results of ethnographic research performed in a set of police organizations that employ sensing infrastructures and algorithmic profiling in their practices. The chapter draws empirically on research performed in the Dutch police, both at municipal and national levels with some additional material gathered in a constabulary in England. In these organizations, resource allocation decisions are often predicated on automated number plate recognition technology that processes data from an array of smart cameras distributed in the environment. In these ways together, the chapter highlights a set of normative issues with implications for the effectiveness and legitimacy of urban security (surveillance) practices in smart environments.

Keywords sensing, infrastructures, policing, philosophy of technology, urban ecosystems

Vlad Niculescu-Dincă (✉)
v.niculescu-dinca@fgga.leidenuniv.nl
Assistant Professor. Institute of Security and Global Affairs. Faculty of Governance and Global Affairs Leiden University. Turfmarkt 99, 2511 DP. Den Haag, The Netherlands.

5.1 Introduction

Contemporary urban ecosystems are increasingly pervaded by ubiquitous and networked sensors and devices communicating with each other and with other (online) services. Combining existing information infrastructures with a stream of initiatives and innovations these sensing infrastructures enable the gathering, communication and processing of data about the urban lifeworld. They support visions – referred to with umbrella terms such as Smart Cities and similar terms – that bring the promise of efficient, green, safe and secure cities (Townsend, 2013; Kitchin, 2014).

In the area of urban security governance, digital infrastructures have long been rendered as key enablers of efficient policing practices. For instance, intelligence-led policing styles promote not only specific tactics and ways of doing the business of policing but is also associated to a significant employment of overt and covert "technical means" (Tilley, 2008; Ratcliffe, 2008). Especially when combined with profiling and algorithms–ranging from rule-based algorithms to machine learning algorithms–digital infrastructures are relied upon in efficient resource allocation and decision-making processes. The role that digital technologies play in contemporary policing has made several authors link them to dramatic changes in the organization of the police (Chan, 2001; Harris, 2007; Byrne and Marx, 2011). At the same time, such solutions often imply and enable surveillance practices. Increasingly practiced by a plethora of public and private actors coming together in security networks, not only at national and international levels but also at local and regional levels (Whelan and Dupont, 2017), surveillance remains a key practice of modern approaches to policing (Leman-Langlois, 2012).

However, many scholars (Ericson and Haggerty, 1997; Maguire, 2000; Neyroud, 2008; Hildebrandt and Koops, 2010) have pointed out that not only criminals but also individuals and groups unrelated to criminal phenomena come under the close inspection of surveillance assemblages (Haggerty and Ericson, 2000) or are being subject to discriminatory decisions (Lyon, 2003; Wittkower, 2017). This is not to say that technology is a priori leading to these outcomes. It has been argued for instance that information technologies can play an important role in minimizing the discriminatory effects of surveillance (Kamiran et al., 2012; Mancuhan and Clifton, 2014), while still enabling an effective policing (Schakel et al., 2013; Hellemons et al., 2013).

In this respect, empirical studies of the ways in which smart digital infrastructures are engaged in policing are viable ways to inform a higher level of transparency and human rights protection and, at the same time, not compromise the effectiveness of police work. That is, such kind of studies (Sanders, 2006; Van Ooijen and Nouwt, 2009) document technologically mediated practices in urban policing (after the fact and without operational information) and enable more clarity over the ways in which software-enabled technologies work in urban security practices.

However, there is still a scarcity of empirical studies of policing practices mediated by smart infrastructure technologies. Of course, there are at least two valid reasons for this gap in the literature. For one, police organizations require long and often difficult procedures for access to empirical research even if they are more transparent then ever (Manning, 2008). Although notable studies took an ethnographic approach to study technologies and surveillance in policing organizations (Norris and Armstrong, 1999; Manning, 2008), obtaining research access is often a difficult undertaking. Secondly, the novelty of technologies themselves and the opacity of algorithms make it such that empirical studies of these technologies in practice do not abound, with a few exceptions (Meijer and Thaens, 2018a, 2018b).

Still, unlike many Smart City visions, some of the technologies are already here: radio frequency identification (RFID), automatic number plate recognition (ANPR), Bluetooth, ZigBee, and more. For instance, in policing literature, ANPR cameras are often regarded as one type of sensor employed by police to detect vehicles in traffic and monitor the road infrastructure from large control rooms that aggregate data flows from the environment. ANPR technology can network with other types of sensors to enable the police to also cover 'railways, waterways and cyberspace' (Schakel et al., 2013, p. 12). Many police organizations utilize ANPR in a variety of practices, from finding stolen vehicles and wanted criminals to profiling suspicious traffic behaviour. Therefore, empirically studying ANPR in these kinds of practices as, well as the ways in which the software code is designed, provides an opportunity to understand how urban security governance engages with smart city digital infrastructures.

Moreover, the chapter offers a vocabulary and approach to research and conceptualizes the complex role of sensing technologies in urban security practices. A vast majority of practitioners' guides, technical reports, policing managerial guidelines, promotional materials of technology producers, and a significant body of policing literature take a standard instrumentalist view on technologies as technical means. However, rendering technologies as neutral means tends to ignore their social, political and ethical charge. Remaining in this framing of technology, the conditions remain arbitrary for a more informed process of using and shaping smart infrastructures and their engagement in urban security governance.

The chapter brings insights from Philosophy of Technology and Science and Technology Studies to produce a more nuanced conceptualization of digital technologies in policing practices, beyond instrumentalist views. For one, it shows how an Actor-Network Theory inspired approach (Akrich, 1992; Akrich and Latour, 1992; Bowker and Star, 1999; Latour, 2005; Law, 2008; Mol, 2010) can be employed to 'dig up' and trace the ways in which suspicion and risk sediment in the layers of software code and get enacted in the broader materiallyembedded policing practices. Engaging with the conceptual framework of mediation theory (Verbeek, 2011), the chapter reflects on how the practitioners' perceptions, experiences, decisions and actions are mediated by sensing infrastructures and algorithmically-generated entities. In these ways together, the chapter highlights a set of normative issues with implications for the effectiveness and legitimacy of urban security in smart environments.

The rest of the chapter is structured as follows. Section 1 gives a brief introduction to ANPR and documents policing practices that utilize this technology. Section 2 outlines an analytical framework to understand the role of technologies by building on research in philosophy of technology (PoT) and science and technology studies (STS). Section 3 shows the active mediation of sensing technologies–from the simplest, most common practice of detecting a priori known vehicles in traffic to the more sophisticated profiling techniques. Section 4 'digs' through the code of a set of profiles and renders the profile design process as a locus of reflection for ethical and effectiveness considerations. Section 5 concludes these investigations and outlines a set of considerations about the conditions that need to be met for these technologically enabled practices to deliver on their promises of enabling both effective and legitimate security practices.

5.2 Doing fieldwork on ANPR in policing

ANPR is a technology enabling the real-time identification of license plates of cars in traffic. Spread in large numbers across the environment or in mobile units that patrol particular areas, ANPR cameras sense the movements of vehicles, transmitting data in real-time to a back office facility. The technology dates from the late ‘70s and has slowly gained a reputation for an accurate technology with high reliability levels (Parker and Federl, 1996). Since its introduction, ANPR has been deployed in parking lots, entrances to areas, highways, roads, in marked and unmarked vehicles, and in any arrangement that needs to monitor road traffic and identify vehicles.

The most common way of engaging ANPR technology is by comparing number plates in realtime with reference lists. These reference lists of numbers are of particular interest to the organization running an ANPR system: road administrators, tax authorities or police organizations. For instance, monitoring the traffic is done to allow/block passage, to select for further investigation or to arrest. The choices of how many lists to define and how many numbers to include in a list are virtually unlimited. Lists may contain from one number plate up to tens of thousands. If the system detects a match in one of the lists, it returns a so-called ‘hit’. The hit is accompanied by additional information on location, date, time, potential intelligence that may prompt further actions, and audible and visual alerts (coloured markers).

Another way to tackle criminal phenomena where the vehicles are not a priori known relies on designing real-time behavioural profiles based on crime models. These models are generalized abstractions of real world criminal phenomena (e.g. burglary, cargo theft, or drug trafficking) and capture various aspects such as locations, times, social networks or modus operandi (Schakel et al., 2013). Because it would be practically impossible to monitor locations all the time, let alone infer behavioural patterns, knowledge rules derived from these models are delegated to automated profiles that select suspicious behaviour based on sensor data and processing algorithms. In this way, the police can detect suspicious behaviour when those vehicles were not included in any police list. It is important to distinguish here between kinds of algorithms. One type of profile is the one generated with machine learning techniques, in which unexpected knowledge is produced, previously not hypothesized (Hildebrandt and Gurtwith, 2008). Another type of profiles are those that are directed, in which the algorithmic rules are previously derived from police knowledge, typically aggregated from different fields of the discipline, and then applied to the live traffic.

The chapter draws empirically on ethnographic research I performed in Dutch police organizations at local and national levels where, at that time, they engaged in the second type of profiling. That is, profiles were built through knowledge sharing between multiple branches of the police. To gain an additional vantage point, I’ve also studied the use of ANPR in a constabulary in England[1] which, at the time of the study had one of the densest networks of ANPR cameras in the UK, storing traffic data in persistent databases.

While both police services employed a similar ANPR system, purchased from the same vendor, they differ in the mode of engagement. Whereas the UK constabulary turned off part of its ANPR system in response to sustained criticism of its surveillance potential, the Dutch police started to explore alternative ways of engaging ANPR. That is, instead of storing all traffic data,

[1] To protect the confidentiality of the individual police officers the name of the organizations are anonymized in this study and the names of individual officers were made generic.

they only select suspicious behaviour based on knowledge rules delegated to real-time algorithms that process ephemeral data streams, aiming to catch criminals red-handed (Schakel et al., 2013). With this way of engaging with sensing infrastructures, they aim at reducing the surveillance impact for most traffic participants, "protecting people's privacy by design" while simultaneously performing their policing tasks (Hellemons et al., 2013).

In both settings I performed semi-structured interviews with members of the ANPR teams. There were ten in-depth interviews in the Netherlands with multiple police officers involved in ANPR operation and with lead designers involved in building profiles. In England I had three in-depth interviews with the head of the ANPR team, control room operator and the senior analyst of the constabulary. In addition, I made ethnographic observations in these settings for more than 50 hours taken together. These included participant observation sessions in control rooms to understand how the system enabled their operative decisions. Additionally, I participated in actions with road policing units to understand the implications of the ways in which officers worked with and talked about these technologies.

5.3 Theoretical underpinnings

So how do policing practitioners typically talk about these technologies? How do they understand their role in daily policing work? What can philosophy of technology bring? This section first discusses some of the most common conceptions of technology in policing and it analyses the assumptions, implications, and limitations of these conceptualizations of technology. It then outlines the theoretical framework of the chapter by bringing together insights from the areas of Science and Technologies Studies and Philosophy of Technology and showing how they can complement each other and offer a more nuanced and theoretically informed way of conceptualizing the role of digital technologies in policing practices.

5.3.1 Technology in policing work-talk

Digital technologies have become constitutive of many contemporary professional practices and feature in their daily routines and ways of relating to the broader socio-technical infrastructures in which they feature. It is therefore no surprise that professionals develop vocabularies to come to grips with these entities that affect their practices so profoundly. The same is the case with policing practitioners. As the importance of technologies is unanimously recognized as a defining characteristic of contemporary policing, practitioners and scholars need to conceptualize their new and older technologies.

For many, technologies are 'technical means' (Tilley, 2008, p. 375), 'computer-based instruments' (Innes and Roberts, 2008, p. 250) or 'powerful tools' (Leipnik and Albert, 2003, p. 3). When technology is talked about on the beat, much of police officers' 'work-talk' involves a vocabulary that mainly covers the use, capabilities and powers of particular systems, equipment, machines and devices (Manning, 2008). They are "tools of communication like radios and call boxes, tools of investigation like cameras and fingerprint kits, and tools of surveillance like video and audio pickups. Increasingly, newer, more specific tools have been developed using emerging technologies. These innovations enhance the old tools and make some new tools possible” (Williams and Williams, 2008, p. 165).

This analysis is not meant to criticize police officers or the larger body of work of some of these authors but to point out the influence and limitations of particular conceptions of technology. In this conception, technologies are rendered as passive and obedient in the hands of their users. Tools do not determine human action. They are neither good nor bad, as people use them for their purposes; in this case the crime control purposes of policing practitioners. To illustrate this view we can find again a quote from the policing literature: “Just as technology can prevent or solve a crime, criminals can use technology to commit a crime. Computers can be used to hack into a company’s computer system and alter information or transfer documents and falsify transactions” (Williams and Williams, 2008, p. 169). In this framing, technologies are value neutral. Technology does not entail consequences by itself but consequences are only stemming from choices made by the users (Sclove, 1995; Brey, 1998).

5.3.2 Theorizing the role of technologies in policing practices

So are technologies adequately understood as neutral tools in the hands of policing practitioners? This framing of technology may seem ‘common sense’ but it carries with it particular assumptions concerning the social role of technologies. To some extent it is understandable to want to think of technologies in policing as just tools in the hands of officers. In an environment pervaded with ever more sophisticated technologies, this conception places the responsibility for the outcomes in the hands of the practitioner. After all, nobody wants a police officer to wrongfully arrest someone or, when failing to catch a criminal, decline responsibility with the claim: ‘The technology made me do it’. This conception of technology places responsibility for the outcomes in the hands of the users, however at a cost. Rendering technologies as neutral tools ignores the social, political and ethical dimensions of technologies as it silences their active role in inducing consequences. It lacks an account of the complex interactions between users, designers, organizations, institutions and legal regimes. Consequently, it provides a rather poor conceptual background for understanding the complex arrangements of smart urban environments and technologically-infused policing.

In the past decades, this view began to be contested by a body of work from an array of directions such as philosophy of technology, history of technology and science and technology studies, to name but a few. Rather than assuming technologies as neutral or explicitly trying to get to a substance of modern technology, these studies analyse technology and science as thoroughly social activities. That is, they follow the technologists, scientists and/or users during their work and activities of producing and using knowledge and artefacts. They follow them as members of communities within which they interact with peers and get connected to broader cultural and societal processes, conflicts and debates. These studies delve into empirical investigations to understand how facts, knowledge, classifications, phenomena or artefacts are constructed or performed and what imprint these processes leave on social activities and their outcomes (Pinch and Bijker, 1987; MacKenzie and Wajcman, 1985; Bijker, 1992; Bowker and Star, 1999; Bijker, 2010; Law and Mol, 2001; Law, 2008).

In the STS tradition, Actor-network theory (Callon, 1987; Law, 1987; Latour, 1988; Akrich, 1992; Law and Mol, 2001; Law, 2009) is a framework, developed initially by Michel Callon, Bruno Latour and John Law, that emphasizes a symmetrical consideration of humans and of non-humans in analysing processes of construction (non-humans meaning anything else besides human beings, usually referring to technological artefacts but also, for instance, institutions, organizations, etc.).

This kind of analyses have been made in a wide variety of studies and, as a general feature, they treat symmetrically a diverse set of components that span materials, equipment, components, people, and institutions as simultaneously participating in the formation of *networks of relations*. For instance, Michel Callon (1987) uses the term '*engineer-sociologist*' to point out that technologies and visions of society are bounded to each other and neither would happen without the other. Similarly, John Law (1987) uses the term '*heterogeneous engineering'* to argue that the work of technologists should not be separated as 'engineering' from the changing of society that is involved in introducing a new technology.
Similarly, for Latour (Latour, 1987, 1988, 1991, 2005), reality cannot be properly understood if humans and non-humans are analysed asymmetrically. Actor-network theory does not wish to prejudge the relative power or influence of any of the *actants*. The term is often used by Latour to emphasize even more the symmetric consideration of humans and non-humans as the term 'actor' usually suggests human agency. In this sense, he argues, what a thing is and does and also what a human being is and does, stems out of the *networks of relations and associations* that they have with other things and humans rather than from an essence that underlies them (Latour, 1988).

We may extend the argument to aggregates in a machine or to relations between machines and other entities such as standardization bodies, users or maintainers. For instance, a bicycle chain rotates the wheels in relation to a sprocket that matches and to a biker who pushes the pedals. A police officer assesses someone as suspect in relation to a risk profile that automatically generates a hit and in relation to an organization that assigns this task. If we want to understand the role of an automated profile in this process, we may want to make Latour's thought experiment and just imagine how much effort might be needed to obtain the same result without it: how many police officers in the field watching and quickly writing down number plates, how many meetings to discuss the findings, in the hope of finally agreeing on an identified pattern. In this sense, he argues, 'purely technical' artefacts should be understood as highly social and moral (Latour, 1988, 298).

5.3.3 On technological mediation

Therefore, we need a vocabulary that could help us talk and think about technologies in policing practices as actively doing something for and among police officers, organizational structures, legal provisions, inter-institutional arrangements and others without reducing them to neutral tools. We need a vocabulary that comes to grips with the active and nuanced role of technologies in influencing officers' practices, experiences, perceptions, their decisions and their actions.

Scripts and mediation of action

A contribution of ANT that conceptualizes the ways in which technologies relate to human action comes from Madeleine Akrich and Bruno Latour (Akrich, 1992; Akrich and Latour, 1992). They propose the notion of *script* and the related family of notions (prescription, inscription, subscription, etc.). In this vocabulary, rooted in ANT, rather than talking about technologies as tools, they *mediate* human action in the same manner in which theatre scripts influence the behaviour of actors: they are compelling enough to tell the actors what to do but do not determine how they will eventually perform.

In this understanding, technologies guide, inform, (firmly) suggest the user what to do/not to do with them (e.g. through user manuals, instructions, their shape but also their material properties and constraints of use). For example, 'two-hands' control mechanism require workers to use both hands to start a press in order to prevent work accidents. Weighted hotel keys are compelling guests to return them to reception if they don't wish to carry all day a bulky piece of metal. Speed bumps, or sleeping policeman as they are sometimes called, are compelling drivers to slow down in order not to wreck their cars or hit their heads, and in this way enforcing traffic norms (Latour, 1994).
At the same time, scripts imply scriptwriters. Designers translate their intentions and values, *delegating* them to the functions of artefacts. Technologies can be said to be more then neutral intermediaries but be involved in *translating programs of action*. This is the case when designers anticipate particular users with their behaviour, interests and motives in relation to the artefacts and they build in *preinscriptions*. For instance, designers of control room infrastructures in policing anticipate that officers need to be quickly alerted to certain situations from whatever state they were in, and they design bright and flashy visual alerts to wake up even the most bored officer. However, in the vocabulary of technological mediation, users can also give meanings to artefacts, thus also taking part in the inscription processes. For instance, officers can also choose to remain in the same state without even a casual glance at the alert.

Moreover, artefacts can be *prescriptive* without this originating in a designer's intention. For instance, visually impaired people were often unable to register for websites that implemented mechanisms for stopping 'robot registration' (website users need to introduce some random and distorted characters that are generated in a difficult to read image). In these cases, users are encouraged to behave in particular ways, as the scripts are guiding and altering their behaviour without the need of the designer's presence. Scripts are thus normative, transforming or reinforcing existing 'geographies of responsibilities' (Akrich, 1992), convincingly demonstrating the normative charge of technological artefacts.

While users may *subscribe* to the artefact's suggestions/constraints (e.g. workers may use both their hands to operate a 'two-hands' control, police officers may arrest those suggested by the profiling algorithms), it may also be the case that they define novel roles in relation to technologies, sometimes in opposition to the program of action (e.g. workers may still use only one hand if they really wish. For instance, by using a long stick that reaches both buttons of the control mechanism). Just like with a theatre script, an actor is able to appropriate it, change it and give it new meanings and interpretations. Even if this sometimes requires extra effort, the outcomes can be significantly different from what the designer intended. ANT does not a priori analyse technological artefacts as determining human behaviour and social relations.

In this light, the development of technologies appears as a heterogeneous process in which a whole set of actors bear parts of the responsibility for their effects. Rather than holding a heroic view of the user, fully responsible of the outcomes of technology, but also steering away from deterministic views in which 'we can't do anything about it', the notion of script conceptualizes both users and designers as actively inscribing their worldviews, interests and values in processes of technological development. Recognizing that technological designs and material artefacts are more than mere tools enables the study of interactions between users and technology with a vocabulary that allows more attention to their active mediation.

Mediating perception and experience

The vocabulary of technological mediation can be further expanded to help us understand more of the complex practices of police officers working with technologies in contemporary policing. Technologies mediate not only action but also human perception, practices and experiences of the world (Verbeek, 2005). What does it mean to 'smell something fishy' when reading indicators on a computer screen? What does it mean when officers say that 'something just didn't feel right' (Hess and Orthmann, 2010, p. 12)? How do police analysts perceive a rise/decrease in criminal phenomena from their computer desk by looking at numbers in a system? How do road policing units experience high-pitched sound alerts and flashy indicators of 'suspect vehicles'? How do mediated perceptions influence decision and action?

Peter-Paul Verbeek expands the vocabulary of technological mediation and shows how it can be applied to many other areas such as industrial design (Verbeek, 2005), engineering ethics (Verbeek, 2006, 2011) or interaction design (Verbeek, 2015). He builds on both ANT and the post-phenomenological approach of Don Ihde (1990). In the post-phenomenological approach technologies and human beings are understood as helping to constitute and shape each other into being. As Verbeek argues this point: "[Technologies] help shape how human beings can be present in the world and how the world can be present for human beings" (Verbeek, 2015, p. 29). For instance, they "help scientists to perceive the world. The reality of a star is profoundly mediated by telescopes, brain activity by MRI scanners, and the health condition of a fetus by ultrasound devices. Such mediations are not merely neutral "intermediaries": What a star, the brain, and an unborn child are for us cannot be understood without taking into account the mediating role of technologies in our perception and understanding of them" (Verbeek, 2015, p. 29).

Both Ihde and Verbeek steer away from approaching technologies in terms of essences or absolute foundations and from locating humans and technologies in two distinct spheres: one of the human subject, the other of the technological object. By understanding them as constituting each other, the approach aims to overcome some of the problems that classical phenomenology has been criticized for – seeking to describe 'reality itself' (Verbeek, 2005) or for "elevating a single person's self-ethnography to grandiose proportions" (Mol, 2010, p. 254). Rather, the approach of Ihde and Verbeek is called 'post' phenomenological as it aims to overcome these problems while still investigating the way in which actual technologies shape human access, experience and interpretation of reality. "Investigations of this type of mediation cannot possibly aim to return to 'the things themselves', but rather aim to clarify the structure of technological mediation and its hermeneutic implications" (Verbeek, 2008, p. 13). Issues of interpretation are central to this approach and its questions concern the mediating role of technologies from a hermeneutical perspective.

Types of relations and influences

Don Ihde identifies several ways in which humans interact with artefacts from this perspective and proposes a taxonomy to characterize these interactions. One type of relation in which artefacts mediate perception he calls *embodiment*. In this kind of relation technologies become a unity with the human being, so the artefacts is part of the experience. For instance, police officers look *through* binoculars, and not *at* binoculars, to follow someone or they perceive suspicious traffic activities on the streets *through* video surveillance systems.

The second relation in this taxonomy, Ihde calls *hermeneutic* and therefore implying the need for interpretation. In this relation of mediation, we experience the world with the explicit contribution of technology that calls our attention. For instance, we interpret the numbers on a thermometer to understand the temperature outside. A too high value means 'it is very hot'. In a similar manner, police agents read indicators on screens and they interpret their values, pitches or tones. They take some to mean, for instance, that 'the old boys are back in town' while others as being irrelevant or indicating 'business as usual'.

Another type of relation characterizes the interaction with the artefact itself. In this type of relation, that Ihde calls an *alterity* relation, human beings interact with technologies while the world is in the background of their interaction. This may be the case, for instance, when police officers operate a device or when police programmers code the criteria for a risk profile, while the criminal phenomenon still unfolds. In this case, Ihde argues, the world is in the background of the interaction with technologies, while attention is directed at the artefact.

In the *background* relation, technology shapes the relation to reality but without having an active role in the experience. In this type of relation technologies are the context for human experiences. In the policing context we can think of the sound of sirens while police officers approach and discuss with a suspect on the street, the humming noise of computers in a control room while officers analyse indicators on screens, or the warm air of the air-conditioning system of a police car. In these examples technologies shape officers' experience – for instance making them more relaxed, alert, stressed or irritated – but in the background of other activities.

Another type of relation that Verbeek (2011) identifies comes from technologies that merge with our environment. Smart environments are more than a background of human experience but have an *interactive* dimension. They form the context of human experience but can actively emerge from this context and call explicit attention. This kind of technology can actively detect vehicle number plates, recognize faces, sense movement and automatically give signals to police officers when detecting suspicious behaviour.

Finally, wearable technologies result in another kind of relation. Smart glasses, for instance, can be simultaneously embodied, just like normal glasses, but at the same time they can produce representations of remote events and indicators. This relation could be called *augmentation*, combining an embodiment relation and a hermeneutic relation. In a policing context we may see this kind of technology emerging with the rise of wearable technologies but we can already see them if we consider complex video surveillance systems. These kinds of systems allow officers to both look through their screens as they monitor the roads, while at the same time they display all kinds of indicators on the same screen (e.g. vehicle information such as speed, ownership or legal status, etc.) that require officer's interpretation.

Of course, the relations with artefacts can be simultaneously characterized by a multitude of relations from this taxonomy. For instance, we can often get lost in activities and embody the computer screen in our experience. Simultaneously, we can interpret various numbers on the screen (e.g. temperature in a weather application) and interpret it to mean "it's gonna be cold". Even more, if we really try, we can simultaneously pay attention to the humming noise of the device and realise how annoyed we are by it. All kinds of relations exist simultaneously and their separation becomes an analytic exercise. Still, it helps us to conceptualize the rich and diverse ways in which technologies mediate perceptions, experiences, decisions and actions.

Besides charting types of relations, the vocabulary of technological mediation is also mapping the kind of influence that technologies can have on human users. Tromp et al. (2011) identify the impact of technologies in terms of visibility and force, on a continuum between 'hidden' and 'apparent' and between 'weak' and 'strong'. On one end of the spectrum, strong and apparent influences can be called *coercive*. In the policing context we can think of access control mechanisms in information systems that require officers to have the proper credentials in order to access classified data (or make certain fields invisible). On the other side of the visibility spectrum we can find *persuasive* technologies. This kind of technology show their influence explicitly, without being overpowering on the user. In the policing context, persuasive technologies can be found in reward mechanisms that give police officers more credits/points when they achieve milestones. Without forcing the officers, persuasive mechanisms nudge them towards certain behaviours, patrol routes or sequences of action that can protect safety and other professional norms. Technologies can also have more soft and subtle influences, which work by *seducing* the users. The influence is hidden as people are generally not aware of the ways in which the technology shapes behaviour. For instance, police forces often place a coffee machine in a central place in the organization, at the junction of more departments, teams or units, to stimulate social interaction. A fourth type of influence in this taxonomy is both strong and hidden. Tromp et al. (2011) call it *decisive* or *implicative* because it exerts influence without this influence being noticed. In the policing context we can find cubicles that separate offices in a control room, for instance, effectively enforcing work division.

Technological mediation and ANT

The approach to study technological mediation presented above differs from the mediation of action, as understood by Latour. Investigating human experience, this approach does not maintain the strict symmetry between humans and non-humans that ANT aims to keep. A postphenomenological analysis of technological mediation takes the standpoint of the human being, experiencing, interpreting or perceiving, whereas in ANT the analyst can change the standpoint between humans and non-humans to chart the configurations and network of relations. Still, Verbeek and Ihde identify similarities between the styles of investigating technological mediation. Both approaches are materially sensitive, recognizing the agency of artefacts, and both have abandoned the 'subject-object' dichotomy, conceptualizing humans and technologies as co-constituting each other.

Verbeek and Ihde argue for complementarity rather than competition between the approaches (Verbeek, 2005; Rosenberger and Verbeek, 2015, xv). "What postphenomenology contributes to actor-network theory is the situated perspective, the perspective 'from inside out', thanks to which part of the perceived associations and translations can be more closely analysed in terms of experience and action, existence and meaning […]. Correspondingly, ANT contributes to postphenomenology a way to elucidate the networks of relations that allow entities to be present" (Verbeek, 2005, p. 168).

For the purposes of this chapter, the vocabulary of technological mediation becomes richer through this complementarity, offering a repertoire that can capture more nuances and dimensions of contemporary technologically mediated security practices. As Annemarie Mol suggests, "a contribution to ANT gently shifts the existing theoretical repertoire. And then, as the theoretical repertoire shifts, it becomes possible to describe further, different cases, and to articulate so far untold events (relations, phenomena, situations)" (Mol, 2010, p. 261). If we want to understand the complex work of technologies in contemporary policing, we need to understand the networks of relations between officers, artefacts, designers or policy makers. At the same time we need to understand what practitioners experience in their technologicallymediated work, how do they perceive criminal phenomena through a screen, or what does it mean to 'have a suspect' when they read indicators from an information system or hear a sound from an automated alert.

5.3.4 Investigating digital infrastructures

From this perspective, it should be clear by now that (digital) infrastructures are not merely applications of mathematics and physics but culturally contested artefacts, with social, ethical and political charge and in their turn are shaping, classifying and ordering the material and social realms alike. We can feel their force instantly if we would try, for instance, to ignore the sign posts at supermarkets indicating cash/pin only or on the streets indicating types and heights of allowed vehicles. Already implicit in these examples is that infrastructures incorporate systems of classifications, rules and procedures that often embody a highly normative charge (Bowker and Star, 1999, p. 4). In order to understand how these networked infrastructures are made and how they are often rendered invisible and taken-for-granted we need a type of 'archaeological approach' (Foucault, 1976) to 'dig up' the origins and consequences of these bureaucratic and technological infrastructures (Bowker and Star, 1999, p. 5).

But how to think of the kind of machine-learning algorithms that cannot be easily traced back to an algorithmic step or design decision? These kinds of algorithms, featuring in predictive policing and many more areas of urban ecosystems, are thus challenging our methodological assumptions. An archaeological approach, with its focus on human activities in the past, assumes and looks primarily for anthropogenic explanations. In this respect we could benefit from expanding and deepening the scope of investigations and bringing in the methodological and conceptual repertoire of *geology* to complement archaeology in our understanding of technological infrastructures. I have shown elsewhere how we can employ a *sedimentological* repertoire to understand phenomena with various degrees of dynamism and depth such as settling, debris, deposition, accumulation, sedimentation, explosion or volcanism in digital infrastructures (Niculescu-Dincă, 2018). Of course, human activity plays various roles in design processes. Still, we may need to be ready to account for a whole set of processes that may not be easily traced back to an initial human activity.

A geological mindset and vocabulary in the study of technological infrastructures gently shifts the theoretical repertoire and might prove a more adequate starting point in researching algorithms without assuming particular distributions of responsibility between the role of humans and non-humans in producing the outcomes. At the same time, geology retains the method of 'digging up strata' to understand the origins of our bureaucratic and technological infrastructures. The planetary scale of digital infrastructures and the far-reaching depth of these systems in our societies, with large software stacks running billions of lines of code and massive data flows running (through) our cities, warrants a new set of metaphors to help us come to grips with the spread and depth of these global phenomena. Moreover, bringing closer the repertoires of geology and technology is a timely step when we contemplate the recent efforts ‘from the other direction’ of the bridge, to expand the geological vocabulary with terms such as the ‘Anthropocene’ to account for human activities and the impact of our technological infrastructures on the earth’s geology (Crutzen and Stoermer, 2000). With this conceptual expansion, even if not yet officially accepted, geology cannot be understood as a domain outside social, political and ethical influences thus warranting the conceptual undertaking to bring these disciplines closer.

A step in this direction it to expand our vocabulary with notions that can help us think about phenomena at this intersection. For instance, *sediment traps* is a rich notion that can be employed in a descriptive and methodological sense. On the one hand, sediment traps refers descriptively in geology to topographic depressions where sediments can accumulate. On the other hand, it refers in oceanography to scientific instruments that can be used to probe aquatic systems, usually oceans, to analyse particle samples. Of course, we need to test and adapt the notions of this interdisciplinary vocabulary.

In a descriptive sense, it can help us think about the ways in which software can accumulate sediments that thicken, become invisible and get taken for granted at runtime. For instance, this can be a design decision but also bias in a training data set that strengthens over time. While some of this bias can be traced back to the training data set, other outcomes cannot be accounted for by a design decision but they stem from accumulations in the layers of algorithmic code. In a methodological sense we can employ the notion of sediment traps to think about the ways in which we can probe and analyse the mesh of sensing infrastructures and the multitude of algorithms running in our cities. Once made available, it might be a gargantuan task to constantly review all algorithms. Therefore, we can think in terms of sediment traps to probe and analyse samples of data and algorithms and request further transparency upon finding ‘explosive’ or ‘toxic’ sediments.

5.4 Mediating perception and action

So, how can we understand the ways in which police officers engage with sensing infrastructures? How are particular ANPR systems and smart camera infrastructures *mediating* police perception and action in specific situations? This section discusses two vignettes. One is about the most common and widespread uses of the technology: checking traffic against predefined reference lists. The other is about the more recent uses of the technology in conjunction with profiles of suspicious behaviour. The first draws on empirical data I collected with a road policing unit during ethnographic research in a constabulary in England. The second draws on data from the control room of a police organization in The Netherlands. The analyses of both vignettes show the active mediation of perception and action of officers when they engage technology, sometimes weaker, sometimes stronger, more hidden or apparent.

In the constabulary where I performed this study the police made use of a large network of fixed ANPR cameras together with mobile cameras mounted on a fleet of marked and unmarked police vehicles. At the beginning of the shift, I was introduced to officers Jim and Morris, from the road policing department. They were preparing for their shift and they explained me the features of their vehicle and the capabilities of the ANPR system:

Officer Jim: "*Jump in I'll give you a quick tour. Ok, obviously we´ve got the police lights and everything [...] an air horn, like a truck horn if people don't see us [...] radio and everything else is standard. Then the screen: we have several different items on here. We have a mapping system, video capability as well, and ANPR. [...] The idea is to read number plates. It can read number plates like that* [officer snaps his fingers]. *It should give a 'hit' signal and who owns the car. So we can see who owns the car, see if it's got MOT on the car, which means if it's roadworthy and whatever year it has to be checked, the size of the engine, car type, etc*."

After this short introduction we took several hours of driving, with the ANPR system turned on. One of the situations I experienced happened soon after. The situation provides an interesting starting point for an analysis that looks at the mediating role of technologies and their interaction with the officers in processes of enactment of suspicion. The officers decided to stop a car for investigation and they explained to me why they did so while they were pulling the car over:

Officer Jim: *"This Volvo has got four people in it and they just looked a bit..."* Interviewer: *"So this wasn't a hit"* [triggered by an ANPR list]?
Officer Jim: *"No, not a hit, no."*

Immediately after, Officer Morris intervened:

Officer Morris: "*Or actually it was, over here, 'no taxes' on the middle lane*. [Officer Morris points to the screen]"
Officer Morris [asking the back office for confirmation and potentially additional information]: "*What's the man's name and where was he from again please? Newcastle?*"
Radio in [from the back office]: *Owen Dumitru* [Romanian name].
Officer Morris: *We get a lot of problems with Romanians and Eastern Europeans travelling the country. This car is registered on a Romanian from Newcastle*.

The officers walk towards the stopped car and ask the driver to step out. After a few seconds, the front passenger steps out and opens the back trunk of the vehicle. One of the officers checks the interior carefully while the passenger awaits impatiently. After performing the search the officers consult for a moment. They turn to the nervously looking driver and decide to let him go, returning afterwards to the police vehicle.

Interviewer: *"So what was the problem?"*
Officer Jim: *"It's not a problem in the end."*
Interviewer: *"So they had paid the taxes in the end?"*
Officer Jim: *"Yes, the tax database is often wrong. Tax is one of the unreliable ones."* Officer Morris [whispering for himself]: *"Every time"* [then louder]: "*It used to be a very good indicator for 'no insurance', but now it's not so good."*

This situation helps to bring to the fore the mediating role of technologies in this police process. On the one hand, the quote shows that technology did not *coerce* the officers or rendered them into executants without responsibility. As we have seen in the dialogue, the officers initially stopped the car not because of the ANPR hit but because they assessed the passengers as ‘looking’ somehow suspicious. Unlike their colleagues in the control room, the officers in the car were able to look at the vehicle and assess both the screen information as well as the situation in the field.

On the other hand, the ANPR system subtly mediated officer behaviour. Taking the number plate as input, the ANPR system generated the name and nationality of the owners of vehicles on the road. Communication with the back office confirmed the information about the registered owner. Unlike with other vehicles in the ‘tax list’, they asked this driver to step out and open the trunk while they performed a close inspection of the vehicle. Being Romanian and traveling the country gave the officers extra incentives for verification which proved unjustified in the end. This situation is illustrative of what Norris and Armstrong argued elsewhere, namely that technologically mediated policing does not exclude target selection based on indices of race, age, appearance or demeanour (Norris and Armstrong, 1999). An identity attribute that would not be particularly sensitive in most contexts–nationality–reinforced in this case the officer’s categorical suspicion and rendered the Romanian driver vulnerable to the officers, enacting him as suspicious.

Still, this situation brings to the fore the need to investigate further how the perception and experience of police officers in control rooms are mediated by these technologies. Being further away from the situation in the field, they are bound to react only on what the system displays and they can only check pictures of license plates as captured by ANPR systems. The following vignette explores this situation. It draws on data gathered in the control room of a Dutch police organization during a special action in which they were monitoring the traffic at particular locations and trying to see how they could translate the findings into profiles that could be automated on the ANPR network.

It was a particularly busy day in the control room. Everyone was curious to see the results of monitoring the traffic at particular points in search for suspicious vehicles. From time to time a high pitched audible alert disturbed the room and bright colours flickered on the screen.

The officer responsible for ANPR was particularly interested to see the results. He had the task to communicate the results to the team on the roads. I asked him about his expectations for the results of the profiling project and his response was:

“*I think that when it is fully developed, it is easier because I won´t have to check it. It´s just BAM, the hit comes. Ok people: check it, it´s weird.*”

His reaction could be used to illustrate the way in which technologies mediate police work in control rooms. As the system runs the profiles on live traffic data, it automatically triggers an alert, actively emerging from the context of the officer’s experience. Once it brings it to his attention he interprets the alert as something ‘weird’. Of course, this does not necessarily need to lead to an arrest. Still, the quote shows that the officer in the control room expected these real-time profiles to deliver more than a mere indication but justifications for suspicion. His way of talking about it (i.e. the use of the interjection BAM) indicates the potential for the profile to strongly mediate his behaviour. He would have otherwise been inclined to perform an extra 'check' but (with the profile fully developed) he would delegate his trust to technology. In conjunction with the assertive visuals and strong audible alerts, technology tended to be trusted and profoundly mediate his perception of traffic participants.

However, being flagged on the screen as suspicious does not necessarily imply criminal behaviour or sufficient reasons for alertness. Technologies do not deliver a transparent and objective rendition of reality. Rather, they play an active role in enacting it. What it means to be a 'suspect' is partly what the screens in front of officers enact as such. Paradoxically, the better the profiles are (in delivering suggestions that turn out justified) the higher the risk to prescribe an overly confident suggestion for action. Therefore, an insight to take out from this analysis is that the less possibilities to understand the full situation (f.i. officers being far away from the field or only getting a few pieces of data to rely on) the less strong, coercive and confident the technology should be designed to perform suspicion. Rather than making similarly strong visual and audible alerts for every profile 'hit', the design of their intensity and assertiveness should correlate with the confidence and amount of information it relies on.

This analysis also implies the need to talk to not only officers in control rooms and in the field but also to designers and programmers, and analysing profiles. Profiles play an active role in the coordination between officers in action and police programmers and they have different meanings across these branches of the police. They are 'boundary objects' (Gerson and Star, 1986) and it is important to constantly investigate their design in order to prevent them "from becoming static and detached from practice" (Schakel et al., 2013, p. 6). This suggests that in addition to their role in mediating the perceptions and actions of officers we need to analyse profiles 'in the making' (Latour, 1987), 'excavating' the layers of their software code.

5.5 Profiles 'in the making'

So how do designers and programmers talk about and engage with profiling and sensing technologies? How do they translate police knowledge in software code? What are their assumptions and some the potential implications that sediment in this process? This section draws on interviews with profile designers and observations of programmers at work in the Dutch police. It explores the ways in which designers relate to sensing technologies and writing the profile code and shows their main motivations and meanings associated with these technologies.

The following quote comes from an interview with a lead designer of profiles. He explains how ANPR is used in their project as a sensor, together with an array of other sensors, in order to build profiles of suspicious behaviour. These profiles would capture various aspects of criminal phenomena such as locations, times, social networks or modus operandi that can be detected by sensing technologies:

"*We are looking for indicators. For instance, that theft is being planned or is being conducted right now. We know now from experience that about 90% of these indicators are only detectable by human beings. You see the conduct of a person, you see how they walk, what they wear. We can't always see that with sensing techniques. But 10% we can. [...] we try to find the things that we can manage digitally with ANPR cameras and other sensors like Bluetooth sniffers, GPS location detection and all kind of sensors".*

As an example of successful behavioural profiling he explains the detection of the so-called ‘canvas cutters’. These are thieves that steal from unattended trucks in parking lots by cutting their canvas in search of valuable goods. Their particular modus operandi is to hop from one parking lot to another–using a car that’s not known to the police–in the search for unattended lorries. To arrive at this knowledge, several branches of the police, such as traffic police and the local police, came together with gas station owners, parking lot administrators and more, to share knowledge about this criminal phenomenon. As a result, they realised that one way to tackle this phenomenon is to detect this particular driving behaviour in the stream of vehicles: moving between multiple parking lots in a short amount of time. The police therefore, used the ANPR cameras of parking lots and designed a real-time profile that triggered an alert when a vehicle performed this behaviour.

The example showed how the police can successfully tackle a complex criminal phenomenon without the need of persistent databases. Instead of storing all traffic data and engage in data mining, the police can build a model of a criminal phenomenon by sharing knowledge between various branches of the police. In this case, criminal investigators, local neighbourhood officers, traffic police and administrators of parking lots got together and created a model of suspicious behaviour. After knowing the behaviour to look for, they translated it into measurable indicators and inscribed it into the code of a real-time profile.

Therefore, it is argued that this way of working “reduces the impact of privacy invasion” (Schakel et al., 2013, p. 7) while still catching criminals red-handed. The data of most traffic participants is not stored in police databases or quickly deleted after the profile runs its code. Any potential further investigation, whether unauthorised searches, curious officers of celebrity whereabouts and more, would not have the data to start with in the first place. At the same time, the quote suggests that this way of working contributes to inferring suspicion based on behaviour and not on identity attributes. Therefore, it contributes to lessening the risk of problematic discriminatory police actions.

Of course, behavioural profiling is often a highly dynamic process where knowledge is gained and lost, as criminals change behaviour and modus operandi, rendering the indicators obsolete and the profile in need of an update. In contrast with the high expectations of the officer in the control room (discussed in section 2.4), the interviewed profile designer was well aware of this phenomenon and its potential risks.

“*So it is not 100% safe. […] it’s just an indication that something is going on. We see this guy driving up and down the parking places. That’s what we really see. Whether there is really a car burglary in this case we don’t know […] There are certain groups of vehicles that have the same conduct. We can white-list them (i.e. exclude the number plates of police vehicles from the profile), but a guy with a bladder problem…*”.

The quote shows that the designer is aware of the potential false positives generated by the profiles which can prescribe an alerted attitude about someone who, for instance, needs to go often to the toilet. In other words, he knows the technology is not delivering certainty. Still, as we have seen in the previous section, his doubts and uncertainties tend to become black boxed at the operational level. The officer in the control room would have seen an assertive indicator that a potential theft is in the process and be inclined to send the nearest patrol to investigate the issue. Of course, we can only imagine from this point the surprise of ‘the guy with a bladder problem' coming out of the toilet to be welcomed by two alerted police officers. And, of course, in hindsight this situation can be seen as funny or at least acceptable.

Still, while investigating the process of designing profiles, new issues of behavioural profiling came to the fore. Despite advertising a lack of identity attributes in the process of behavioural profiling, identity attributes can be inscribed as well when necessary. The following quote, from an interview with a police programmer in the project, shows the practice of translating police knowledge into profile code. The programmer was responsible for redesigning a profile that should give a hit whenever a set of known and problematic number plates were performing a certain behaviour: returning to a certain location by night. In other words, a profile hit would indicate to the police that 'the old boys are back in town'. The police programmer explained that he translated the specific police knowledge into the profile code by connecting to particular sensors and building a minimum threshold of 50 points, calculated from several parts:

"*I made two indicators. Each one of them has 'a camera part' and 'a name and time part'. I'll explain.* [Each vehicle] *gets 20 points for passing by the cameras* [near the location], *additional 20 for passing it by night: then they have 40. When their name matches* [compared to a list], *they would get an additional 10 points* [and trigger the alert]".

Still, as he later mentioned, the 'name part' is problematic for both effectiveness and ethics:

"*In my opinion the profile is not really strong because maybe they like that place so much they come there to go to the toilet or to buy some food, for pleasure, and not to steal some stuff. I would prefer a profile with some more behaviour elements, for example these movements* [the programmer points on his screen to show a particular behaviour that could be suspicious]. *I don´t know if this one is accurate at the moment, but a few months ago it was accurate and at that moment this element was very valuable for us. At that moment we knew, we saw the boys and we saw them working".*

The quotes above can be used to highlight three issues related to combining sensing technologies with persistent databases in an aggregated profile. For one, even if the profile is meant to assess behaviour it also requires an inquiry to the vehicle registration database. Therefore, even if behavioural elements are key, the designer inscribed indicators regarding identity attributes but he doubts their effectiveness.

Secondly, once connecting to persistent databases, knowledge-based behavioural profiling may lose its announced advantages with respect to privacy and non-discrimination. The translation of identity attributes into profile code can be fraught with normative charge. Of course, in this case, the profile looked for a list of already problematic vehicles but the practice raises a point of concern. When is it acceptable that vehicles are assessed for going to a particular location? Which identity attributes are part of a profile and which parameter values are assessed? Through connections to persistent databases and other sensor networks, profiles can aggregate identity related attributes such as name, age and nationality. Without careful assessment, this can result in the close surveillance of categories of people that are unrelated to criminal phenomena. It is clear that we cannot simply rely on 'hard-coding' human rights protection (Koops and Leenes, 2014). Therefore, because of the dynamic character of how suspicion is enacted in the midst of these relationships, we need approaches that offer the flexibility to keep neither law nor technology as mere means to specified ends (Hildebrandt and Koops, 2010; Hildebrandt, 2011). Although technical solutions can reduce the risks associated with surveillance, at the same time these practices may create new ones.

Thirdly, the relations between criminal behaviour, ubiquitous sensors and organizational factors are increasingly unpredictable and rapidly changing while software infrastructures tend to trap sediments of prejudice. As the programmer mentioned, he doubted the current effectiveness of the profile in delivering valuable actionable knowledge and implicitly acknowledged the abovementioned risks for discriminatory actions. A recurring challenge for these issues remains the opacity of software (Pasquale, 2015; Kitchin, 2017) that increasingly enables decision-making in policing. Of course, to a certain extent opacity is constitutive and legitimate of policing practices. Criminals should not be able to easily anticipate their next move. At the same time, the software that enables police decisions is increasingly underlined by proprietary algorithms that can be seen as a competitive advantage. Thus, a case can be made prima facie not to make this kind of algorithms fully transparent to the public at large (but, at least presently, only to oversight bodies) (De Laat, 2018).

Even so, this line of argument contends that a higher level of transparency and a "spirited and open public discussion" about algorithms in general is still legitimate (De Laat, 2018). Especially when we contemplate how the perceptions, decisions and actions of policing practitioners are increasingly mediated in their daily routines by all kinds of software-enabled artefacts (e.g. automated alerts, risk profiles, rule-based suspicion algorithms, crime hotspots, etc.)–with implications for the effectiveness and legitimacy of urban security governance. An argument can be made that at least "over the years and the decades to come, they be made part of a public record available to us all" (Pasquale, 2015). The public needs to be able adequately conceptualise and relate to these entities that are profoundly affecting our cities and our societies in general. If we want an effective urban governance and if we aim for public acceptability of smart cities infrastructures, the public needs to be included in these debates.

However, from the examples discussed above we can see that adequately detecting criminal behaviour and simultaneously protecting human rights is not only a matter of algorithmic code but it depends on a whole set of socio-technical factors that need to be aligned. This way of working requires a concerted organizational, technological and imaginative effort. The following quotes from an interview with an officer some months later can be used to make this point:

"[The project] *hasn't seen much progress other than one camera will be installed near* [location] *to see what kind of cars are passing at this specific point. So thinking in terms of what kind of movements we expect to see this is not taking place yet. And therefore the discussion of where to deploy other cameras or other sensors is being postponed*".

"Availability of technology is not the problem but more the insight of what we can or must do with it seems to be the problem. Our imagination on how it can help us isn't growing as fast as I would like to see it. Changing old ways of working is hard. It'll have to take its time I guess".

His testimony illustrates both the promise and the difficulties that police officers face in engaging with sensing technologies in an effective and legitimate way. Behavioural profiling may offer better privacy protection and effective crime control, at least for a while, but *after* profiles become finished artefacts, ready to be inscribed in algorithms. Until then, the knowledge that can be used in building them can still be made by installing cameras 'to see what kind of cars are passing'. The process involves trial and error and the officer laments the slow progress. When ‘the availability of technology is not the problem’ and when perceiving the organizational arrangements as failing, monitoring seems to be the default option.

5.6 Conclusion

Knowledge-based behavioural profiling predicated on ephemeral sensor data streams holds the promise of effective policing actions while “reducing the impact of privacy invasion” and minimizing unfair discrimination (Schakel et al., 2013, p. 7). Still, this is not an automated discovery in which the police would find the relevant associations at a push of a button. This way of working requires certain conditions to deliver on its promises compared to storing and analysing data in bulk. These conditions imply that police organizations build profiles through knowledge sharing–and not thorough the use of persistent databases. It only works when many branches of the police do collaborate and continuously exchange knowledge rather than sharing data. In addition, they restrict themselves to behavioural profiling–and do not involve identity attributes–and the processing of data should be done locally (as much as possible) and not centralised. In short, sensing technologies and profiling algorithms are not flawlessly working surveillance machines that only select the perpetrators from the innocent, the bad from the good. Without concerted efforts to promote imagination in using sensing technologies in policing ‘old habits’ seem to die hard. Effective security governance while upholding our ideals of human rights in a world of smart cities *can* be achieved but with a heavy support for knowledge sharing between organizational, legal, policy and technological decision making, rather than just sharing data.

Still, engaging in this approach does not guarantee effectiveness and legitimacy. Police programmers are bound to continuously redesign profiles to catch criminals red-handed. This is done in order adapt to changes in criminal behaviour but also to prevent the erosion of the presumption of innocence when rising numbers of false positives get caught in their net. This process renders the profile design as a locus of analysis for both reasons of effective security governance as well as ethics. These evaluations depend not only on broad architectural choices to interconnect databases and sensor networks or not but on Boolean operators, algorithmic steps, and values given to parameters in suspicion and risk profiles. In other words, suspicion and the way it is enacted becomes a ‘gateway’ to the revocation of privacy. Preventing ‘unnecessary infringement on the privacy of people’ (Hoogewoning, 2006, p. 79) through technology design can also be read from the other direction: who *is* under suspicion can have their privacy rights legally lifted.

Therefore, an argument can be made that ‘digging up’ the layers of software code needs to be an ongoing endeavour just as technologies constantly and actively mediate their perceptions, actions and experiences of practitioners on a daily basis. By continuously tracing the enactment of suspicion in technologically mediated policing practices we can hope to counter more adequately some of the risks to police legitimacy while promoting an effective security governance within current and emerging forms of digitally infused urban environments. To be sure, the organizations where this study was conducted did have processes in place to evaluate profiles. Still, as this chapter suggests, the frequency of these evaluations did not keep up with the dynamics of police work and of criminal phenomena. At the same time, the normative charge of profiles was predicated on quickly changing parameter values and algorithmic steps.

Therefore, to promote an effective and legitimate security governance, requires the regular involvement of a broader set of disciplines with their sensibilities and theoretical insights in the evaluation of technologically mediated policing. This chapter showed how concepts and insights from Philosophy and Technology, Science and Technology Studies and Geology can be employed to 'dig up' and trace the ways in which suspicion is enacted in software code and in the broader materially-embedded policing practices. Moreover, it outlines and engages the conceptual framework of mediation theory to reflect on the ways in which the practitioners' perceptions, experiences and actions are mediated by sensing infrastructures and algorithmic profiles.

Acknowledgements

The author wants to thank Tsjalling Swierstra, Irma van der Ploeg, and Jason Pridmore as well as the police staff, municipality officials and technology developers for their generous collaboration and support for this research.

References

Akrich, M. (1992). The de-scription of technical objects. In W. Bijker, & J. Law (Eds.), *Shaping Technology/ Building society: Studies in Sociotechnical Change* (pp. 205-224). Cambridge, MA: MIT Press.

Akrich, M., & Latour, B. (1992). A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies. In W. Bijker, & J. Law (Eds.), *Shaping Technology/ Building society: Studies in Sociotechnical Change* (pp. 259-264). Cambridge, MA: MIT Press.

Bijker, W. (1992). The Social Construction of Fluorescent Lighting, or How an Artifact was Invented in its Diffusion Stage. In W. Bijker, & J. Law (Eds.), *Shaping Technology / Building Society: Studies in Sociotechnical Change* (pp. 75-104). Cambridge, MA: MIT Press.

Bijker, W. (2010). How is technology made?—That is the question! *Cambridge Journal of Economics, 34*, 63-76.

Bowker, G. C., & Star, S. L. (1999). *Sorting Things Out Classification and Its Consequences*. Cambridge, MA: MIT Press

Brey, P. (1998). Artifacts as Social Agents. In H. Harbers (Ed.), *Inside the Politics of Technology. Agency and Normativity in the CoProduction of Technology and Society* (pp. 61-84). Amsterdam: Amsterdam University Press.

Byrne, J., & Marx, G. T. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. In E. D. Pauw, P. Ponsaers, K. Van der Vijver, W. Bruggeman, & P. Deelman (Eds.), *Technology-led policing* (Vol. 2011/3, nr. 20, pp. 17-40). Antwerpen | Apeldoorn | Portland: Maklu.

Callon, M. (1987). Society in the making: The study of technology as a tool for sociological analysis. In W. E. Bijker, T. P. Hughes, & T. J. Pinch (Eds.), *The social construction of technological systems* (pp. 83-103). Cambridge, MA: MIT Press.

Chan, J. B. L. (2001). The technology game: how information technology is transforming police practice. *Journal of criminal justice, 1*(2), 139-159.

Crutzen, P. J., & Stoermer, E. F. (2000). The 'Anthropocene'. *Global Change Newsletter, 41*, 17–18.

De Laat, P. (2018). Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability? *Philosophy & Technology*(https://doi.org/10.1007/s13347-017-0293-z).

Ericson, R., & Haggerty, K. D. (1997). *Policing the Risk Society* University of Toronto Press.

Foucault, M. (1976). *The Birth of the Clinic: An Archaeology of Medical Perception*. London: Tavistock.

Gerson, E., & Star, S. L. (1986). Analyzing due process in the workplace. *ACM Transactions on Information Systems (TOIS), 4*(3, Special issue: selected papers from the conference on office information systems).

Haggerty, K. D., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 17.

Harris, C. J. (2007). Police and soft technology: how information technology contributes to police decision making. In J. Byrne, & D. Rebovich (Eds.), *The new technology of crime, law and social control* (pp. 153-183). Monsey, NY: Criminal Justice Press.

Hellemons, A., Beek, P. v. d., Malenstein, J., Goor, A. a. t., Kuijten, C., & Schewe, W. (2013). Final Report on DEPET (Dissemination all over Europe of know-how of Privacy Enhancing Technologies). Prevention of and Fight against Crime 2010. European Commission. Directorate–General HOME. Directorate F – Security.

Hess, K. M., & Orthmann, C. H. (2010). *Criminal Investigation* (9th ed.). Canada: Delmar Cenage Learning.

Hildebrandt, M. (2011). Legal protection by design: objections and refutations. *Legisprudence, 2*(5), 223-248.

Hildebrandt, M., & Gurtwith, S. (Eds.). (2008). *Profiling the European Citizen*. Berlin: Springer.

Hildebrandt, M., & Koops, B.-J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review, 73*, 428-460.

Hoogewoning, F. C. (Ed.). (2006). *The Police in evolution - Vision on Policing*. The Hague: Project Group Vision on Policing. Dutch Police Institute.

Ihde, D. (1990). *Technology and the lifeworld*. Bloomington: Indiana University Press.

Innes, M., & Roberts, C. (2008). Reassurance policing, community intelligence and the coproduction of neighbourhood order. In T. Williamson (Ed.), *Handbook of Knowledge Based Policing* (pp. 241-262). West Sussex, England: John Wiley & Sons.

Kamiran, F., Karim, A., Verwer, S., & Goudriaan, H. Classifying Socially Sensitive Data Without Discrimination: An Analysis of a Crime Suspect Dataset. In *Data Mining Workshops (ICDMW), IEEE 12th International Conference, Brussels, 10-10 Dec. 2012 2012* (pp. 370-377): IEEE. doi:10.1109/ICDMW.2012.117.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1-14.

Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society, 20*(1), 14-29, doi:10.1080/1369118X.2016.1154087.

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law. *International Review of Law, Computers & Technology, 28*(2), 159-171.

Latour, B. (1987). *Science in Action*. Cambridge: Harvard University Press.

Latour, B. (1988). Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer. *Social Problems, 35*(3 Special Issue: The Sociology of Science and Technology), 298310.

Latour, B. (1991). Technology is Society made Durable. In J. Law (Ed.), *A Sociology of Monsters: Essays on Power, Technology and Domination* (pp. 103-131). London: Routledge.

Latour, B. (1994). On technological mediation: Philosophy, Sociology, Genealogy. *Common knowledge*.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory* New York and Oxford: Oxford University Press.

Law, J. (1987). Technology and Heterogeneous Engineering: The Case of Portuguese Expansion. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The Social Construction of Technological Systems* (pp. 111–134). Cambridge MA: MIT Press.

Law, J. (2008). Actor-network theory and material semiotics. In B. S. Turner (Ed.), *The New Blackwell Companion to Social Theory, 3rd Edition* (pp. 141–158). Oxford: Blackwell. Law, J. (2009). Seing like a survey. *Cultural Sociology, 3*(2), 239-256.

Law, J., & Mol, A. (2001). Situating technoscience: an inquiry into spatialities. *Environment and Planning D: Society and Space, 19*(5), 609-621.

Leipnik, M. R., & Albert, D. P. (Eds.). (2003). *GIS and law enforcement: Implementation issues and case studies*. London: Taylor & Francis.

Leman-Langlois, S. (2012). *Technocrime, Policing, and Surveillance* (Vol. 3): Routledge.

Lyon, D. (Ed.). (2003). *Surveillance as Social Sorting* (Privacy, risk and digital discrimination). NY: Routledge.

MacKenzie, D., & Wajcman, J. (Eds.). (1985). *The Social Shaping of Technology: How the Refrigerator got its hum*. Milton Keynes, Philadelphia: Open University Press.

Maguire, M. (2000). Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Policing and Society, 9*(4), 315-336.

Mancuhan, K., & Clifton, C. (2014). Combating discrimination using Bayesian networks. *Artificial Intelligence and Law, 22*(2), 211-238, doi:10.1007/s10506-014-9156-4.

Manning, P. (2008). *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York and London: New York University Press.

Meijer, A., & Thaens, M. (2018a). Quantified street: Smart governance of urban safety. *Information Polity, 23*(1), 29-41.

Meijer, A., & Thaens, M. (2018b). Urban Technological Innovation: Developing and Testing a Sociotechnical Framework for Studying Smart City Projects. *Urban Affairs Review, 54*(2), 363-387, doi:10.1177/1078087416670274.

Mol, A. (2010). Actor-Network Theory: Sensitive terms and enduring tensions. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 50*(1), 253-269.

Neyroud, P. (2008). Policing and ethics. In T. Newburn (Ed.), *The Handbook of policing*. Cullompton: Willan publishing.

Niculescu-Dincă, V. (2018). Towards a Sedimentology of Information Infrastructures: a Geological Approach for Understanding the City. *Philosophy & Technology, 31*(3), 455-472, doi:10.1007/s13347-017-0298-7.

Norris, C., & Armstrong, G. (1999). *The Maximum Surveillance Society*: Oxford, Berg Publishers.

Parker, J. R., & Federl, P. (1996). An Approach To Licence Plate Recognition. *Computer Science Technical reports, University of Calgary, Alberta Canada, 591*(11).

Pasquale, F. (2015). *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press.

Pinch, T., & Bijker, W. (1987). *The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*: MIT Press.

Ratcliffe, J. H. (2008). *Intelligence-Led Policing*. Cullompton: Willan Publishing.

Rosenberger, R., & Verbeek, P.-P. (Eds.). (2015). *Postphenomenological Investigations: Essays on Human–Technology Relations* (Postphenomenology and the Philosophy of Technology): Lexington Books.

Sanders, C. (2006). Have you been identified? Hidden boundary work in emergency services classifications. *Information, Communication & Society, 9*(6), 714-736.

Schakel, J.-K., Rienks, R., & Ruissen, R. (2013). Knowledge-Based Policing: Augmenting Reality with Respect for Privacy Discrimination and Privacy in the Information Society. In B. Custers, T. Calders, B. Schermer, & T. Zarsky (Eds.), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases* (Vol. 3, pp. 171-189, Studies in Applied Philosophy, Epistemology and Rational Ethics). Heidelberg, New York, Dordrecht, London: Springer

Sclove, R. (1995). *Democracy and Technology*. New York: Guilford Press.

Tilley, N. (2008). Modern approaches to policing: community, problem-oriented and intelligence-led. In T. Newburn (Ed.), *Handbook of Policing* (pp. 373-403). Cullompton: Willan Publishing.

Townsend, A. M. (2013). *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: W. W. Norton.

Tromp, N., Hekkert, P., & Verbeek, P.-P. (2011). Design for socially responsible behavior: A classification of influence based on intended user experience. *Design Issues, 27*(3), 3–19.

Van Ooijen, C., & Nouwt, S. (2009). Power and Privacy: the Use of LBS in Dutch Public Administration. In B. v. Loenen, J. W. J. Besemer, & J. A. Zevenbergen (Eds.), *SDI Convergence. Research, Emerging Trends, and Critical Assessment*.

Verbeek, P.-P. (2005). *What things do: Philosophical reflections on technology, agency, and design*: Penn State Press.

Verbeek, P.-P. (2006). Materializing Morality. Design Ethics and Technological Mediation. *Science, Technology, & Human Values, 31*(3), 361-380.

Verbeek, P.-P. (2008). Obstetric Ultrasound and the Technological Mediation of Morality: A Postphenomenological Analysis. *Human Studies, 31*, 11–26.

Verbeek, P.-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*: University of Chicago Press.

Verbeek, P.-P. (2015). COVER STORY Beyond interaction: a short introduction to mediation theory. *interactions, 22*(3), 26-31.

Whelan, C., & Dupont, B. (2017). Taking stock of networks across the security field: a review, typology and research agenda. *Policing and Society, 27*(6), 671-687, doi:10.1080/10439463.2017.1356297.

Williams, V. S., & Williams, B. O. (2008). Technology applications: Tools for law enforcement. In J. Ruiz, & D. Hummer (Eds.), *Handbook of police administration* (pp. 165-173, Public administration and public policy). Boca Raton, London, New York: CRC Press, Taylor& Francis Group.

Wittkower, D. E. (2017). Technology and discrimination. In J. C. Pitt, & A. Shew (Eds.), *Spaces for the Future: A Companion to Philosophy of Technology*. New York: Routledge.