Policing Matter(s)

Policing Matter(s)

Policing Matter(s)

Towards a sedimentology of suspicion
in technologically mediated surveillance

Dissertation

to obtain the degree of Doctor at Maastricht University,

on the authority of the Rector Magnificus, Prof. Dr. Rianne M. Letschert

in accordance with the decision of the Board of Deans,

to be defended in public

on Wednesday, September 28th 2016, at 14:00 hours

by

Vlad Niculescu-Dincă

born April 22nd 1978

in Bucharest

Supervisor:

Prof. Dr. Tsjalling Swierstra

Co-supervisor:

Dr. Irma van der Ploeg

Assessment committee:

Prof. Dr. ir. Harro van Lente (chairman)

Prof. Dr. Monica Den Boer, Politieacademie, Vrije Universiteit Amsterdam

Prof. Dr.ir. Peter-Paul Verbeek, University of Twente

Prof. Dr. Sally Wyatt

ISBN: 978 94 6159 582 9

The research leading up to this book has received funding from the European Research Council under the European Union's Seven Framework Programme FP7 2007-2013 / Grant. No. 201853

The printing of this dissertation has been financially supported by Maastricht University
Printed by DataWyse BV, Universitaire Pers Maastricht

Cover image by Steven Michael: "Blue eyed circle of sand". A concretion/sedimentary rock formation at Shore Acres State Park, Oregon.

CONTENTS

Acknowledgements

A book about such a vast area as policing with one author on its cover may look a bit… suspicious. This book you are about to read received the help of many people and organizations. They contributed in numerous ways to the shaping and sharpening of the text you hold in your hands or that you read on your device. These professionals, colleagues, scholars and friends helped me with direct feedback, with moral support, with engaging discussions, with harsh comments or with warm embraces. I will try here to mention them all.

First and foremost I want to thank my promoter, Tsjalling Swierstra. Our relation goes back in time to my master years at the Universtiy of Twente. My passion for reflecting on the relation between technology and society was carefully nourished by Tsjalling during the courses I took with him and within our mentoring relation. Later on, during the PhD years, our discussions moved to new levels of engagement in his office at Maastricht University. Throughout these years, Tsjalling, you have been not only an efficient promoter but also an inspiring mentor. You helped me in the crucial moments of the writing of this book with pertinent comments and always pragmatic suggestions. This book could not have been finished without you.

I also want to thank my co-promoter, Irma van der Ploeg for her contributions throughout these years. Her initial guidance at Zuyd University Maastricht combined with her sharp feedback on the early versions of many of the chapters in this book. Irma, I always appreciated our musical encounters. We shared our joy for listening to the Bălănescu quartet and you introduced me to the work of Simeon Ten Holt. Thank you for this! Listening to these composers was a major factor that helped in the process of writing this book.

Equally important, I want to thank Jason Pridmore, the senior researcher during the DigIDeas project. His friendly availability and knowledge about surveillance were important factors that contributed to the success of this project. Jason, your funny and easy going style, combined with your insightful reflections and your teaching experience, always brought light. This project could not have been carried out without you.

I also want to thank my colleagues during the DigIDeas project, Isolde Sprenkels and Karolina Owczynik - La Fors, as well as Govert Valkenburg and Annelies Falk. Dear colleagues, thank you for sharing with me many joyful moments, for commenting on each other's work and for your moral support throughout these years in Maastricht. As you know, performing PhD research and writing a dissertation can often be a lonely experience. You have been there when I needed it. A warm thank you to each and every one of you.

Before writing this dissertation, the empirical research that stays at its basis could not have been done without the generous and friendly cooperation of so many policing professionals. I want to thank every officer, field agent, analyst, programmer, manager and police chief that I talked to in England, in The Netherlands and in Romania. Whether in the field or at the back-office, on the beat or at the coffee machine you have generously collaborated with this project, talking about your practices and sharing your challenges. Thank you for your professionalism and openness.

Putting together the empirical data during the early stages of this research gained a lot from the friendly feedback received from colleagues in the academic community. I want to thank the Netherlands Graduate School of Science, Technology and Modern Culture (WTMC) for

their great workshops and summer schools. In particular, I appreciated the Dissertation Days and I want to thank Koen Beumer and Adri de la Bruheze for their insightful feedback on an earlier version of a chapter in this book. Last but not least I want to thank the coordinators Willem Halffman and Teun Zuiderent-Jerak as well as Sally Wyatt, the academic director of WTMC.

I also want to thank the Centre for Ethics and Politics of Emerging Technologies (EPET) at Maastricht University for the valuable feedback and friendly collaboration I received throughout these years. Equally important I want to thank the Surveillance Studies Centre at Queen's University in Canada for their great Surveillance Studies Summer Seminars. In particular, I want to thank the facilitators Valerie Steeves and David Murakami Wood as well as David Lyon, the director of the Surveillance Studies Centre.

The shaping and polishing of many chapters of this book benefited from the feedback received at academic conferences and workshops. I want to thank the organizers of the Computers, Privacy and Data Protection conferences for giving me the opportunity to present my work several times in Brussels and in particular Ronald Leenes for coordinating the academic sessions at those conferences. I also want to thank the organizers of the Living in Surveillance Society workshop in Iași. In particular, I want to thank William Webster and Doina Balahur for the chance they gave me to present this work in Romania. Equally important I want to mention the Framing Screens workshop at the IT University of Copenhagen, and in particular Brit Ross Winthereik, Lucy Suchman and Helen Verran for their warm thoughts and for organizing a great event.

A special place throughout the years of this project is taken by the Romanian-Dutch community in Eindhoven and my friends in Bucharest. My friends, thank you for your generosity. Even if you may feel you did not literally contribute to the writing of this book, the project could not have been carried out and finished without your ongoing care. Whether through an embrace, a gentle word, a warm soup or 'just' a smile, you have made me feel supported by a strong community.

Another special place, particularly in the second part of this project, is taken by so many doctors and nurses in the Dutch medical system. Your professionalism in caring for our youngest daughter solved crucial problems during her difficult surgeries and, later on, when she came home among her sisters and family. Special thanks go to dr. M. ter Laak-Poort, dr. Noel Bauer, dr. Joost Nicolai and nurse Jaqueline Mantel. Your friendliness and ongoing help are invaluable for us to this day in being able to do our work and daily tasks while caring for her and her sisters.

Talking about family, this project could not have been done without the moral support of my family in Romania. I want to thank my mother, my (late) father, my sister and my parents-in-law for their support throughout these years. Special thanks go to prof. Cezar Mereuță for his advices and enduring confidence in my capabilities.

Last but definitely not least I want to thank my wife, Mateia. Mateia, words cannot capture well the unfailing faith, love and support you have given me. Thank you for everything and I am looking forward to share with you and our girls many more years to come.

Chapter 1

Introduction

This is a book about policing, suspicion and surveillance in our high-tech, information societies. In contemporary societies, we've come to rely heavily on digital technologies in our daily activities. Communicating through social media, browsing for information from our mobile devices, traveling through our increasingly smarter cities or shopping online in the comfort of our smart homes we daily produce significant amounts of data about our behaviour, our choices and our views. Some of this data we consciously produce ourselves, for instance through interactions across social media. But much of this data is produced automatically. Smart phones generate and communicate location data, automatic recognition systems identify vehicle number plates in traffic, travel passes and other machine-readable objects produce logs as we present them by sensor networks. Ubiquitously present, uniquely identifiable, built into the layers of our infrastructures and "*disappearing* from the consciousness of the user" (Gubbi et al. 2013, 1645), these networked entities seamlessly gather and communicate large amounts of data about the environment and ourselves.

On the one hand, we can hardly conceive our life without digital technologies. Their capabilities have made them wanted and often indispensable in our daily interactions. Moreover, ubiquitous computing power promises significant gains in convenience and contributions to solving pressing social problems: unburdening traffic congestion and reducing pollution in cities through intelligent transport systems and remote vehicle identification; enabling fast check-in for passengers through smart cards and predictable public transport with real-time tracking of vehicle fleets; enabling smart homes to react to personal behavioural patterns for reducing energy consumption. On the other hand, the capabilities of many of these technologies enable the storing of vast amounts of data. These digital traces are routinely classified and analysed in complex information systems and data centres. A wide variety of public and private organizations draws on them to enable decision-making about dynamic resource allocation, customised policies or targeted strategies. Monitoring social media, interconnecting databases or using sensor networks are already part of the activities of many public and private organizations. The sheer size and scope of this data combined with powerful search engines results in unprecedentedly detailed analysis of behavioural choices. Its prolonged storage and spread can therefore cast long term influences on our lives. Sophisticated algorithms mine large data sets to find surprising insights and identify patterns; for example trends in social media or in transport infrastructure usage. Based on these correlations, groups and categories are constructed and subsequently targeted within programs and strategies of various organizations.

Policing and law enforcement is one of the domains influenced by such technologies and practices. For instance, the dramatic increase in the use of surveillance cameras by police organizations or the employment and dissemination of geographic information systems in crime mapping and emergency control centres are only two pertinent examples of technologies that have significantly shaped the delivery of policing services. Since the turn of the century, the image of officers in big control rooms (monitoring large numbers of cameras, following suspects in real-time or analysing geo-spatial crime distributions on screen walls) has become iconic for 21st century policing.

Policing is, of course, being practiced by a variety of public and private bodies, including local policing agencies, neighbourhood watch patrols or private sector security. Still, the public, specialized and professional police remains one of the major actors in policing. This is in part because it is being granted monopoly in society to exercise force in many situations with potential for conflict, crime and deviance. Prima facie, we associate the public, uniformed police with, for instance, motorized patrols in traffic, riot police, criminal investigators or neighbourhood patrols. Still, policing also includes back office professionals, analysts and

control room staff with dedicated access to a whole set of information infrastructures and the legal clearance to monitor them. And with the technological developments announcing ubiquitous identification, new opportunity for policing is opening up.

On the one hand this opportunity is fostered by changes in the areas of crime prevention and crime control. A broad movement in policing promotes a shift from reactive, investigative approaches towards more proactive styles (Ratcliffe 2008, Tilley 2008). While reactive policing aims to solve committed crimes, proactive policing aims to strengthen the preventive character of policing. In this approach, policing involves practices such as behaviour analysis to infer suspicion before an actual crime is committed or risk assessments rather than only post-factum identification of suspects. As I will detail in Chapter 2, a constant of this trend has been the increasing reliance on digital surveillance to enable the decision-making process. In a proactive approach to policing, surveillance often becomes the solution for crime prevention, expanding further by seeking out "new target populations that ostensibly require a greater degree of monitoring" (Ericson and Haggerty 1997, 615).

On the other hand, these practices are predicated on the development of powerful information technologies such as geographic information systems, data mining, internet and social media monitoring or intelligent video surveillance. These technologies afford the processing of large amounts of data from various sources such as road traffic, internet traffic or social media, and aggregate it with a variety of police databases (e.g. history of incidents or wanted persons) as well as non-police databases (e.g. vehicle register). This ensemble of technologies enables the police to engage in practices such as profiling, monitoring, crime mapping, predicting behaviour and early signalling, prompting interventions and more efficient resource allocation.

While information technologies promise to improve the speed and efficiency of the police in protecting us from criminal manifestations, they may also bring about problematic outcomes: erroneous interventions that are difficult to prevent, as databases often contain hidden partiality, ambiguity and error; discriminatory measures towards persons, groups, areas or communities, as algorithms often contain explicit or implicit, intended or unintended classifications based on identity attributes and socio-economic status; violations of personal privacy, as they facilitate easy access to the personal data of large numbers of people; erosions of the presumption of innocence, as they automatically generate indicators of suspicious behaviour before/without crimes being committed. Playing an influential role in police decision-making processes, information technologies can often contribute to redefinitions of deviancy and suspicion that call for critical reflection.

At the same time, many of the factors that play a role in these decisions are built in the design of information infrastructures: suspicion indicators, pattern recognition algorithms, profile rules, surveillance categories, police knowledge or strategic choices (along with the practitioners' conceptions of the world) are often invisible, featuring only in the layers of software code that enables technologies to work. Of course, in all these situations, technologies only play a part along a multitude of other (f)actors (e.g. field officers, mid management, higher management, organizational policies, regulatory and legal frameworks and others) that together produce the outcomes. Still, embodying a highly normative charge, these long and interrelated arrangements of technological, organizational and legal factors only add to the complexity of decision making in contemporary policing. If we want to promote a fast and efficient police while avoiding many of the problematic outcomes of policing practice we need to unpack these arrangements.

1.1 Research questions

Freedom from arbitrary arrest, from arbitrary interference with privacy, family, home or correspondence, protection against discrimination or the presumption of innocence are rights and freedoms inscribed in the Universal Declaration of Human Rights, the European Convention of Human Rights and repeatedly recognized in many policy frameworks and reports. However, in the context of rapidly changing innovations in technology and in policy, the nuanced understanding of the risks and challenges posed by technologically mediated policing often lacks detailed articulation. If fundamental human rights and values should be persistently upheld, if we want them to play an important role in shaping our future societies and if we want a police that is transparent and accountable in a dynamic, technologically-pervaded environment, this gap needs to be bridged.

From one direction of this 'bridge', the present book[1] aims to contribute with an analysis of the ways in which digital technologies are implicated in transformations of policing practice. This implies a study of their role in changing policing routines, shaping practitioners' perceptions and influencing police action. Therefore, one set of sub-questions derived from this goal looks at the ways in which technologies influence police decision; what roles do they play in processes of inferring suspicion; how do they influence practitioners' behaviour? In sum, what are the police doing with technologies and what are the technologies doing to them? The emphasis in this book falls on information technologies and practices of the public police, organized at local and state levels.

From the other direction, this book aims to contribute with an analysis of the ways in which the design of policing technologies is being shaped within socio-technical arrangements. If the problematic outcomes of certain contemporary policing practices partially stem from the normative charge of technologies, we should reflect on the ways in which norms get built in technology design. This implies asking what values are implicitly built in policing technologies; how do designs get their moral charge; how do values and norms get to play a role in the design of classifications, profiles or suspicion categories in police systems; how do the developers of technologies explicitly build values and norms in design; what are the ethical implications of the practice of translating norms and values into computer code?

1.2 Studying technologies in society

Engaging in an analysis of technologically-enabled practices, with potentially profound implications for social values and fundamental human rights, requires a sufficiently broad understanding of the relations between technology and society. In this respect, the book draws

[1] The research leading up to this book was part of the DigIDeas project, hosted at the Infonomics and New Media research centre of Zuyd University Maastricht and UNU-Merit/ Maastricht University, The Netherlands. The project has received funding through a starting grant awarded to Dr. Irma van der Ploeg from the European Research Council under the European Union's Seven Framework Programme (FP7 2007-2013)/ Grant. No. 201853. The DigIDeas project examined the social and ethical aspects of digital identities in the context of an increasingly digital world. The aim of the project was to increase understanding and awareness of the social and ethical aspects of digital identity management, as well as to contribute to the quality and the social and ethical acceptability of these technological developments.

on the body of knowledge developed for many decades in the fields of social studies of science and technology (STS) and philosophy of technology. As I will detail in Chapter 3, these fields of research have come a long way in conceptualizing the complex and intricate ways in which we interact with technologies, both individually and collectively, moving our understanding beyond our immediate explanations of the role of technologies.

One of these insights developed in the STS literature is that technology and society shape and construct one another, rather than one determining the other. In other words, it is difficult to speak of 'technical' and 'social' aspects in terms of pure entities or domains. It is more adequate to think of 'socio-technical ensembles'. On the one hand, as in the previous examples, the outcomes are brought about not only by officers but also by automatic algorithms, which compute, inform and suggest, influencing and inducing decisions; for instance in which areas to concentrate interventions, which groups to put under surveillance; which persons to label as suspicious due to their behaviour. These outcomes can have profound social influences: they can lead to arrests, provoke debates, influence laws, trigger protests and in general shape our society. This insight goes against our intuition that people develop and use technologies so people determine their outcomes. On the other hand, technologies would not work without designers, maintainers, laws, organizations and a whole set of other entities that contribute to their development, functioning and maintenance. This insight resists the tendency to see technology as developing autonomously, outside the reach of people's influences. Technologies, including those in policing, can be changed and are being shaped.

Implied above already, is the insight that technologies actively influence our day-to-day behaviour and actions and are not mere neutral tools for our clearly formulated ends. It is not only us that do something with technologies but technologies do something to us as well, and influence the ways we act. For instance, when we drive and we see a speed camera on the side of the road, we might be less inclined to press the gas pedal further. For those with a passion for speed this might even mean to deny who they are as drivers and alter their driving style. This is because accelerating might result in the camera automatically taking a picture and sending them a fine directly at home. The software of the camera has been programmed to take a picture when it detects cars whose speed exceeds beyond a certain legal limit. This was done in order to punish risky drivers (who can still choose to pay the fine and continue to speed), while placing it visible was done to discourage those drivers that might have considered speeding. In both cases the arrangement of a bulky, visible camera on the roadside, its automated software, hardware, cabling, and mailing infrastructure work together to try to influence drivers to slow down, aiming to improve safety on the roads. Therefore, this insight highlights that the technologies around us play a role in changing the way we drive, the way we act and, in general, the ways we relate and perceive the world and the ways we understand and perform our identity.

These insights have been articulated and developed in the literature of science and technology studies (STS) (Bijker 1995, Bowker and Star 1999, Callon 1987, Gerson and Star 1986, MacKenzie and Wajcman 1985, Pinch and Bijker 1987, Van der Ploeg 2005, Wyatt 2008). This field of research has proven fruitful in producing detailed accounts of technology in practice due to its 'theoretically agnostic' stance. That is, instead of starting analyses of technology with overly optimistic or overly pessimistic assumptions about their social role (e.g. technology brings about total surveillance or, contrasting, technology brings about unparalleled safety in cities) this approach leaves more room for studying the actual uses, offering a better grip on the issues at stake. Aiming to understand the details of how decisions are made in policing practices

aided by information technologies, the analyses of this book benefit from concepts and approaches developed in the studies of science and technology.

As I will further explore in section 3.3, Actor-Network Theory (Akrich and Latour 1992, Akrich 1992, Callon 1987, Latour 1987, Law 2009, Law and Mol 2001) offers a particular approach within this field, emphasizing a symmetrical consideration of the role of humans and technological artefacts. As we have seen in the previous examples, outcomes cannot be easily attributed to a single entity; either human or technological. In stressing the need to analyse symmetrically the role of human and non-human actors, this approach aims to avoid considering technologies a priori to determine social relations (whether for better or worse) or to reduce them to the clear-cut results of social processes (e.g. modern technologies are the result of capitalism). From an ANT perspective, actors, defined as entities that do things, should be conceived in relation with other actors for it is in these networks of relations and associations that they become what they are and do what they do.

Against this background, 'identity' is also conceptualized here as something relational, mediated, and dynamic, as opposed to something defined in essential terms (Rorty 1982), given a priori and ready to be expressed or registered. And with the growing amount of personal data that is being stored, processed and used within the systems of classification that pervade our contemporary information societies it is to be expected that processes of transformation of identity will also be influenced. Sometimes explicit and mostly invisible, systems of classification are powerful artefacts ordering material and social realms alike (Bowker and Star 1999). They pervade not only the area of policing but penetrate a whole array of processes of human life. We can feel their force instantly if we would try, for instance, to ignore the sign posts at supermarkets indicating cash/pin only, at public toilets indicating male/female or at borders indicating types of passports. Already implicit in these examples is that classifications are often built into infrastructures and procedures where they often embody a highly normative charge, shaping the way we understand and perform our identities (Bowker and Star 1999, 4). If identity is mediated by technologies, as we have seen in the above examples, it implies that it is also produced to some extent in these interactions with technologies.

In order to understand how these networked infrastructures are made and how they are often rendered invisible, 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, 5). As detailed in Chapter 7, this book move the argument a step further and proposes a geological approach to understanding software layers and information infrastructures. A *sedimentology of infrastructures* maintains the approach of 'digging up' strata that potentially encapsulate relevant deposits (for instance of prejudice) while simultaneously resisting a bias for anthropocentric explanations. Unlike archaeology, which studies human activities in the past, a sedimentology of infrastructures might prove here an adequate metaphor to study the role of both humans and non-human actants.

For instance, for the case of policing, the approach can help us to analyse how stronger or lighter monitoring and interventions, discriminatory practices or erosions of the presumption of innocence are being influenced not only by organizational arrangements or the practitioners' idiosyncrasies but also by *pockets of prejudice* accumulated within software layers. In order to understand the kind of problematic outcomes of policing highlighted above, we need to *drill* through the layers of our infrastructures and analyse the specific socio-technical entities that emerge from these networks of actors and relations (e.g. 'suspicion', 'suspects', 'problematic groups', 'cases'). This also implies that the normativity of technology would have to be located

within the interplay of (f)actors that constitute the socio-technical arrangements. As Van der Ploeg argues, this requires "an agnostic approach to what should be considered 'technical', 'social', 'ethical', 'legal', 'political', 'organizational' etc. issues; put differently, it means looking for the social and normative *in* the technical, the technical and material *in* the legal and the social, and vice versa and so on" (Van der Ploeg 2008, 7). In this case, it means going beyond discursive claims about neutrality of technology to potentially disclose issues of normative relevance embedded in technology design or taking value statements as empirical categories and analysing the way they are implemented in software code.

1.3 On technological mediation

With this analytical stance we can investigate the role of particular technologies in policing practices. For this we need a vocabulary that is rich enough to capture the variety of relations that practitioners have with technologies. In this respect, I draw from philosophical investigations in the social role of technologies and the vocabulary of technological mediation. For instance, a contribution of Actor-Network Theory to the vocabulary of technological mediation is a conceptualization of the way in which technologies relate to human action in terms of *scripts* (Akrich 1992, Akrich and Latour 1992). That is, technologies 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 eventually act. Actors are able to appropriate the text and give it new meanings, unintended by the script writers.

As I will further elaborate in Chapter 3, the vocabulary of technological mediation can help us to understand more of the complex, technologically-infused, practices of contemporary policing. When we study the role of technologies in policing we need to also conceptualize how they *mediate perceptions* of suspicious behaviour or of criminal phenomena, how they *mediate experiences* of officers working in technologically-pervaded environments and how they *mediate actions* at strategic, tactical or operation levels. For this I critically draw on the work of Peter-Paul Verbeek, who expanded the vocabulary of technological mediation by building on the insights of both ANT and the post-phenomenological approach (Ihde 1990). As I will elaborate later, Verbeek shows how the vocabulary of technological mediation can be applied to many other areas such as industrial design (Verbeek 2005), engineering ethics (Verbeek 2006, 2011) or interaction design (Verbeek 2015) to provide a rich account for the mediating role of technologies.

In Chapter 4, 5 and 6 I will show how technological mediation can be adapted to the context of policing practices. For instance, it can help us understand what does it mean to '*smell something fishy*' when police officers interpret indicators on a computer screen; it can help us investigate how police analysts, working from their computer desks, perceive a rise/decrease in criminal phenomena in a city; or how do road policing officers experience high-pitched sound alerts and flashy indicators (e.g. about '*a weird vehicle*') when they work in the enclosure of their habitable. We need to be able to conceptualize these mediations of perception and experience as these often play an important role in the decisions and actions of policing practitioners to put a person, a group or a category under surveillance.

1.4 Studying surveillance

Surveillance is, of course, one the main policing practices, especially in proactive policing approaches. The fast growth of surveillance in policing and, in general, in late modernity has made the study of surveillance more relevant than ever (Lyon 2003). As I will further elaborate in section 3.5, surveillance studies is a rapidly growing multi-disciplinary field aiming to understand issues of visibility and of 'looking'. These studies deal with a broad array of themes having political, social and ethical implications (Bogard 1996, Dubbeld 2004, Steeves 2012, Wood 2006, Zureik and Salter 2005). These aspects of the emerging field of study make it relevant for an analysis of normative issues at the intersection of technological developments and proactive policing practices.

Unsurprisingly, many concepts developed in surveillance studies have been often used in investigations of the area of policing (Marx 2009, Norris and Armstrong 1999). For instance, one of the biggest influences in understanding the work of surveillance from an academic perspective has been Michel Foucault's interpretation of the Panopticon prison design (Foucault 1977). Foucault's panopticon pointed at the ways in which the person is being constantly disciplined within power relations as it passes from one environment of enclosure to another (family, school, workplace, sometimes hospital or prison). In its circular design – in which the few guardians are watching from a central, obscured position – inmates are fully exposed in their lighted cells, having to assume constant surveillance. Foucault elaborated the panopticon as a multifaceted concept for understanding not only transformations in the penal system but of society at large.

Another aspect of contemporary surveillance has been articulated by Haggerty and Ericson. They draw from Deleuze and Guattari and propose the metaphor of a surveillance assemblage (Haggerty and Ericson 2000). This notion proposes to analyse surveillance as an emergent rhizome-like network, spread mostly underground and often sending out shoots from its nodes. Within this analytical framework, surveillance is not seen as being directed by one centralized entity but is polycentric with data flowing between nodes. These data flows, fostered by computerization and the vast growth of means of identification and classification are scrutinized, translated, categorized, aggregated and made ready for intervention. The surveillance assemblage invites us to see also the networked and non-hierarchical aspects of surveillance.

Consistent with an agnostic approach, the present book approaches surveillance also from an STS perspective. That is, in order to understand contemporary practices and innovations in policing, it does not approach surveillance with an a priori model on how should we understand police surveillance. This does not mean that concepts and metaphors developed in the literature of surveillance studies are not drawn upon, but the analyses in this book allow the understanding of surveillance to emerge from the networks of actors and relations. This approach has already been adopted in a growing body of literature in surveillance studies (Norris and Armstrong 1999, Martin, Van Brakel, and Bernhard 2009, Van der Ploeg 2003, Dubbeld 2004, Leman-Langlois 2012, Steeves 2012) and benefits from typical STS commitments and predispositions: empirical substantiation of claims, detailed analysis of phenomena, interviews and ethnographic observations.

1.5 Empirical data

With these concepts and analytical stance, the research leading to this book benefited from an empirical grounding. As explained in more detail in section 3.7 of Chapter 3, the analyses draw from ethnographic research I performed at the premises of various European police organizations, among officers, agents, cubicles, cameras, screens, vehicles, suspects and many other entities featuring in policing practices. The organizations that I visited engaged with both well-established practices and technologies such as crime mapping/crime analysis and geographic information systems (GIS) as well as with still emerging ones such as data mining, sensor networks, automatic number plate recognition (ANPR) or internet and social media monitoring. They were all employed in daily policing routines, involving digital identification and management of information related to suspects, problematic groups or to suspect behaviour.

Performing ethnographic research at multiple sites allowed for highlighting differences and sharpening contrasts. This was achieved through my significant immersion in the contexts that I studied and familiarity with the settings in the form of participant observations (in day and night shifts), in-depth interviews (of around 3 hours each) as well as casual conversations that I had with practitioners and designers (for instance during encounters at the coffee machine, in police vehicles or in control rooms). Additionally I analysed documents of these organizations that pertained to the design of their systems as well as policy documents and relevant reports. With these methods the study explored various police configurations and drew points of comparison when they emerged from the analyses.

1.6 Outline of the book

In these ways together, the chapters of this book analyse the role of information technologies in various policing models and practices. First, Chapter 2 gives an overview of contemporary policing models and styles and their association to information technologies: Community policing and its 'low-tech' practices, Compstat and its relation to geographic information systems, intelligence-led policing and surveillance technologies, and knowledge-based policing and its relation to automated profiling. This review of policing literature includes a brief historical account of the ways in which these influential policing models came about in the past decades. At the end of the chapter, the reader should be familiarized with the panoply of contemporary policing models and associated technologies.

Chapter 3 offers an analysis of the ways in which technology has often been rendered in the literature on policing. Drawing from insights from philosophy of technology, the chapter illustrates the influence, implications and limitations of several discourses on technology. It points out how some authors rendered technology as a tool for efficient police work or as instrumental for implementing organizational innovations in policing, while others gave it an almost autonomous agency, whether with a positive or a negative character. In-between these views the chapter lays out the analytical stance of the book. It explains the relevance of insights from science and technology studies (STS), surveillance studies and philosophy of technology in providing a more nuanced analysis of technologically-mediated policing practices.

The following three chapters explore various technologically-mediated practices at police sites across Europe. Chapter 4 draws on research at a local police station in Romania. It offers an analysis of practices associated to geographic information systems (GIS) as a widespread and well established technology in policing. The chapter demonstrates that rather than playing a mere instrumental role, technologies actively mediate the practitioner perception of suspects. It does this by analysing in a detail one example observation about the geo-positioning of a report about a suspect boy. This detailed analysis of a basic routine renders suspicion as a complex socio-technical construct, even in the seemingly simplest and widespread technologically mediated policing practices.

Building on the insights of the previous chapter, chapter 5 shows how technologies mediate police action. The chapter looks not only at the classification and geographic mapping of youth but also at more recent policing practices: proactive monitoring of internet and social media behaviour[2]. It draws on data in the Netherlands, where 'problematic youth groups' are under systematic police surveillance as part of comprehensive proactive approaches. The chapter shows that larger or small data gathering from social media is entailed by the ways in which youth groups are enacted as 'cases' and performed as 'problematic' in government discourses as well as in police systems (Niculescu-Dinca, Van der Ploeg, and Swierstra 2016).

Chapter 6 makes a transition from asking questions about the role of technologies in influencing the practitioners' behaviour towards questions about the design of policing technologies. It asks how do technologies get their value charge and in-built norms? In particular, it investigates how 'the idea of privacy by design' was translated in configurations of sensor networks and employed in policing practices. The chapter draws from data in both The Netherlands and England, where automatic number plate recognition (ANPR) technology is widely employed in road policing practices.

The chapter analyses the design choices related to storing all traffic data (police in England) and to selectively store data based on real-time profiles (Dutch police). This latter engagement with sensor networks, among which ANPR is seen in the police as one type of sensor, is regarded as a promising way to both identify suspect behaviour in big flows (of vehicles, ships, transactions, etc.) while being 'protective of privacy by design' for most of the other traffic participants. The chapter highlights how the profile design – with its criteria and knowledge production processes – becomes an important locus of ethical reflection concerning the planned engagement of sensor networks in police surveillance.

The analyses in these three chapters show various ways in which technologies actively mediate police perception of criminal phenomena, their decisions and their actions. Technologies turn out to be important factors in performing suspects, suspicious behaviour, situations, vehicles or groups. Entities that play important roles in influencing police decision, behaviour and action are software-enabled artefacts such as geo-spatial representations, risk profiles, classifications and algorithms. Their designs influence surveillance practices, privacy revocation, discriminatory actions and other choices with ethical implications.

The last chapter summarizes the findings and discusses a set of themes that cut across the empirical material. First, it discusses the role of technologies in processes of inferring suspicion. Drawing from the material of the previous chapters it shows a paradoxical solidifying effect

[2] A previous version of this chapter features in the book *Digitizing Identities. Doing Identity in a Networked World* (Van der Ploeg and Pridmore 2016)

induced by technologies in mediating suspicion and legitimizing surveillance. Despite the flexibility offered by code to capture a wide variety of situations, software-enabled artefacts related to 'suspicious' or 'problematic' entities contribute to solidify the practitioners' perception of those entities.

Second, the chapter discusses how this 'solidification' effect impacted police relations with communities, groups and categories of citizens. It shows how the design of policing infrastructures can accumulate 'depositions of prejudice' in a sedimentary process. These 'sediments' that trickle down in technological infrastructures tend to harden and become simultaneously potent and invisible. When they carry discriminatory potential, they contribute to eroding the trust between communities and the police.

Third, and finally, the chapter discusses more generally the relation between technology design and values. Drawing from the findings of the previous three chapters, it highlights the ways in which particular conceptions of values such as non-discrimination and privacy were implicitly and explicitly built in as well as influenced by technology designs. The chapter formulates some suggestions for designers and managers of policing technologies. It argues for the need and opportunity for a larger uptake of Value Sensitive Design in developing but also managing technologies in policing. By considering values up front in the design process, the approach can bring to the surface the latent ethical concerns of the designers as well as render more visible their own values and the elements of the decisions in front.

Still, the chapter ends by qualifying this suggestion. Building of values in design is a promising undertaking but far from a silver-bullet solution to avoid all problems in policing. Technologies work in complex networks of organizations, laws, policies and criminal phenomena in constant change. If we want to promote an efficient and transparent police as well as avoid the kind of problematic outcomes discussed in this book, we need to continuously analyse technologically-mediated policing practices in the socio-technical ensembles in which they feature. In this sense, the chapter proposes a geological approach and vocabulary to understand technological infrastructures and argues for a *sedimentology of suspicion* to dig-up potentially explosive '*pockets of prejudice*' that may have formed in our smart environments.

Chapter 2

A quick glance at policing

2.1 Introduction

A study of technologically-mediated policing at multiple police sites across Europe requires an introduction to policing as well as a set of justifications and a contextualization. This chapter provides these on several dimensions. On a conceptual dimension, it discusses definitions and distinctions made in the academic literature on policing. This short analysis serves to introduce the reader to the field of policing, to some of its main practices and their scope. Second, the chapter gives an overview of influential policing models since the mid of previous century. The emphasis is on their relation to information technologies of the time. At the end of the section, the reader should be familiarized with the panoply of contemporary policing models and associated technologies. The delineations in the last section provide the conditions of possibility for studying technologically mediated policing practices at several police sites within the European Union.

When we think of policing a diverse set of images come to mind: they may be of units of public order maintenance acting with batons, shields and helmets during protests or supporter clashes; we may also think of the officers on the beat, talking through their radio units with their colleagues in the control centre, while strolling through the neighbourhood. Yet again images of motorized units on highways come to mind, stopping us for speeding or for not paying the road tax in time, after being prompted by their automated recognition systems. These images are probably dominant because the public, uniformed police is still one of the main actors in policing (Pakes 2010).

We may also think of private security guards, policing semi-private areas such as shopping malls, large housing estates or cinemas, or of local municipalities' patrols in parks, hospitals or schools. Policing can be practiced by the public police organized at state level, but also by a wide variety of local bodies, private sector security organizations, neighbourhood watch patrols, etc. as accounted by the studies on the plurality of policing (Button 2002, Rawlings 1995, Shearing 1996, Jones and Newburn 2006).

This does not mean that public and private policing are completely separate. Public-private partnerships are at work in a wide range of settings (Newburn 2001). For instance, we may think of the collaboration between privately owned businesses (gas stations, shopping malls, etc.) who share (video surveillance) data with the public police for catching 'fill and fly' thieves or shoplifters. These partnerships involve a distribution of responsibilities between policing bodies, as private security bodies have "limited powers to detain suspects or to stop vehicles" (Newburn 2008b, 108). Contrasting, the public police is invested with monopoly in society to exercise force in many of the situations involving transgression and breeching of norms.

So what is policing? Taking Reiner's definition as a backdrop, policing is 'an aspect of social control'; it 'occurs in situations with potential for conflict, deviance, or disorder'; it involves 'surveillance to discover actual and anticipated breaches', and it 'mobilizes sanctions to ensure the security of order' (Reiner 1994, 722). One observation to make when juxtaposing the general terms of this definition with the above images of policing is the distinction between policing and the police. Police bodies may vary widely in terms of their organization, functions, themes, priorities or jurisdictions. While they engage in a wide variety of activities, they may share styles, models and technologies for doing policing.

Another observation is that surveillance is a key practice in policing. From the walking patrols, scrutinizing the streets, to their colleagues in control rooms watching myriads of cameras or programming automated profiles to scan and detect suspicious behaviour, policing agents engage in surveillance in order to discover breaches of the law and/or impose sanctions. Already implied from the above examples, is a third observation. Much of the contemporary police surveillance is technologically enabled. From the 'low-tech' neighbourhood patrols, whose choices and decisions can be informed through their GPS-enabled radios to the back-office analysts, drawing from sophisticated data mining and pattern recognition, policing is increasingly imbued with information technologies.

This kind of technologically enabled practices have made many authors link technology to important changes in policing in the past century (Newburn 2008a, Manning 2008, Williamson 2008, Ratcliffe 2008). The review of this literature serves as a background in the next section for making an analysis of some of the changes that have taken place in policing models since the middle of the previous century. The focus of this historical account will be on their interpolation with information technologies.

2.2 An overview of policing models with an eye to information technology

Whether some authors render information technologies as driving forces for innovation in policing or others see them as instrumental for implementing organizational or conceptual innovations or simply as tools for bettering old ways of working, the issue of technology returns regularly in the literature on policing. Williamson (2008), for example, situating his analysis in the '50s United Kingdom, sees important changes in policing being triggered by three factors: the introduction of the motorized patrols, personal radios, and the creation of the 'post of collator'. The latter was a constable who coordinated the field activities from the police station, receiving, aggregating and disseminating information. Williamson goes on to analyse that these changes fostered an unintended, 'fire-brigade', reactive style of policing. Police officers tended not to go out of their cars, moving from one event to another, and in this way loosing contact with the communities, except for raids and stop-and-search when the situations required their swift and often brutal intervention. This shift is then partly credited for allowing the emergence of public discontent and riots in the decades that followed. Of course, public discontent may have had many other causes of institutional, cultural or economic character than just technological innovations. Still, this analysis is interesting in that it points towards the active role of technologies in shaping policing practice and broader social processes.

2.2.1 Community policing

Community policing grew out of an effort to reconnect the police with the public, answering to this loss of contact, attributed by Williamson and others to reactive policing. Aiming to police by consent, this managerial philosophy seeks to gain the support of local communities for police actions and priorities and promotes greater collaboration between the public and the police (Alderson 1977). It involves regular consultations with local communities to cultivate awareness to their particular characteristics and sensitivities (Skogan 2008). At the same time, community policing is associated with a decentralization of police hierarchy (Scarman 1982). Skogan and Harnett (1997) drawing from their experience with implementing community

policing in Chicago, emphasise that community policing is much more than a tactical plan. It is also an organizational strategy that redefines policing as a social service.

As easy as it is to state the goal of community policing to reconnect with the public, so difficult it has been to characterize its delineations in practice. Many authors noted the ambiguity of community policing deriving from the slippery notion of 'community' (Skogan and Hartnett 1997, Tilley 2008, Wisler and Onwudiwe 2009). Communities are often fractured, deeply divided, with different attitudes, including different implication levels with the police. Moreover, people often reinforce their belonging to multiple communities with different sets of values and practices.

Nevertheless, Skogan and Harnett (1997) also give examples of what community policing has been associated to in practice: opening up of small police stations in neighbourhoods, conducting surveys to measure community satisfaction, organizing public meetings and crime prevention seminars, forming neighbourhood patrol groups, conducting drug education projects and youth activities, patrolling on horses and bicycles. On top of these, Pakes illustrates this diversity of community oriented programs by documenting how Japanese community policing officers "advise on addresses, lend out umbrellas [or] may act as a lost and found office" (Pakes 2010, 49). This list can be easily extended by referring to the hugely diverse local contexts in which community policing has been implemented. As Skogan notes, its popularity became so big that "scarcely a chief wants his department to be known for failing to climb in this bandwagon" (Skogan and Hartnett 1997, vii).

2.2.1.1 Spread

The discourse and appeal of community policing achieved a global spread. In the absence of a unitary doctrine, community policing had many different versions and constant redefinition in each local context in which it was implemented. For instance, according to Wiesler and Onwudiwe, the movement had an important influence in the democratic transitions after the fall of the Berlin wall (Wisler and Onwudiwe 2009). However, this has not been an easy transition in Eastern Europe, as Haberfeld, Walancik and Uydess (2002) argue, documenting the implementation of community policing in post-communist Poland. While the demise of communist regimes officially removed direct political control, the police remained enmeshed in a long and difficult process of reconstruction.

Community policing became a tool for the reconciliation between police and society in these former totalitarian and authoritarian regimes. For example, in the post-communist Romania, community policing organizations were established in the mid '90s but under the authority of municipality councils. Set apart from the centralized national police, these organizations aimed at regaining the legitimacy of the police, long eroded by its predecessor, the authoritarian *Miliția*. As models for their programs, many municipalities looked for successful community policing in western countries, especially in the US, following a general societal tendency towards western models.

In The Netherlands, Punch, Hoogenboom and Van der Vijver (2008) identify four generations of community policing since the mid '70s. For them, the Dutch police changed from the 'reactive, rigid, distant and bureaucratic' officer before the mid '70s, through the 'long haired, nonchalant, lay-back style' of the late '70s and '80s towards the 'assertive, crime fighter' of the 21st century. As triggers for changes in the Dutch police they see not so much technological

developments but crisis events in the Dutch society: events such as the murder of Dutch politician Pim Fortuyn; the murder of Theo van Gogh, a film director, by a Dutch-Moroccan associated with a Muslim group; and the terrorist events that took place on 11th of September, 2001. Under the influence of these events and rising levels of criminality, they argue that at the turn of the century, the Dutch police are slowly sliding towards a central-repressive model, in contrast with the de-centralized and preventive orientation of much community policing (Punch, Hoogenboom, and Van der Vijver 2008).

2.2.1.2 Unequal policing and information gathering

Despite its influence and wide-spread adoption, community policing has also been criticized for assuming a high degree of harmony within communities. Still, in many diverse communities only some members actively engage in communication with the police and that often leads to unequal policing. In this way, only a part of the community influences the decision making at the expense of those that don't communicate with the police (Pakes 2010). And, as Tilley agues, it is usually the marginalized and disaffected, whose trust in the police was already low, that are not easily participating with the police in the agenda setting. The parts of the public that do engage become 'the eyes and ears' of the police gathering information on suspicious behaviour and communicating it to the police (Tilley 2008).

Community policing has not been usually associated to high tech information technologies for gathering and managing information – as can be intuited from the above examples of concrete community policing initiatives. However, the tendency to gather local information under the community policing banner took new forms with the advent of information technologies. Ratcliffe, for instance, notes that community policing entailed a greater flow of information about crime problems, with community police officers getting information about and from communities (Ratcliffe 2008). Tilley notes a report quoting some UK police officers who refer to community policing as meaning "electronic surveillance of shopping malls, enhanced traffic enforcement, and any police action that instils public confidence" (Tilley 2008, 377 quoting Bayley 1994, 104).

In the Dutch context, Punch, Hoogenboom and Van der Vijver also identify that information technologies were explicitly promoted in more recent generations of community policing. Especially the district managers embraced new information technologies to gain access to databases and inform beat officers in detecting local crime. This "more intelligent use of ICT" by the police was especially welcomed by residents in areas with many 'nuisance' offences – a constant source of irritation for Dutch citizens – committed by youth groups. Combined with the 'zero tolerance' policy, imported from the New York City Police Department, this gave a more assertive role to the police patrol, enabled by "swift use of information" (Punch, Hoogenboom, and Van der Vijver 2008, 72)

The trend to harness community intelligence is also analysed by Innes and Roberts, in relation to a new iteration of community policing in England, aimed at public reassurance (Innes and Roberts 2008). In their analysis, they document how a 'computer-based instrument' was devised to help officers elicit detailed information from communities about local crime problems. It was designed to systematically collect and aggregate data from members of the public in a format that allows practitioners to paint a richer picture of the issues and concerns of specific neighbourhoods. Combining this form of community intelligence with other crime intelligence sources, the police are thus in a better position to have a nuanced view of what is

happening in a certain area about people, places and events. This systematic way of gathering community intelligence from a diverse set of key individuals is regarded as a way to better control crime as well as to manage the concerns of communities and the perceptions of safety. At the same time it is a way to counter the bias towards those with 'the loudest voices' that community policing has been criticized for (Innes and Roberts 2008).

In sum, community policing initiatives worldwide vary significantly and address a broad range of community issues. They can coexist in practice with other police models, strategies and technologies that influence each local version. On the one hand, this variability is no surprise since communities and their needs differ from one place to another and so does what is implemented in the name of community policing. On the other hand, many programs are often placed together under the wing of its popularity. And it is no exaggeration to say that community policing became an international phenomenon in policing with influence in all corners of the world.

2.2.2 Compstat and geographic information systems

A particular place in this account of policing and information technology is taken by Compstat. While some do not place it as a separate police model (Tilley 2008), Compstat became an influential approach since the mid '90s after its association, albeit contested (Eck and Maguire 2000, Moore 2003), to significant crime reduction in the New York City Police Department. Despite its contestation, Compstat spread rapidly and became adopted in many police organizations throughout the world.

Compstat introduces an accountability mechanism in order to increase the efficiency of resource allocation towards crime control and ultimately to improve the quality of life for citizens. Compstat empowers and holds responsible police commanders to give rapid answers to crime problems in their areas. This is achieved by giving crime mapping and geographic information systems an important role in devising operational strategy. In weekly meetings, ranking executives meet with local commanders to discuss emerging problems. Therefore, Compstat is usually implemented for street crime, robberies, assaults, property crime and not so much for cross-border international crime. Compstat analyses are based on geospatial information and statistics gathered from each area. Accordingly, the police update their strategies and tactics in order to tackle crime.

Geographic information systems used in this approach basically include databases with spatially represented entities (e.g. crimes, incidents, suspects, weapons, groups) and software components that convert geo-coded data and superimpose it on the map of the city or the area. The information thus processed can be viewed on multiple layers. The images are able to cover the location patterns of a wide range of elements, from crime incidents, juvenile groups, offender activities to police patrol movements. In short, any element of interest in an area that can be represented spatially on a map can be included in a GIS.

Together with the spread of Compstat, crime mapping and geographic information technologies have been widely employed by police organisations worldwide, being considered "a powerful technological tool for spatial analysis" (Leipnik and Albert 2003, 3). The decisive step in this spread was fuelled, according to Ratcliffe, by the drop in prices of computer technology as well as by advancements in software and storage technologies. These had "a significant impact in introducing GIS in new areas such as policing" (Chainey and Ratcliffe 2005, 2). In this context,

geospatial analyses in the police witnessed a significant growth in the past decades, which went beyond its application in the context of Compstat.

The advent of geographic information systems gave a boost to a much older preoccupation in policing with spatial distribution of crime and efficient resource allocation. For instance, studies as old as the one of Shaw & McKay (Shaw and McKay 1931) show how mapping the activity of youth gangs in 1930s Chicago helped the police to understand movement patterns and thus allocate resources accordingly. This ongoing interest for studying spatial-temporal behavioural patterns is attested by a multitude of studies of the employment of GIS in police work (Eck and Weisburd 1995, Sherman 1995, Weisburd, Bernasco, and Bruinsma 2009).

Geographic information systems enable police analysts to engage in a wide range of practices at operational, tactical and strategic levels. These include command and control actions, where police units dispatched and guided in real-time on the map; monitoring delinquency groups whose activities over time are represented and analysed spatially and temporally; identifying clusters of crime or modus operandi in crime audits; plotting temporal diagrams representing the times in a day/week/month when a type of crime tends to happen; in short, visualizing information as *hotspots*, *hot-times* and *hotshots*. Moreover, GIS has been employed in more sophisticated analyses when combined with algorithmic data-mining to identify crime patterns and offender patterns in geographic profiling practices and translate them into intelligence.

2.2.3 Intelligence, knowledge and technology

This kind of sophisticated computerized analyses, combined with other intelligence sources on criminals, took centre stage in intelligence-led policing. A more recent model than community policing, intelligence-led policing developed within the broader context of the 'risk society' that fuelled the spread of all kinds of risk management strategies (Ericson and Haggerty 1997). These entailed a growth in demand for knowledge of the situation in order to efficiently direct resources. Maguire defined intelligence-led policing in 2000 as "a strategic, future-oriented and targeted approach to crime control, focusing upon the identification, analysis and management of persisting and developing 'problems' or 'risks'" (Maguire 2000, 316).

In the UK, intelligence-led policing was promoted through the National Intelligence Model, a business process and management philosophy to which every police force in the UK has to commit since its introduction in 1999. The movement of intelligence-led policing spread worldwide in the past decade, especially in the aftermath of the events on the 11th of September, 2001 in the United States of America. The emphasis on prevention of future terrorist incidents represented the argument fuelling the spread of intelligence-led policing in this context. It was thought that if enough information sharing was in place to 'connect the dots' and to signal a growing risk, this kind of disastrous events could be prevented rather than dealt with in a reactive manner.

Initially, however, intelligence-led policing grew out of an effort of the police to target prolific offenders and to cope with a supposed failure in targeting the sources of crime (Tilley 2008). Just like community policing, this model is aligned with a proactive approach to crime and aims to shift away from reactive, case-by-case policing. By contrast, however, it started from the idea that offenders act as part of networks and that the police can and do know a great deal about offenders and offending patterns to target interventions (Tilley 2008, 375). This was to be achieved by an active use of intelligence, focused on maximizing disruption to their organization and activities. In this approach, 'the computer enables better management of the

flow of information that the police receives about criminals, their behaviour, organization and lifestyle' (Tilley 2008, 389). In turn, this targeted focus is expected to lead to both improvements in crime control as well as in crime prevention. In short, crime can be reduced by having a tighter grip on those who produce it.

Ratcliffe (2008) argues that this initial framing of intelligence-led policing set the tone but that the model is in constant change. He argues that a view of intelligence-led policing as a 'technological effort to manage information about threats and risks' (Sheptycki 2005) does not do justice to this model that aims to define a way of doing the business of policing. In this broader understanding, intelligence-led policing is evolving into a managerial model of evidence-based resource allocation in the police and is associated with a holistic approach to all key areas of policing.

Irrespective of these changes in scope and definitions, intelligence-led policing places greater emphasis on information sharing and collaborative solutions and promotes the employment of a far wider range of intelligence products than the tables and maps of Compstat. These are used to picture trends, offer forecasts, order priorities and inform resource allocation. In this context intelligence-led policing also needs a broader view on intelligence to capture the reality of police work in the intelligence cycle (Ratcliffe 2008). According to Ratcliffe, drawing on Brodeur and Dupont (2006), intelligence is part of a continuum with data, information and knowledge. He criticises the view that restricts intelligence to 'information + analysis' and extends it to a data-information-knowledge-intelligence continuum that characterizes the intelligence cycle.

For example, 'data' can be the computer records of incidents about burglaries in a residential area. When a crime analyst assesses this data and recognises a pattern of new burglaries this becomes 'information'. If the analyst subsequently shares that information with a detective who remembers that a new pawnshop opened in the area and that he saw some known burglars around it, this collective awareness becomes 'knowledge'. It came from multiple strands of information which enabled the two officers to build a picture of the criminal environment and further make hypotheses about its causes and implications. Moreover, if they co-opt a senior officer and together decide to mount particular surveillance operations and technologies to gather more information, knowledge becomes 'intelligence'. Only in this situation, knowledge becomes actionable, something that does not always happen in the intelligence practice. Often information and knowledge remain locked in the heads of detectives and analysts or in information systems and do not transform into intelligence. These stages are distinguished in a more analytic way by Cope as data collection, data representation, interpretation, recommendation for action and evaluation (Cope 2008).

2.2.3.1 Stages

'Data collection' is the stage in which analysts pull together a range of data sources. These can include data from police databases and other institutions of the criminal justice system. According to Cope, this is a long and often difficult process where 'technology may assist' but often needs experiential knowledge, which is not always systematically recorded but only shared informally. Moreover, the process is influenced by the 'bedevilled form-filling by police officers and staff' and by technology that has not been designed with police analysis in mind. She argues, along with Ratcliffe, that "the growth of computer and information technology has supported the increasing demand for information' and that this entailed a tendency in which information is stored 'just in case'" (Cope 2008, 405).

A second stage is data representation. Also here 'technology has dramatically affected the capacity of crime analysis to chart key variables associated with crime data'. This led to a significant 'reliance of crime analysis on technology' which often involves the automation of this step (Cope 2008, 407). In this context, the role of police officers has increasingly become one of 'providers of risk-related information' (Ratcliffe 2008). In practice, this step is often plagued by the lack of relevance, low reliability, accuracy and timeliness of data and these factors often affect the quality of the analytical reports. For an explanation of this enduring challenge of the police, Cope identifies again the 'technology architecture that was designed to record and retain facts, not to develop and link inferences and contextual information to provide greater insight and enhance the ability to assess risk' (Cope 2008, 407).

In a third stage, interpretation drives the analysis towards inferences. Analysts may take a deductive or inductive stance towards the represented data to hypothesize about what has happened or to offer explanations of the patterns. For instance, an analyst may try to explain a particular crime distribution in an area. The analyst may need to link the reported crime concentration with knowledge about the development of a large entertainment or residential complex in the vicinity of an area with low income residents. According to Cope, this step is 'far more cognitive than technical and computer-driven'. These analyses often prove a difficult task in policing practice, both technically and intellectually (Tilley 2008, 392) given the quality of the data and the difficult task of making complex inferences about the environment.

The fourth stage involves recommendation for action and intervention. Analysts prioritize problems so that police activities can maximise crime reduction or prevention. This step requires analysts to get involved with local issues and to understand the environment in order to give meaning to local trends in crime. As crime analysis is usually 'office-based' and 'computer-driven', this is also a challenging task, generating friction with the action-oriented tendency of police officers on the street. This is where the recommendations of analysts, derived from computer generated information, can get discarded by officers in operational practice. According to Chan (2001), when officers do not value the information or do not trust the process of analysis, they are unlikely to respond to the analysts' intelligence products.

Evaluation is the final stage of the analysis process and aims to assess the impact of the police actions. While continuously monitoring crime, analysts are well placed in this phase to evaluate the results of particular police actions and their impact on crime levels. It is therefore a crucial phase in the whole analysis cycle that allows the possibility to inform evidence-based resource allocation and the police organization to adapt its policies accordingly.

2.2.3.2 Variations

Just like other policing models, intelligence-led policing did not impose globally a standard model of practice and it was interpreted with variations in multiple practicing contexts. Ratcliffe (2008), argues that 'one has to infer the meaning of intelligence-led policing from researchers and practitioners writing about it'. Against this background, intelligence-led policing gave rise to several spin-offs such as 'knowledge-based policing' (Brodeur and Dupont 2006) and 'nodal orientation' (Van Sluis, Marks, and Bekkers 2011) which coexist in practice, both with each other and with older policing models.

One of the practices of knowledge-based policing implies the modelling of police knowledge about crime into automated risk profiles (Schakel, Rienks, and Ruissen 2013). While much of analysis work in intelligence-led policing has a tactical and strategic scope, this interpretation of knowledge-based policing concentrates on the operational level. In this context, Schakel et

al. (2013) refer to a restricted notion of knowledge, emphasizing the role of know-how in addition to know-what in police practice (Orlikowski 2002). For example, they argue, 'knowing how to recognize a criminal in action may include the identification of a number of indicators'. When this 'knowing what' of indicators can be encoded in the profile of an automated recognition system, police knowledge of criminal patterns becomes actionable. This is, of course, 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.

The approach proposes to 'augment the reality' of police officers with software-enabled risk profiles. In the Netherlands, these profiles have been implemented to filter real-time streams of computer-synthesized data, such as car license plates (ANPR) in search for certain identity attributes and behavioural patterns. For example, automated profiles calculate the average speed of vehicles by measuring the times at which vehicles pass between two points. In this way profiles give a signal when they identify a pattern of speed driving.

Automated profiles can process data pertaining to all kinds of entities besides vehicles (ships, persons, transactions, etc.) and trigger signals when their criteria are met. This spin-off to intelligence-led policing emphasizes the role of police knowledge in selecting what is considered a risk and what information is acted upon. Instead of first storing data to derive knowledge from it, in this approach knowledge drives data storage.

This development comes against the background of other related concepts that were introduced in 2005 in the Dutch police: 'nodal orientation' and 'nodal police'. The concepts got their articulation in a policy document, *Police in Evolution* (Hoogewoning 2006) and refer to a general shift in policy towards a network orientation of the police (Bakker 2006, Van Sluis, Marks, and Bekkers 2011). The assumption of 'nodal orientation' is that the police – traditionally organized by geographical areas – needs to adapt to the networked structure of contemporary society and to the increased mobility of people, goods, money and information. Accordingly, the police should focus on flows (i.e. on infrastructures such as road networks, waterways, communication networks) and on nodes where these flows come together. These can be airports, seaports, highway junctions but also social media or business centres. The approach draws from the work of Manuel Castells and his idea that the rise of information technology has transformed society into a 'network society' (Castells 1996).

On one dimension, nodal orientation for the Dutch police translates into intensive 'surveillance of the infrastructure, or rather, of the flows of people, goods, money and information' (Hoogewoning 2006, 78). In this approach, "technology is expected to become increasingly important" and to enable a more proactive style of policing aimed at monitoring for suspect behaviour. In practice this is achieved through technologies that sense the environment and automatically recognize patterns. Besides monitoring the vehicle flow with Automatic Number Plate Recognition (ANPR) these strategies may involve monitoring servers of internet providers, scanning ships with radio frequency identification technology for the presence of particular materials or cargos, monitoring social media for discussions on riots or other subjects of police interest, or monitoring financial transactions for large sums of money to/from particular accounts. In all these examples, a signal of suspicious behaviour entails the "removal of anonymity and invisibility" (Hoogewoning 2006, 79).

On another dimension, 'nodal policing' implies that the police collaborate with other partners in order to deliver security. The police is an actor in the security network, along with other

actors with their own interests, duties and powers in supervision and investigation into suspect activities (Shearing 2005). This involves sharing of information between partners who collect and combine information in order to develop adequate interventions. For instance, traffic data collected by the police through ANPR can be combined with partner databases such as vehicle registers or municipal administration and, in this way, information can be obtained about the owner and status of a vehicle.

In sum, 'intelligence-led' and related styles of policing promote not only specific new tactics and ways of doing the business of policing but they are also associated to a significant employment of overt and covert "technical means" (Tilley 2008, 375) to producing data, information, knowledge and intelligence: analysis products gather data from a broad range of databases that are aggregated and algorithmically mined; geographical profiles describe emerging patterns and hotspots of crime; automated risk profiles filter suspicious behaviour aggregating multiple sensors. The information that gets fed into these processes is both received and actively sought by the police from their own databases, partner databases, and citizen informants. The role that information technologies are playing in policing made several authors see these technological innovations as the driving force reforming crime prevention and control and being linked to dramatic changes in the organization of the police (Chan 2001, Harris 2007, Byrne and Marx 2011).

2.2.4 Relations between policing models

The outlined models differ in multiple ways. They serve different purposes, have different priorities and are related to different organizational structures. Intelligence-led policing works with a top-down decision-making, in contrast to the community-based agenda setting of the community policing movement. Whereas community policing is built bottom-up and community centred, intelligence-led policing is hierarchical and uses crime intelligence to devise an evidence-based resource allocation. If community policing is justified by increasing the level of police legitimacy, especially among minority groups, intelligence-led policing emphasizes the law enforcement role of the police by focusing on offenders and disrupting their organization. While intelligence-led policing is similar to Compstat in terms of hierarchical organization and crime fighting, it differs significantly from the latter in the focused approach to combating offender behaviour and in its geographical scope.

In practice however, these models and others (e.g. problem oriented policing) often coexist in police services. Also the distinctions are often not that stark and elements of various models can be seen blending together with components of the others. To a certain extent this is explained by the diversity of criminal behaviour and also of communities, with their specific needs and structures. In other words, emergencies need to be addressed at the same time in which offenders need to be apprehended, communities consulted and order maintained.

Moreover, there are various situations of convergence in practice where the distinctions between models become even harder to maintain. For instance, we have seen in this chapter how new iterations of community policing make use of community intelligence and surveillance technologies. In those approaches, community policing initiatives effectively blend with crime intelligence sources, thus bringing intelligence-led operations to bear on community related problems. This link of community policing and intelligence-led policing can also be seen in crackdown strategies (Tilley 2008, 390). These strategies involve efforts of intensive enforcement to disrupt and deter offenders and their structures. The approach has longer-term

beneficial effects beyond the operation of the crackdown itself when community policing measures sustain the impact of the crackdown in the window of opportunity that is created.

2.3 Studying policing in a European context

We have seen so far several models for doing policing that are shared by many policing organizations. Despite their differences there are many commonalities and shared technologies employed in these organizations. Moreover, forces towards convergence in policing are at play at various levels in the context of the European Union (EU), not only in terms of shared technologies but also in terms of models, strategies and organization. For one, institutionalised police education at the European level contributes to the sharing of ideas and models and thus to the spread of commonalities between policing systems (Mawby 2008). Long before the EU, the Interpol provided a framework for senior officers to gather and exchange ideas and models of policing. Moreover, the European Police College was created in 2000 to encourage cross-border cooperation in police education.

Second, institutionalized transnational policing is increasingly at work at European Union level. This is manifest at various levels of operational cooperation between police forces of member states and through the creation of new and specialized European structures. After the Maastricht Treaty entered into force in 1992, marking the establishment of the EU, the setting up of Europol, which began its full activities in 1999, gave a significant boost to these collaborations. The scope of these supra-national police agencies in the European Union goes beyond the boundaries of the national state police.

Third, European-wide information systems are at work (and in development) to enable operational practices. These include the Schengen Information System (SIS), the European Police Record Information System (EPRIS), or the Europol Information System (EIS). Through such systems police agencies across the European Union routinely exchange information about suspects, wanted persons, stolen goods or documents in a context in which EU citizens are able to move and reside freely within the EU borders. These systems allow professionals to have a standardized way for exchanging locally produced data about crime events and suspects. Data sharing is encouraged by an emphasis in policy on interoperability, ease of information exchange, and multi-disciplinary cooperation (Den Boer 2011).

Fourth, processes of harmonization gained a broader spread with the enlargement of the European Union, the North Atlantic Treaty Organization (NATO), and the Schengen Agreement (Papanicolaou 2011). For instance, in post-communist Central and Eastern Europe this implied processes of decentralization and demilitarization of the police. The countries in this area generally took inspiration from older EU member states, resulting in the formation of new community policing forces and the adaptation of policing models. On the other hand, historically decentralized police forces, as in England and The Netherlands, have seen processes in the other direction. For instance, the Dutch police changed from 148 to 25 forces in 1993 being structured more akin to the police in England and Wales (Mawby 2008), and later moving towards a model with one police force with ten regional subdivisions. At the same time, the police in England and Wales witnessed also a slow process of centralization (Emsley 2008).

Fifth, the definition of common approaches and threats in security strategies and policy documents is another pressure towards convergence. This can be illustrated by the emphasis on

cyber-crime and terrorism in the European internal security strategy, calling for common responses of member states (European Commission 2010b). The internal security discourse permeates the institutional framework of the Area of Freedom, Security and Justice, which is a collection of policies aiming to promote cross border police cooperation among EU member states. For instance, the European Arrest Warrant – one of the outcomes of these policies – enables member states to arrest and transfer a criminal suspect or sentenced person to the issuing state.

These five points emphasise the forces that are at work in processes of policing harmonisation. Still, they do not suffice to conclude that there is already a harmonised policing at the European Union level. Several comparative policing studies (Mawby 1999, Pakes 2010) attempted to cluster police systems and analysed aspects such as the degree of centralization in decision making, the structure of the organization, or the degree of accountability and control. They point towards diversity on several dimensions. For example, many European countries have single forces, centrally organized (e.g. Denmark, Greece, France) while others share responsibilities between state and federal levels (e.g. Germany). Differences can be identified with regard to themes in policing, for example between Dutch and German policies on drug control (Chatwin 2003).

Nevertheless, studies that draw on data at more European police sites are possible and necessary for contrasting variations as well as for understanding transformations in contemporary European policing. On the one hand, as argued in this chapter, policing in the EU exposes significant commonalities. Despite differences in legal frameworks, priorities and organization, analyses are possible at the level of models, practices and technologies. On the other hand, such studies are acutely necessary against the background of an increasingly mobile and migratory citizenry, in which massive amounts of people, goods and information are able to move smoothly across the European Union, often in multiple cities and jurisdictions. At the same time, analyses of the role of information technologies in policing are especially relevant in the context of significant investments in technological innovation, promoted across European police forces (European Commission 2009b, 2010b, Den Boer 2011). Such innovations land on the organizational background of police services, which have often been shown to face difficulties in integrating new technologies in their processes, struggling with internal resistance and with the persistence of old routines (Manning 2008, Lemieux and Bales 2013).

It is thus becoming particularly stringent to analyse the role of information technologies in more detail, as contemporary styles of policing promote intense monitoring of infrastructures and raise a significant set of questions with normative charge. As argued in the introduction of this book, such analyses benefit from insights produced in the fields of philosophy of technology and the studies of technology and society, and would strengthen the body of literature that has already begun to do so (Leman-Langlois 2012, 174). The next chapter gives an account of these studies and their relevance for the research questions of this book.

Chapter 3

Studying technologies and surveillance in policing

3.1 Introduction

The previous chapter offered a review of some important contemporary policing models in the policing literature. As a focus, the chapter followed their relation to information technologies of the time. In this way, it highlighted several accounts of technologies, present in the discourses of the authors. For instance, technologies are 'powerful tools' (Leipnik and Albert 2003, 3), 'technical means' (Tilley 2008, 375) or 'computer-based instruments' (Innes and Roberts 2008, 250). 'Any modern society needs police who can make use of technology' (Byrne and Marx 2011, 32). Concerning their future role in policing 'technological control will march forward' (Bruggeman 2011, 160) and technologies have 'the potential to dramatically improve the efficiency and effectiveness of the criminal justice system' (Byrne and Marx 2011). Concerning their social role, 'the impact of information and communications technology has been changing the world that we inhabit' to the point that 'we already live in a surveillance society' (Williamson 2008, 5). Concerning technological change in the police, one other account claims that 'the IT train has jumped the rail tracks and has taken off on the information superhighway' (Chu 2001, 3), while another warns of 'the danger of self-amplifying technical means determining the ends and even becoming ends in themselves' (Byrne and Marx 2011, 34).

As illustrated above and in the previous chapter, technologies are both the necessary tools in the hands of police officers, enabling 'surveillance to discover actual and anticipated breaches', and simultaneously a self-amplifying danger threatening legal provisions and social values. How can we understand these apparently contrasting accounts of technology in the policing literature? Moreover, how can we understand their coexistence with other accounts in policing literature in which technology is the very solution to protect the public by preventing an "unnecessary infringement on the privacy of people who are not under any suspicion" (Hoogewoning 2006, 79)? As we have also seen in the previous chapter, 'technology is expected to become increasingly important in policing, especially high-tech applications' (Hoogewoning 2006, 79), detecting suspicious behaviour and sending automated alerts.

These accounts explicitly frame technology and its role in policing and in the societal context in which it features. Given the scope of their claims, the assumptions they make as well as their coexistence in policing theory and practice, these accounts invite philosophical reflection on technology. The quoted authors may display various nuances when accounting for technology in various parts of their work. I will discuss them here not to critically analyse their work but to illustrate the influence, implications and limitations of several discourses on technology. As this chapter will show, this influence is important. The way in which we talk about technology has implications for analysing consequences, for motivating or demotivating change and for the possibility of steering this change (Van der Ploeg 2003).

This chapter starts from these accounts of technology to analyse important themes in philosophy of technology. It then introduces important concepts developed in science and technology studies and more recent research in philosophy of technology that provide a more nuanced vocabulary of technological mediation. Next, the chapter introduces critical notions elaborated in the surveillance studies literature and shows their relevance for understanding technologically mediated policing. With these theoretical underpinnings, the chapter positions this book in a family of related studies and announces the research gap closed by the following chapters. Finally is elaborates on the methods pursued in this research, including the sites investigated, the sampling methods, data analysis, validation and ethical issues.

3.2 Common accounts of technology

Technologies are all around us, affecting our lives when we interact with them as well as in the background of these interactions. All kinds of technologies – from the 'simplest' matchstick to the most complex ones such as computers, mobile phones and satellites – have various degrees of influence on our lives. Some of them are 'nice-to-have' gadgets that we think we can live without but more and more technologies are life supporting – from energy, transport or communications infrastructures to medical technologies. At the same time, technologies tend to enter new domains of society and become constitutive of our practices and ways of life. It is therefore not a surprise that we develop vocabularies to come to grips with these entities that affect our lives so profoundly.

The same is the case with policing technologies. Policing practitioners also need to conceptualize their new and older technologies. As the importance of technologies is quasi-unanimously recognized as a defining characteristic of contemporary policing, the literature is pervaded by law enforcement, by legal and by managerial discourses on technology. This section discusses some of the most common conceptions of technology in policing literature and analyses their assumptions with the insights produced with the philosophy of technology. Are technologies obedient tools in the hands of policing practitioners or are they doing more than that? Are designers and engineers taking the wishes and needs of policing practitioners into account or is technology developing independently of their input, insights and knowledge?

3.2.1 "Powerful tools"

The first examples above frame technology as the means for doing policing more efficiently. 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 view on technologies as "tools that officers have to have in order to perform their law enforcement duties" (Williams and Williams 2008, 165). When technology is talked about, much of police officers' 'work-talk' involves a vocabulary that mainly covers the use, capabilities and powers of particular systems, equipment, machines or devices (Manning 2008).

Many more examples can be found in the policing literature: Technologies like geographic information systems are "powerful technological tools" (Leipnik and Albert 2003, 3). There 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, 165).

There are several implications of this conception of technology. Framing technologies, implicitly or explicitly, as useful tools renders them as means for realizing the user's ends, in this case, the ends of policing practitioners. This is the standard instrumentalist attitude, according to which technology does not entail consequences by itself but consequences are stemming from choices made by the user (Sclove 1995). The often evoked example to illustrate this conception is the gun that can be used in legitimate ways but also for murdering someone. The choice and its consequences depend solely on the intentions of the one holding and using the gun, and not on the gun itself; or so the argument goes.

From this perspective, technologies are rendered as passive, obedient in the hands of users. Technologies are neither good nor bad, as people use them for their purposes, which can be better or worse. Tools do not determine human action. 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, 169). In this framing, technologies are value neutral. Their moral dimension is given by their users. When they are not used, they do not result in anything, good or bad.

However, a corollary of this standard conception of technology has implication for understanding technological development. As this view does not give an active role to technology in producing the outcomes, bad or good, it tends to ignore or not properly account for the role of designers in contributing to these outcomes (Brey 1998). For example, the reasoning goes, how can we meaningfully hold Diesel accountable for the pollution that came about with the spread of cars and the use of the combustion engine? Of course, technology is developed by engineers and designers, but their choices are based on physics, mathematics or biological laws, and largely independent of society's priorities and values.

Therefore, the instrumentalist perspective tends to favour a view of technological change in which users and society at large cannot exert much influence on its design and development. Often associated with this view is a conception of technological development as an unavoidable progress. If society does not have much say in its development, technology moves forward in virtue of its internal dynamics, as science discovers new laws of nature or as technologists find ingenious ways to recombine existing discoveries and materials. These implications of our conception of technology have been theorized in the philosophy of technology literature as the themes of *technological determinism* and of *autonomous technology*.

3.2.2 "Taking off on the information superhighway"

We find these views also in the quoted policing literature. For example, in the managerial, operational and practical guide to the use IT in law enforcement, ex-police officer Jim Chu writes: "Luddites in policing beware. The train is leaving the station. In fact, the IT train has jumped the rail tracks and has taken off on the information superhighway[3]" (Chu 2001, 3). More recently, in a volume on *Technology-led policing*, Willy Bruggeman writes: "Technological control will march forward. It will have widespread effects on policing across the globe" even if "the effects of the technological revolution will not be uniform […]" (Bruggeman 2011, 160).

Technology here is an unstoppable force and somehow unpredictable and autonomous, as it 'jumps the rail tracks' or 'marches' as an army. It is able to effect change irrespective of the different forms of resistance, including from within police organizations themselves. Even so, Bruggeman argues, "citizens and decision makers need to inform themselves about technological control" in order to "prevent naïve decisions, maximize technologist's benefits given personal values and identify inflection points at which decisions can have the desired effect […]" (Bruggeman 2011, 160). But what motivation do we have to get involved if we think that technology will march forward anyhow?

[3] The term 'Luddite' refers here, derogatory, to "a person opposed to increased industrialization or new technology" (cf. Oxford Dictionaries. Accessed from http://www.oxforddictionaries.com/)

In the above accounts, technological change is portrayed rather positively for policing, bringing about organizational progress and more efficient policing. However, in other accounts, the 'self-amplifying technical means' (Byrne and Marx 2011, 34) are 'a danger' that needs to be tackled. Here technologies are portrayed as dangerous forces for both policing and society due to their "potential danger of the misuse of power and information collected via control technologies" or due to 'technological failures' (Bruggeman 2011, 160). The implication is that technology is ubiquitously present having power to negatively affect policing and the social domain by 'fostering suspicion', 'reducing public trust in policing' and resulting in 'worse outcomes for life-chances' (Bruggeman 2011, 160). In both accounts, the character of technology changes from the passive tools to an autonomous force, refusing social conditioning and possessing not only potential but intelligence and agency.

The view of autonomous technology has been also taken up in scholarly work on technology. Jacques Ellul, one of the most important thinkers in this strand of thought on technology, speaks of *technique* and defines it as "the totality of methods rationally arrived at and having absolute efficiency (for a given stage of development)" (Ellul 1964, 25). With this definition come two implications. If it is applied scientific rationality then technique is shaped by scientific knowledge and, as in many popular accounts, by its claims to objectivity and access to truth about the natural world. A second implication of this definition is that improvements in efficiency will necessarily occur in each stage of development to solve problems, whenever new technological solutions become available. Ellul calls this phenomenon 'self-augmentation'. Its further development follows by way of necessity.

Many examples of this view can be found in lay understandings on technological development. For instance, we hear time-and-again that integrated circuits made personal computers possible due to their efficiency in processing data. It is also common place to hear that because of the computer's efficiency and increasing speed, electronic communications came to dominate over handwriting, typewriters and surface mail. At the same time, these capabilities led to the storage and processing of larger and larger amounts of data, with a big part being personal data. Therefore, often lay opinions hold that this state of affairs makes the defence of a value like privacy unfeasible as it is a consequence of a process outside our possibility of influence.

From this perspective, technology is autonomous from human choice as the logic by which it changes and develops ignores ethical argumentation or moral and spiritual values. It now also becomes clear why this view is supported by an understanding of technology as value-neutral. As long as technology presents itself as value-neutral tools, based on mathematical and physical laws, then the social, political or spiritual values that might have played a role in their design and development become hidden or not easily recognized.

3.2.3 "Means determining the ends"

Technological determinism is the claim, considered with various degrees of strength, that technology causes or determines the structure of the rest of society and culture. We find it also present in the contemporary literature in policing: "In the future, exponential technological advancements will continue to increase social vulnerability and fear, give terrorists and criminals new methods and opportunities, and give police new tools to stop them. […]. The development of new technologies will ultimately change the nature of society and the way humans conduct their lives" (Bruggeman 2011, 159). The idea is related but not identical to the one of autonomous technology, developing independently from the influence of society. The

thesis of autonomous technology generally presupposes technological determinism. If technology determines the rest of culture, then culture and society cannot affect its direction. Technological determinism does not, however, presuppose autonomous technology. One could still take the view that free, creative inventors devise technology but once used and disseminated into society at large, technology induces change in the social structure (Collingridge 1980). For instance, take the view that 'the Internet' was designed in a military context but once it spread and became used it caused big changes in people's habits and behaviour across the globe. One can choose to focus on the flexibility of early stage designs, when researchers and designers played an important role and render them as free agents outside the technological determinist cycle.

As the above quotes and examples illustrate, the theme of autonomous technology is still significantly influential in contemporary managerial and policy literature in policing. Moreover, several authors point out that technological determinism is still the dominant underlying theme in many accounts of technology today (Feenberg 2002, Wyatt 2008). As Wyatt argues, the force and endurance of these views on technological development stem in part from the daily experience of the large majority of technology users: "For most of us, most of the time, the technologies we use every day are of mysterious origin and design. We have no idea where they came and possibly even less idea how they actually work. We simply adapt ourselves to their requirements and hope that they continue to function in the predictable and expected ways promised by those who sold them to us. It is because technological determinism conforms to a huge majority of people's experiences that it remains the "common sense" explanation" (Wyatt 2008, 169).

3.2.4 Partial conclusion

In this section we have analysed a few of the prevalent conceptions of technology in policing literature. These framings of technology may seem 'common sense' but they carry with them particular views and assumptions concerning technological change and the social role of technologies. To some extent it is understandable to think of technologies in policing as tools that officers 'have to have'. 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 and, when proven wrong, decline responsibility with the claim: 'The technology made me do it'. A standard instrumentalist conception of technology places responsibility of outcomes in the hands of the users but, as we have seen, at a cost. Ignoring the social, political and ethical dimensions of technological development it silences the social role of technologies in inducing consequences.

A view of technology as the main force determining society has problems in articulating the interdependencies that enable technologies to work. It lacks an account of the complex interactions between users, organizations, institutions and legal regimes. Consequently, this view fails to properly account for the role of designers, engineers or policy makers in shaping the direction of technological change. A substantive view on technology, as possessing autonomy and developing independently from social forces, is thus providing a rather poor conceptual background for understanding the complex arrangements of a highly technologically-mediated policing. Why would we devote energy to try to shape the next technological wave or particular projects in policing if we think that technology changes independently from our input or by forces outside our realm? Remaining in this framing of

technology, the conditions remain arbitrary for a more ethically informed process of shaping technology that takes into account a broader set of values and norms.

3.3 Studying the social role of technology

In the past decades, these views began to be contested by a body of work from social studies of science, history of technology and philosophy of technology (known generically as Science and Technology Studies). Rather than assuming 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, engage in rhetorical work (for instance to attract funding and support for their projects and ideas), and get connected to cultural and societal processes, conflicts and debates. These studies delve into empirical investigations to understand how scientific facts, knowledge, phenomena or technological artefacts are constructed and what imprint does this process leave on the activities and the outcomes (Pinch and Bijker 1987, MacKenzie and Wajcman 1985, Bijker 1992, 2010)[4]. From this perspective, the development and use of technologies appear to be not merely applications of mathematics and physics but culturally contested processes, shaped by social, ethical and political choices.

3.3.1 On the politics of technology

One of the first illustrations of these points has been the discussion of Langdon Winner's by-now-classical article "Do artifacts have politics?" (Winner 1980). Winner argues that technologies embody specific forms of power and authority as they possess political qualities. In one example, Winner tells the story of the low-hanging bridges in New York designed by the architect Robert Moses. This architectural choice was allegedly done in order to prevent the passing of busses and to allow only cars to reach the Long Island beach resort. In this way, the argument goes, the bridges would discourage the presence of the black and the poor populations, usually dependent on public transportation in that period (1920s New York). If the vehicle was able to pass below the bridge, the reasoning went, it meant it was likely to be a car and this would increase the probability that the owner had the desired status. Therefore, the low-hanging bridges would act as a material barrier, embodying the political values of the designer without the need of the designer's presence or active involvement.

The example produced a significant impact on generations of students in Science and Technology Studies with contestation and approval taking turns. Besides contesting it as counterfactual (i.e. the actual bridge is not low enough to block busses), critics pointed at the ambivalences of technologies and argued that the alleged consequences of those bridges are *not definitive* (Joerges 1999, Woolgar and Cooper 1999). Therefore, technologies cannot be said to be inherently political. That is, the low-hanging overpasses may only contingently embody the norm that the poor and the black population should not be able to pass. Taking different routes

[4] There are of course, differences between STS analyses that look at how science and how technology are social activities. For instance, the claim that facts, realities, and nature are socially constructed, are much less central to considerations about technology. That is, technological artefacts are more clearly made/designed/produced than scientific facts, even if the theme of autonomous technology persists in some accounts of technological development.

or being able to afford cars are alternatives that make those bridges fail as a political barrier embodied in technology.

Radder defends Winner's phrasing of the point. Whereas critics interpreted Winner's account of the bridges as fully blocking access to the beaches, he reminds that Winner only claimed that the bridges *limit* access. In general, that technologies *influence* behaviour, practices and the lives of the people involved. "In all the cases cited above [including the bridges] the technologies are relatively flexible in design and arrangement and variable in their effects. Although one can imagine a particular result produced in a particular setting, one can also easily imagine how a roughly similar device or system might have been built or situated with very much different political consequences" (Winner 1986, 29 as cited in Radder 2009).

The discussion of Winner's example indicates that artefacts may be more than neutral tools but also that the politics of artefacts should not be interpreted as invariable features. The roles of artefacts are contingent on many factors of design and use, institutional arrangements, cultural processes that feature in each particular situation. It is also a contingent issue whether the norms they embody are political, moral, environmental, etc. In a general sense, technologies can be seen as inherently normative (Radder 2009) but it remains an epistemological and empirical question, which specific norms they embody in each particular case.

3.3.2 On Science and Technology Studies

STS scholarship produced a solid body of work concerning a variety of aspects related to science and technology. Concerning technological development many STS works showed that rather than developing autonomously from social forces, technology is shaped by a multiplicity of actors that give different meanings and uses to them. For instance, Wiebe Bijker's largely cited study of the development of the bicycle took a historical approach to highlight the role that various social actors played at times in this technological development (Bijker 1995). He showed that what looks to many people as a linear and unstoppable process towards efficiency – from the high-wheeler penny-farthing bicycle to the modern safety bicycle – could have taken different turns. Bijker showed that despite the argument that it is safer and more stable, the group of 'young male riders', for instance, did not appreciate too much the early versions of what is now called the modern safety bicycle. They interpreted it as not being at all superior to the high-wheeler and as sacrificing on style for a claim to stability, which they contested. Upon closer analysis the development of the bicycle was shaped by a variety of *relevant social groups* with different interests and views. These actors embraced bicycles for their own reasons, shaping bicycle designs in different directions. Whether a bicycle 'worked well' was a product of the character and interests of a user group. In this analysis, designs have *interpretative flexibility*, referring to the different meanings that audiences give to technologies. This study emphasizes the *social construction* of technologies and suggests that designs do not become successful because they are intrinsically good but what becomes a 'good design' is the result of being adopted and socially successful.

In another STS study, Grint and Woolgar (Grint and Woolgar 1997) showed that successful designs also require controlling, educating as well as defining the users of a technology. Their study took an ethnographic approach and looked at the development process of a computer company that aimed at developing a new 'user-friendly' product. While testing the product to try to understand what needed to be done to make it more user-friendly, one conclusion that the company drew was that the new product also required the *users to be configured* and be made computer-friendly. Successful technologies do what they do only in the context of appropriate

users. Building artefacts implies a simultaneous construction of social realities, from which they cannot be separated in practice. From this perspective, technologists have the task of building stable networks that bind together a heterogeneous set of components.

Some STS studies concentrated more on user-technology interactions. They highlighted the active role of users in giving new meanings and finding new ways of using artefacts that designers did not intend (Pinch and Bijker 1987, Oudshoorn and Pinch 2003). From this perspective, any a priori distinction between technologists and users is arbitrary as it cannot adequately account for the multiple ways in which *users and technologies co-construct each other* (Oudshoorn and Pinch 2003). For instance, early versions of the Internet may have been developed in a military context but people appropriated it and are constantly changing Internet technologies in both content and structure. These STS studies show how even non-users – meaning those do not use technologies – either from active resistance or from lacking access, can be important actors shaping technological development (Wyatt 2003).

To accommodate these various insights brought by a growing number of empirical investigations into the construction, development and use of technologies, STS scholarship introduced new terms and, in time, a whole vocabulary for speaking of technology-society relations. Rather than speaking of 'social relations', 'tools' and 'technical aspects' as purely distinguished domains these works propose to speak of '*socio-technical ensembles'* or *'socio-technical systems*'. Taking the concept of socio-technical ensemble as a unit of analysis acknowledges that to understand an artefact or a social practice as an independent entity can be misleading. Focusing on 'just' an artefact can cause an abstraction away from all the social practices and social meanings around it.

At the same time, concentrating only on social practices tends to ignore the active role of the artefacts in shaping the social arrangement or practice at stake. Some STS scholars criticize social constructionism for overemphasizing the power of the 'relevant social groups' or 'society' in constructing artefacts as "the social is kept stable all along and accounts for the shape of technological change" (Latour 2005, 10). Also Grint and Woolgar argue that approaches concentrating on the social shaping of technology "rescue technology from the clutches of technological determinism, only to reaccommodate it as one among several independent variables which determine action and behaviour" (Grint and Woolgar 1997, 7). In this sense, the following section elaborates on Actor Network Theory as a framework that aims to avoid both tendencies.

3.3.3 On Actor-Network Theory

In the STS tradition, Actor-Network Theory (Callon 1986, Law 1987, Latour 1988, Callon 1991, 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, bacteria, laboratory animals, institutions).

ANT-type of analyses have been made in a wide variety of studies. 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 (Callon 1987) uses the term '*engineer-sociologist*' to speak about the work that engineers at the Electricite de France needed to do for developing an

electric car. They needed to deal not only with the nuts and bolts but they simultaneously needed to project a vision of the French society in which these cars would fit. The technology and the vision of society are bounded to each other and neither would happen without the other. Similarly, John Law (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. Technologists face technical, social and economic problems together and they need to combine knowledge, skills, materials and a diverse set of actors in a configuration that works.

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. He shows how 'purely technical' artifacts can be highly moral and social (Latour 1988, 298). Latour shows that what a thing is and does and also what a human being is and does, stems out of the relations they have with other things and humans rather than from an essence that stays behind them. For example, a door groom automatically closes doors in association with a hinge. This may be called a relation between two non-humans (Latour 1988). It is in *networks of relations and associations* that they are enacted in specific ways, becoming what they are and doing what they do.

We may extend the argument to more aggregates in a machine or between artefacts, as they do what they do as being in relation to each other, and perhaps with other machine components and with 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 him this task.

The reason that justifies analysing them symmetrically rests, according to Latour, in the equivalent roles that they play in these networks of relations in producing outcomes. To understand what a nonhuman does, Latour invites analysts to make a thought experiment and "imagine what other humans or other nonhumans would have to do were this character not present" (Latour 1988, 299). For instance, Latour argues funnily, every time someone wants to pass through a door, an analyst might want to imagine that a hinge has to be replaced by somebody with a pick, to open a hole through a wall, as well as someone with mortar and bricks, to put the wall back in order for stopping the draft and other unwanted entities to go through. Similarly, if we want to understand the role of an automated profile in policing, we may want to imagine how much effort might be needed to obtain the same outcome: how many police officers in the field watching and taking notes of traffic behaviour and then how many meetings to discuss the findings in order to hopefully agree on identifying a pattern.

A relation between a human and a non-human, could be the one between a hinge and a groom, a biker and a bicycle, a driver and a bus or between a police officer and a profile or a GPS screen or a gun. Furthermore, a relation between two humans could be the one between, an employer and an employee, an officer and a police chief, etc. So, every relation between humans and between humans and non-humans forms a chain of relations. Latour's point is that these relations, including the ones between humans and non-humans, are always integrated into longer chains and it is these chains and their transformation that should be studied if we want to overcome arbitrary delineations and a priori hierarchies between 'society' and 'technology'.

3.3.3.1 Centres of calculation

Important places in these chains of relations are, what Latour calls, *centres of calculation* (Latour 1987). He illustrates this abstract notion with the story of the mapping of certain areas of the East Pacific; or with the story of a professor Bijker from the Delft Hydraulics Laboratory who built several miniature dams in order to learn what shape a new dam in the port of Rotterdam should take for best limiting the inflow of water. With these stories, Latour shows that *knowledge is also constructed* within networks of relations in cycles of accumulation. Instead of understanding space and time as something immutable in which events take place, centres invite us to understand space and time as constructible and produced inside the networks of relations.

Through this process, long dams become, for instance, a few square meters in laboratories, long distances in the East Pacific become centimetres on a map, nanometers and billions of years become centimetres on paper. In these centres new spaces and time are produced. Latour's approach to studying techno-science is one in which facts and artefacts are not ready made but in the process of making. In this view, knowledge also is not something fixed that could be described by itself but dynamically produced in *cycles of accumulation*. Repeatedly bringing things to a place, a centre, to be analysed and made available for other interventions. After being mobilized and moved into the centres, traces and events are being translated and represented several times to become maps, diagrams, pie charts, etc. This movement from periphery to the centre and back makes places, people, phenomena or events mobile in order for scientists and technologists to cumulate and recombine them.

Centres of calculation provide an important advantage as they increase the combinability of the inscriptions through sets of translations. By writing down inscriptions, calculations become easier for scientists and engineers who are able to draw together all mobilizations and reap the benefits of this process. Each stage of translation and re-representation translates traces and places from various realms into forms and figures on paper or on a computer screen. At the same time, these artefacts may not survive outside these centres if the networks are not in place to carry them. For example, even with a map in our hands we would be lost if there would be no links with the landscape (a name of a road, a reference tree, etc.). The map would become useless without these signs. Still they give a strategic position to those in the centres of calculation as the ones translating back the strength that has been made favourable to them from the centres to the periphery.

This does not imply that this view is total, Latour argues elsewhere (Latour 2005, Latour and Hermant 2006). Even if he reserves the term centre of calculation for places where actual mathematical or arithmetic computations take place, he proposes the term 'oligopticon' as a more generic way to understand this kinds of connecting or structuring sites. From the Greek oligo meaning little, these are places from which one cannot see everything about the whole but framed aspects of reality. Oligoptica, such as the control rooms of water services, phone companies, police stations, electricity companies, communication companies, central registers, cadastre offices afford a narrow and framed view of reality. "From there very little can be seen at any one time, but everything appears with great precision owing to a dual network of signs, coming and going, rising and descending" (Latour and Hermant 2006, 32). At the same time, this view is dependent on a whole chain of human and non-human actors like maps, police agents, computer programs, personal data and so on.

Given the amount of computation that takes place in contemporary policing, at operational, tactical or strategic levels (as we have seen in chapter 2), we could understand them not only as

metaphorical oligoptica (as I will detail later in this chapter) but as centres of calculation where data about people, places, events is repeatedly aggregated, translated, processed and made ready for intervention. We can see police control rooms as centres of calculation in which vehicles become number plates and people become database records or 3D representations in smart video surveillance systems. Similarly, this notion allows us to understand that police knowledge is also accumulated, translated and constructed.

3.3.3.2 Some objections to ANT

Since its elaboration, many STS scholars took Actor Network Theory as a constant reference in their approach. Despite its big influence, ANT also received objections that concern this research. When considering the outcomes of technology design and use, one problematic aspect is the ANT's distribution of agency. Despite its emphasis on a symmetrical treating of humans and non-humans, ANT analysts tended in practice to favour the accounts of human actants such as scientists and technologists. This is also visible in the brief summary of some of ANT's seminal works in the previous section. ANT analysts often find human beings more interesting and exposing richer repertoires. Many of the early works in ANT present the stories of hero scientists or technologists and thus may miss other perspectives. In time, STS scholarship, especially feminist STS, provided radically different insights, balancing this tendency (Star 1991, Wajcman 2010). At the same time, technology changed as well. Callon articulated one of his ANT points about the agency of non-humans by taking the perspective of the scallops of St. Brieuc Bay (Callon 1986). It may be much easier now to acknowledge this STS point when considering autonomous robots, automatic devices or self-organizing sensor networks as the ones anticipated in Internet of Things developments.

Another problem related to agency distribution is the so-called 'problem of many hands'. In situations in which there are many actors that play a small part in a chain of relations, it is difficult to pin-point who is responsible for the outcomes. By analysing artefacts as actants in networks of relations, ANT does not make this problem simpler. In fact, the network can quickly expand with a multitude of actants and this can dilute moral responsibility. As Waelbers argues, "Latour is not talking about moral responsibility at all and focuses solely on causality" (Waelbers 2011, 41). Still, the ANT vocabulary and approach are fit for charting the "geography of responsibilities" (Akrich 1992, 207) between human and non-human actants. Although not a guarantee for an adequate attribution of moral responsibility, ANT analyses offer thick descriptions of socio-technical arrangements, informing evaluations of moral responsibility despite the problem of many hands.

To understand how the charting of networks of human and non-human relations can inform evaluations of moral responsibility we can look at a situation analysed by Vermaas et al. (2011). The authors describe the case of a plane crash that took place in Brazil in 2007. An Airbus overshot the end of the runway, crossed the nearby motorway, plunged into a warehouse and finally exploded, making more than 200 victims. Initially, the conclusion was that the cause of the accident laid in the short runway combined with wet weather conditions. However, the authors show how the distribution of responsibility changed at different stages, depending on the results of the investigations. The investigators followed the trace of the involved actors and, after it was clear that there was actually not so much water on the runway to justify slippery wheels, they directed their trace elsewhere. In this way they found responsibility distributed in a heterogeneous set of actors. They identified an engine component that did not start, looked at the actions of the pilots and "other actors that could possibly have borne some responsibility in this case such as the air traffic controllers, the aviation authorities, the plane's maintenance

technicians and the engineers, who designed the airplane and drew up the flying instructions" (Vermaas et al. 2011, 107).

This detailed analysis of human and non-human actors and their relations helped the authors to point more precisely towards the moral responsibility of various actors. The analysis of this case demonstrates that the problem of many hands is not a sufficient ground to inhibit analyses of networks of relations and surrender to moral relativism. Following the actors and taking a symmetric view towards the role of human beings and that of artefacts, ANT analyses can support fine grained responsibility attribution.

Yet again, emphasizing a symmetrical consideration of human and non-human actors, ANT posits non-humans as acting in the same way as humans do, having interests, enrolling other actors, etc. Conversely, such an approach can fail to protect people from being rendered as 'mere things'. While it is one of the more controversial issues, this is an analytical position, allowing for the development of multiple perspectives. Nobody would take a knife to court and, hopefully, nobody will read an ANT analysis and consider a person to be a thing. This symmetric move is done to counter the drawbacks of determinisms by doing away with the divide between 'society' and 'technology' as being strictly delimited realms.

For Latour, this can be done by asking a different set of questions. Instead of asking has 'society' influenced 'technology', or has 'technology' influenced 'society', ANT proposes a different set of questions: has a human replaced a non-human, has a non-human replaced a human? Has a competence of this actant been modified? Has the chain of associations been extended or modified? By viewing them in this way and following the actants, a whole set of concepts (association, delegation, translation, mediation) emerges. This vocabulary may help us to see that "any divisions we make between society on the one hand and scientific and technical content on the other is necessarily arbitrary" (Latour 1991, 106).

3.3.3.3 ANT and material semiotics

Objections and refutations can continue but perhaps this may not be the most fruitful way to understand ANT. Annemarie Mol suggests that "ANT is not a "theory", or, if it is, then a "theory" does not necessarily offer a coherent framework, but may as well be an adaptable, open repository. A list of terms. A set of sensitivities. The strength of ANT, then, is not that it is solid, but rather that it is adaptable. It has assembled a rich array of explorative and experimental ways of attuning to the world. […] The point is not to fight until a single pattern holds, but to add on ever more layers, and enrich the repertoire" (Mol 2010, 253). And she appetizingly concludes her text on ANT: "A good colleague has been invited to now engage in criticism (of me? of this text? of actor-network theory?). We will see. I do not think that I have prepared us (myself, this text, actor-network theory) very well for a fight. I have not crafted a stronghold that is easy to defend. There are no walls around this text, instead it is quite open. I have written this as a present. Here it is. Enjoy it or forget it. Eat from it, as much as you like, and digest it – or push your plate away." (Mol 2010, 266).

In a similar but more abstract definition, John Law invites us to see ANT as "a disparate family of material-semiotic tools, sensibilities, and methods of analysis that treat everything in the social and natural worlds as a continuously generated effect of the webs of relations within which they are located. It assumes that nothing has reality or form outside the enactment of those relations. Its studies explore and characterize the webs and the practices that carry them. Like other material-semiotic approaches, the actor network approach thus describes the enactment of materially and discursively heterogeneous relations that produce and reshuffle all

kinds of actors including objects, subjects, human beings, machines, animals, "nature," ideas, organizations, inequalities, scale and sizes, and geographical arrangements." (Law 2008, 141)

For a study of technologically mediated policing, perhaps we are better off to take ANT not as an ossified theory that explains criminal phenomena or why technologies do what they do. As Mol and Law suggest, we might take it as an open and a flexible approach with a set of notions and terms, whose strength comes from its adaptability and richness to attend to phenomena. As such, an ANT inspired approach can be expanded, nuanced and sharpened to help us come to grips with technologies in policing. How can we speak about what officers do with technologies and what technologies do to them?

3.4 Technological mediation

An ANT-inspired vocabulary can help us to steer away from fatalist stances towards technological development, while at the same time not reducing technologies to neutral, obedient tools. In stressing the need to analyse the agency of technological artefacts to the same extent as that of human beings, ANT conceives technologies as actively doing something beyond their intended functions. At the same time, we have seen that technologies in policing do what they do as part of networks that include multiple actors. We need to understand what they do among police officers, organizational structures, legal provisions, inter-institutional arrangements and others. It is thus relevant and feasible to study what technologies do in particular policing projects. For this we need a vocabulary that comes to grips with the active role of technologies in influencing officers' practices, experiences, perceptions, their decisions and their actions.

3.4.1 Scripts and mediation of action

A contribution of ANT that avoids deterministic views on technology is a vocabulary that conceptualizes the way in which technologies relate to human action. Madeleine Akrich and Bruno Latour propose the notion of *script* and the related family of notions (Akrich 1992, Akrich and Latour 1992). In this approach, rooted in ANT, rather than taking them as tools, technologies *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 eventually act.

On the one hand, 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 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 are compelling drivers to slow down in order not to wreck their cars and hit their heads (Latour 1994).

On the other hand, 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 user behaviour, interests and motives in relation to artefacts and they build

preinscriptions. For instance, smart homes designers anticipate that people want to relax while living in them. They make their algorithms, say, automatically reinforcing patterns of use (e.g. coffee strength, sugar level, etc.). However, users can also give new meanings to artefacts, thus also taking part in inscription processes. For instance, the owner of such a smart home may consider the coffee too soft in some mornings, when factors outside the reach of the algorithm played a role.

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 all 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 are 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 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 technological development', 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 mediating role.

3.4.2 Mediating perception and experience

The vocabulary of technological mediation can be further expanded with insights from the philosophy of technology research that can 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. 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, 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, an American philosopher of technology. 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, 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, 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 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, 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, 13). Issues of interpretation are central to this approach and its questions concern the mediating role of technologies from a hermeneutical perspective.

3.4.2.1 Types of relations

Don Ihde identifies several ways in which humans interact with technological 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, scientists look *through* the microscope, and not *at* the microscope, to perceive microbes and to understand what they are. In a similar manner, police officers look through binoculars to follow someone or they perceive suspicious 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 or hear beeping sounds produced by systems. They interpret their values, pitches or tones and take some of them to represent important indicators while others as irrelevant or as indicating 'normal activity'. For instance, they can interpret the high value of a financial transaction as being 'a sign of money laundering'. They can interpret the rise of a number of committed offences in an area as indicative of 'a new criminal group in town'.

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 in the background of the interaction with technologies, while the 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 centre while officer analyse indicators on screens or the worm air produced by the air-conditioning system of a police car. In these examples technologies shape the policing experience – for instance making officers more relaxed, alert, stressed or irritated – but in the background of other activities.

Of course, the relation with concrete artefacts can be simultaneously characterized by a multitude of relations from this taxonomy. For instance, when we work with a computer we can often get lost in activities and embody the screen in our experience. Simultaneously, we can interpret various numbers on the screen (e.g. outside temperature in a weather application). Still, at the same time, we can pay attention to the humming noise of the device. All kinds of relations exist simultaneously and their separation becomes an analytic exercise.

Verbeek expands this set of interactions to account for a whole set of relations that cannot be properly understood in either of these categories. He gives the example of a brain implant. This kind of technology "is not merely embodied; rather, it merges with the human body into a new, hybrid being" (Verbeek 2015, 29). He proposes to call this 'a *cyborg* relation'. Still, the term 'relation' presupposes a distinction, however small, between the entities that take part in it. When he proposes that the brain implant *merges* with the human into a new being, the term 'relation' loses ground in this taxonomy. Perhaps this kind of technologies require a wholly different vocabulary that captures interactions at a neurological level. Still, for the purposes of this research, this relation is not useful as contemporary policing does not (yet) employ this kind of technologies.

Another type of relation that Verbeek identifies comes from technologies that merge with our environment. In 'smart environments' or 'ambient intelligence' technologies 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 technologies can actively detect vehicle number plates, recognize faces, sense movement and 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 technologies 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.

3.4.2.2 Types of influences

Besides charting the type of relations, the vocabulary of technological mediation is also mapping the kind of influence that technologies can have on human users. Tromp, Hekkert, and Verbeek (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*. As examples they give turnstiles that force one to buy a ticket before entering the subway. In the policing context we can think of the 'drop safety' mechanism that prevents the discharge of a gun as long as it is not explicitly removed. Or we can think of access control mechanisms in information systems that require officers to have the proper credentials in order to access classified data.

On the other side of the visibility spectrum we can find *persuasive* technologies. This kind of technologies show their influence explicitly, without being overpowering on the user. Tromp, Hekkert, and Verbeek (2011) give the example of smart energy meters that provide feedback on energy consumption, aiming to convince the users to make a more efficient use of their appliances. 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. For instance, the management of a police force may consider that public safety is better protected when agents keep their guns locked by default with a safety mechanism in place.

Technologies can also have more soft and subtle influences, which work by *seducing* the users. Tromp, Hekkert, and Verbeek (2011) give an example from architecture, where placing a coffee machine in a central place in an organization can stimulate social interaction. The influence is hidden as people are generally not aware of the way in which this arrangement stimulates lateral discussions in the organization. Police forces often implement this kind of arrangements by placing a meeting place, table or the coffee machine at the junction of more departments, teams or units.

A fourth type of influence in this taxonomy is both strong and hidden. Tromp, Hekkert, and Verbeek (2011) call it *decisive* or *implicative* because it exerts influence without this influence being noticed. They give the example of an apartment building without an elevator, implicitly forcing people to use the stairs. In the policing context we can find cubicles that separate offices in a control room, effectively protecting officer privacy or enforcing work division.

3.4.3 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 post-phenomenological 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 Don 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 Don 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, 168).

For the purposes of this research, the vocabulary of technological mediation becomes richer through this complementarity, offering a repertoire that can capture more nuances and dimensions of contemporary technologically mediated policing. 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, 261). If we want to understand the complex work of technologies in contemporary policing, we need to understand both the networks of relations between officers, artefacts, designers or policy makers but also what practitioners experience in their technologically-mediated 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.

3.4.4 Implications for engineers and designers

In the previous sections we have seen how the notion of script demonstrates that technological artefacts can be prescriptive, guiding users without the need for the designer’s presence and often without this normativity emerging from a designer’s intention. Artefacts prescribe behaviour, while users are able to subscribe or not to their program of actions or appropriate them differently and give them new meanings. We have also seen how designers and engineers can explicitly delegate their values to artefacts and can try to anticipate mediations when designing a product using the vocabulary of technological mediation.

Rejecting the idea of autonomous technology allows us to see that the work of designers and engineers does not happen in the absence of social relations. The decisions they make do not occur by virtue of a logic solely guided by science and nature but they are simultaneously having social, political and ethical dimensions. The insights brought by STS and philosophy of technology (through the notions of script and technological mediation) demonstrate that the design of artefacts functions as a form of guidance of human behaviour. Whereas the activities of designers and engineers are usually associated to ‘technical decisions’, research in STS and philosophy of technology show that engineering work cannot be separated from the moral and political dimensions of socio-technical arrangements.

Working in interaction with other (f)actors within networks of relations, designers and engineers are also nodes, albeit important, in processes of technological development (Johnson and Wetmore 2008). On the one hand, this insight suggests that engineers and designers are limited in influencing the outcomes of their work: in a network, one shares responsibility with a whole set of other entities (users, laws, institutions, policy makers). On the other hand, ethnographic studies into engineering work show that the limitation of their capacity to influence outcomes does not imply that they are powerless actors (Swierstra and Jelsma 2006). Engineers and designers are able to choose among multiple design solutions and propose various use contexts. Abandoning the view of technologies as value neutral leaves room for acknowledging that the responsibility of engineers is bigger; at least compared to a view in

which they follow nature and design neutral devices that users decide if and how to engage them.

Designers and engineers share at least part of the responsibilities for the outcomes, appropriate for their level of interaction within socio-technical systems. They can engage in reflection on the values and norms that they delegate to designs and can engage in designing the mediations of technologies. Even if individual engineers cannot be always held responsible for not reflecting on the value charge of their work, institutional arrangements can be put in place on the engineering work floor to facilitate ethical reflection and enable the assumption of moral responsibility by engineers and designers (Swierstra and Jelsma 2006). Together with policymakers but also with users, designers "should be enabled to read, design, and implement technological mediations, in order to be able deal in a critical, creative, and productive way with powers that remain hidden otherwise" (Verbeek 2015, 31). Drawing on these insights, engineers and designers can make more informed choices about the value charge of their artefacts and, as we will see in the coming chapters, this holds also for the designers and engineers of policing technologies.

3.4.5 Partial conclusion

A common feature of STS studies and one of the main messages of contemporary philosophy of technology is a forceful rejection of the autonomous technology thesis and technological determinism as they show how technologies are forged within the pressures exerted by a heterogeneous set of (f)actors. In the analyses of these studies it becomes visible how engineers, designers, policy makers, standardisation and governmental bodies, and diverse kinds of users play a role in the design and use of technologies, influencing their shape, development and outcomes. If to billions of people, technology looks like an unpredictable, external fate falling on their heads, the effort made within STS and philosophy of technology offers a set of empirical investigations, notions and concepts with which we can understand the choices that were made in their construction and use. What this effort reveals is a rich image of the intricacies of techno-science and of the mediating role of technologies, demystifying the ideas that technology is neutral and that it develops autonomously from social interactions. In other words, things could have been different and can still be made differently, including for technologies in policing.

3.5 Studying surveillance

The previous sections introduced and elaborated a set of notions and concepts derived from empirical studies on science and technology. With these we can understand the role of technologies in policing beyond instrumentalist and determinist accounts. How should we study surveillance in policing while taking these insights into account? As we have seen in the previous chapter, surveillance is one of the key practices in policing in strategies of prevention and investigation of criminal behaviour. But surveillance goes way beyond the police, contributing to transforming the very practices, organization and models of policing. In contemporary societies, people are moving and living in interaction with an increasingly thicker and intimate technological environment (mobile internet, social media, interconnected databases, internet of things, smart homes, etc.) to which a plethora of entities, including

policing agencies, have various degrees of access for management, use but also design and development.

The fast growth of surveillance has made its study more relevant than ever. Surveillance studies is a multi-disciplinary enterprise, drawing from sociology, philosophy, technology studies, media studies and other areas of research that aim to understand the phenomenon of surveillance in its multiple aspects and guises. Amongst issues of power, knowledge, legality or ethics it deals with the role of technologies in practices of surveillance. This aspect of the emerging discipline makes it relevant for a study looking at the intersection of policing practices with new technological developments (e.g. internet of things, mobile internet, intelligent transport systems, social media, etc.).

3.5.1 Surveillance in novels and films

Police surveillance is actually one of the first areas of interest in surveillance studies, developed as such in the '70s and '80s (Marx 1988). Still, a much older interest in police surveillance has been cultivated in novels and films, which provide insights to this day for academic investigations in surveillance studies. For instance, the 1956 short science-fiction story of Philip K. Dick, *The Minority Report*, portrays a police department that relies on the prediction of crime rather than on a posteriori investigation and punishment. In the novel, the police uses a computer system that processes the reports of 'precogs' – a group of three mutants whose talent is to see into the future (for up to two weeks). The novel (also adapted into a film in 2002) touches on contemporary policing themes and practices as it deals with prediction and pre-emption and with the police officer's reliance on technology in decision making (Van Brakel and De Hert 2011).

In the novel, when the computer identifies that the visions of at least two of the 'precogs' overlap to a significant extent in predicting a crime it produces a majority report. Police officers interpret these reports as future unfolding of events and act on those identified to be the likely perpetrators. An important theme problematized is that of the condition of the police officer in relation to the privileged access to these technologies. In the novel, the commissioner has access to prediction systems when he receives a majority report about his own potential criminal future. This enables him to change his course of action and search for the minority report.

Many other novels and films deal with surveillance in policing, often producing valuable insights and powerful portrayals of technologically mediated surveillance[5]. But no other novel has dominated the branch of police surveillance as George Orwell's *Nineteen-Eighty-four*. As David Lyon reminds us – one of the leading scholars in surveillance studies – the early works of the emerging field of surveillance studies were dominated by the *Nineteen-Eighty-Four* scenario. The book has often been used to analyse the role of new technologies in supporting not only authoritarian regimes of the time but also the totalitarian tendencies of bureaucratic liberal states (Lyon 2006).

[5] For an inventory of the literature on the theme of surveillance in novels, films and television the reader is invited to consult and explore Kammerer (2012)

3.5.2 Brothers and sisters in surveillance

In George Orwell's book, citizens are constantly monitored for social control by a totalitarian state. The state uses a tele-screen, which both records citizen's behaviour and projects images of a sinister Big Brother. In this society "The telescreen received and transmitted simultaneously. Any sound […] above the level of a very low whisper, would be picked up by it […] There was of course no way of knowing whether you were being watched at any given moment […] It was even conceivable that they watched everybody all the time…" (Orwell 1949 Part 1, Ch. 1). Orwell's Big Brother character became a synonym for totalitarian state surveillance, while the novel is credited for neologisms such as 'orwellian' or 'thought police' entering contemporary popular culture.

While prophetic in the use of screens in practices of social control, Orwell's book did not foresee in 1949 the rise of computer power and the spread of digital surveillance. In chapter 1 of the book, Orwell described a scenario in which the vast majority of the population – the 'proles' – would be largely exempt from being targeted by surveillance. The book did not anticipate the sheer spread and intensification of surveillance towards virtually all aspects of society and the large majority of the population. Moreover, the emphasis on state surveillance appears today too restricted in a society where a myriad of state and non-state entities, public and private policing bodies, are engaging in multiple surveillance projects for continuously changing purposes.

The metaphor became so widespread and overused that it became a trope in popular culture in relation to domesticating surveillance (Andrejevic 2004). In academic literature it has transformed into 'some brothers' (Mannermaa 2007), 'little sisters' or 'soft sisters' (Frissen 1998, as cited in Koops and Leenes 2005) with reference to the plurality of centres of surveillance in contemporary arrangements. However, as Lyon remarks, the 'totalitarian potential' of surveillance made a return in academic understandings of surveillance – as in the work of Maria Los (2006) – and retains some of its power as a warning (Haggerty and Ericson 2000).

3.5.3 The panopticon family

In the academic understanding of surveillance, perhaps the most dominant concept is Michel Foucault's interpretation of the *Panopticon* prison design (Foucault 1977). The Panopticon is sometimes interpreted as a generalization of the Big Brother metaphor, away from its focus on totalitarian state surveillance (Simon 2005). Michel Foucault (1977) interpreted the prison design devised by the Bentham brothers (Werret 1999) and elaborated by Jeremy Bentham as a multifaceted concept for understanding modern surveillance.

In the panoptic arrangement inmates are kept in lighted cells placed circularly around a central observing tower. Forced by this enclosure and unable to see whether guardians are actually present and actively watching, inmates have to assume that this is the case if they wish to avoid punishment. Thus the arrangement is meant to induce inmates to police themselves and in this way to insure the automatic functioning of power[6].

[6] In order to avoid doing injustice to the richness of the concept in a few paragraphs presentation, the reader in encouraged to consult the extensive literature on Foucault and the Panopticon. See for an overview Lyon (2006b).

With this metaphor, Foucault aimed to go beyond the penal system, to understand transformations in society at large. Foucault's work emphasizes the productive role that surveillance has on disciplining 'the soul', when panoptic schemes govern multiple aspects of disciplinary societies. In the words of Foucault: "he who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection" (Foucault 1977, 203). Knowing that he/she is constantly watched and assessed, the person begins to internalize behavioural norms, morals and values as he/she passes from one environment of enclosure to another (family, school, workplace, sometimes hospital or prison).

There has been much debate in surveillance studies concerning the implications of the panoptic scheme as an adequate model for understanding contemporary surveillance. Foucault used an enclosed space for his elaboration of the panopticon and in general for many of his studies (hospital, prison). However, his approach concentrated on 19th century arrangements that more authors saw as failing to provide an adequate model for understanding contemporary surveillance (Haggerty 2006). The rise of networked databases and more recently mobile internet and sensor networks together with a pluralization of surveillance actors, sparked an ongoing quest for models, metaphors and concepts to come to grips with the dynamics of contemporary surveillance. This struggle with the dominant influence of the panopticon in understanding surveillance gave rise to two sets of approaches in the surveillance studies literature. On one hand, an array of 'opticons' that looked to update the panoptic scheme in order to account for changes in contemporary surveillance. On the other hand, several authors proposed more radical departures from the panoptic model (Deleuze 1992, Green 1999, Haggerty and Ericson 2000).

3.5.3.1 The 'Opticons'

The panoptic scheme works as a disciplinary mechanism by keeping inmates in an enclosure arrangement. For this arrangement to work, the inmates should be kept long enough for the norms of the panoptic arrangement to be instilled so that they begin policing themselves. One line of critique pointed out that the panopticon model fails in its conditions of enclosure to be an adequate metaphor for understanding modern surveillance arrangements (Boyne 2000). Whereas the benthamite project assumes immobility, contemporary urban environments allow citizens to permeate them and move outside their gaze. Because they cannot contain urban populations they can't isolate them long enough for the panoptic mechanism to function. For instance, crime would be displaced towards other places outside of the gaze of cameras. This inadequacy of the panopticon to understand urban surveillance gave rise to a set of updated 'panopticons'. Notions such as the 'electronic panopticon' (Gordon 1990) or 'urban panopticon' (Koskela 2003) aimed to account for this state of affairs.

Panopticism in this line of thought is understood in a broad sense even if Foucault didn't seem to sufficiently acknowledge the mobility of late modern urban arrangements. Enclosure is still present even if not in the same literal sense in which a prison contains inmates. These authors point at relative enclosures, which are sufficiently constraining, spatially and temporally, to instil an adoption of norms. Examples are passengers in airplanes who need to assume airplane discipline and material constraints for the duration of the flight; car drivers on highways who need to assume traffic rules and road boundaries to avoid accidents and interactions with the police. Bart Simon points also at the reinforcement of 'cultural perception of limits' when isolation and differentiation are still possible as for example in front of the computer or in one's car on the road (Simon 2005).

Another related notion in this strand of thought is Didier Bigo's 'ban-opticon' (Bigo 2006). The concept points at the effects of profiling 'the foreigner' and 'deviant behaviours' compared to 'a normalized population which is pleased to be monitored against danger' (Bigo 2006, 63). Rather than highlighting disciplinary power and the inclusivity of the panopticon, the notion points at the exclusionary effects of proliferating surveillance practices targeted on various groups of dangerous 'others'.

Coming from STS scholarship, Latour and Hermant proposed the term 'oligopticon'. As mentioned in section 3.3.3.1, oligoptica are the control rooms of police stations, electricity companies or communication companies. In contrast to the ideal of the panopticon, oligoptica offer a particular, partial and framed view of reality, dependant on a whole chain of human and non-human actors like maps, police agents, computer programs and so on. However, the notion retains an important position, even if not dominant, for those placed in the centres such as police officers, analysts, etc. Whereas Latour and Hermant frame oligoptica in contrast to the flawless and frictionless view of the panopticon, Simon argues that Foucault anticipated this kind of criticism. Writing about what is needed on the side of the observer for the panoptic scheme to work: "What are required are mechanisms that analyse distributions, gaps, series, combinations, and which use instruments that render visible, record, differentiate and compare: a physics of a relational and multiple power" (Foucault 1977, 199).

According to Lyon, the panoptic scheme retains the role of a marker and it cannot be ignored at least because it continues to drive policy initiatives in security, intelligence, urban planning or policing. It remains an ideal of omniscient visibility (Lyon 2006a) and as an ideal it is abstracted from any obstacles, resistance or friction. But surveillance theory "can surely move beyond it" (Lyon 2006a, 12) in understanding the dynamics and complexity of contemporary surveillance.

3.5.4 Panning outside the panopticon

These updates of the panoptic arrangement highlight different aspects of contemporary surveillance. However, they do not depart far from the explanatory model and architecture of the panoptic scheme, reinforcing its dominance while pointing at its various limitations. These limitations also gave rise to a quest for radically new theories of surveillance to come to grips with aspects of surveillance that have been overlooked.

Haggerty (2006) criticizes the approach that takes the panopticon as a starting point and applies it to the study of various developments and domains. This tendency of a large body of literature on surveillance results in analyses where the panopticon is not necessarily the best explanatory model of surveillance. Even if these studies provide valuable insights into the working of modern surveillance they remain bound by the architecture of the model, ignoring or downsizing other important aspects of surveillance.

3.5.4.1 Normative orientation

For instance, Hille Koskela (2004) suggests that surveillance can be experienced from both sides of the lens as 'fun', empowering or liberating. Especially in relation to social media, users want to be 'followed'. Visibility in this sense becomes empowering. This image of surveillance contrasts the predominantly negative image of surveillance stemming from the panoptic model. Following Foucault's own characterization of the panopticon as 'cruel', many surveillance

studies tend to replicate this normative orientation. They read surveillance a priori in a negative light. While pointing out important civil liberties issues, this tendency also functions as a limit for understanding contemporary surveillance. Failing to acknowledge the broad diversity of surveillance they also neglect certain surveillance projects or developments in policing that could be seen as positive or at least not as a priori negative developments.

Using the panopticon as an explanatory model tends to also portray citizens as helpless inmates subjected to an all-powerful gaze. As Bart Simon points out: "The panoptic structure seems to speak to the sense of helplessness individuals often feel in the face of the overwhelming force of institutions (prisons, hospitals, schools, workplaces, families) to determine life within their confines… the sense that there is nowhere to run and nowhere to hide" (Simon 2005, 3). This view then reinforces a deterministic view on technologically mediated surveillance with implications for the possibility of resistance and change.

3.5.4.2 The battle of many 'towers'

Other lines of critique of the panopticon draw on the problematic of the watcher. The panoptic model works with one central tower from which the observer watches all inmates. The multiplication of sites and technologies of surveillance question the unidirectional gaze of the panopticon. Haggerty points at transformations of contemporary surveillance towards a dynamic characterized by 'criss-crossing, overlapping and intersecting' views. He refers to the multitude of contemporary institutions that aggregate and disseminate personal data in various configurations, sometimes in competition with each other, undermining the clear distinction between the watchers and the watched. This insight speaks also to the pluralization of policing in which multiple public and private policing entities are developing surveillance projects, sometimes overlapping each other but also collaborating and intersecting in common cases. Surveillance is employing a whole set of information technologies but their operation and dynamics are not necessarily panoptic.

Continuing the problematic of the watcher, in the panopticon it doesn't matter who sits in the tower. Foucault credits the architecture itself for ensuring the automatic functioning of power by concentrating on the effects on the watched. He suggests that it does not matter who is doing the watching if the inmate feels watched. Even when broadening the understanding towards a "generalized mechanism of panopticism" (Foucault 1977, 216), ethnographic studies into police control rooms showed that it makes a big difference who is doing the watching and for what purposes. For instance, the study of Norris and Armstrong (Norris and Armstrong 1999) analysed the operation of video surveillance in urban environments. The analysis showed how the gaze is shaped by the predispositions, personal idiosyncrasies or biases of CCTV operators. This entails different levels of intensity for particular racial or ethnic groups, with implications for their welfare and their attitudes towards the police and public authorities. A similar study by Dubbeld (2004) who studied the surveillance of railway stations in a Dutch context reinforces these insights. In this respect Foucault's writings on the panopticon provide little insight in the attitudes and values of the watchers in surveillance practices.

Shifting the focus on the watched, Foucault stressed that the Panopticon works as a disciplinary mechanism if those being watched are conscious that they are under scrutiny. In the absence of or with little awareness that surveillance is being performed there is also no leverage for internalizing the rules. However, many surveillance projects work precisely by not disclosing these practices. This is particularly the case in policing. It is sometimes paramount for the success of an investigation that the suspect remains largely unaware of the categories, extent and precision of monitoring movements and communication.

3.5.4.3 Crisis with enclosures

While giving credit to Foucault for his analysis of disciplinary surveillance, Gilles Deleuze proposes that what we are increasingly shifting from discipline to control as a way of regulating society (Deleuze 1992). In his work he comments on the generalized crisis of environments of enclosure (factory, family, school, prison) in late modern societies. In this frame of analysis, combined with the rise of information technologies, Deleuze proposes the term *societies of control* as the new mode of regulating societies. "'Control' is […] a term for the new monster, one that Foucault recognizes as our immediate future" (Deleuze 1992, 4).

Deleuze paints his notion of control in contrast to that of enclosures: "enclosures are moulds, distinct castings, but controls are a modulation, like a self-deforming cast that will continuously change from one moment to the other, or like a sieve whose mesh will transmute from point to point" (Deleuze 1992, 2). Whereas the panopticon assumes immobility, the control allows mobility as it aims to manage the wider territory and not just the social space of enclosures. The deleuzian notion of 'control' employs mechanisms that "give the position of any element within an open environment at any given instant (whether animal in a reserve or human in a corporation, as with an electronic collar)" (Deleuze 1992, 4).

He proposes the concept of 'dividual' as key for understanding the shift from disciplinary to control mechanisms. For Deleuze, with the rise of information societies the individual has been doubled as code, as information, or as simulation. This phenomenon enlarges the decoupling between the watchers and the watched. Whereas in the panopticon the gaze was pointed at the body, as in the factory or in the prison, it is now the 'data double' that is analysed. This questions one of the basic premises of the panoptic scheme.

Deleuze associates this form of control with the proliferation of digital technologies and their capacities to process digitized personal data. Although he is careful not to characterize this relation in deterministic terms, he retains a foucauldian normative orientation by characterizing the mechanisms of control as 'the new monster'. In this sense, he acknowledges the important role played by information technologies in the dynamics of contemporary surveillance, making the 'password' his icon exemplar for understanding 'societies of control'. Unlike analysts who seek panoptic features in contemporary surveillance, Deleuze goes beyond, assuming the uniqueness of the characteristics of technologies employed in surveillance and their potential to raise new sets of questions.

3.5.5 The surveillance assemblage

Drawing from Deleuze and Guattari, Haggerty and Ericson propose the metaphor of *surveillance assemblage* (Haggerty and Ericson 2000). The metaphor characterizes surveillance as a rhizome-like structure growing like weeds, mostly underground and coming to the surface occasionally and surprisingly. Within this framework, surveillance is not directed by one centralized entity but is polycentric and networked. Data are being dynamically brought together from otherwise distinct data flows that move between nodes.

The surveillance assemblage does not imply that the data flows are randomly moving between the nodes. Instead, the metaphor of an assemblage points to a convergence of previously distinct flows, which are assembled for functional purposes (e.g. the aggregation of various databases in police investigations, the aggregation of traffic data or market information). This is, according to Haggerty and Ericson, the underlying characteristic of contemporary surveillance:

"It is this tendency which allows us to speak of surveillance as an assemblage, with such combinations providing for exponential increases in the degree of surveillance capacity" (Haggerty and Ericson 2000, 610).

Many contemporary and envisioned systems and developments rely on tagging, identification, profiling and decisions based on anticipating the next moves. Whether we speak of behaviour recognition, location tracking, crime mapping or of intelligence-led surveillance, *data doubles* are scrutinized, translated, categorized, aggregated and made ready for intervention. These data flows are fostered by computerization and the vast growth of means of identification and classification (biometric data, medical records, and location data).

On the one hand, the surveillance assemblage portrays surveillance as inescapable, announcing 'the disappearance of disappearance' (Haggerty and Ericson 2000, 15). This is signalling a process whereby it is difficult for individuals to withdraw from the monitoring of various public institutions and private entities. On the other hand, it avoids the image of surveillance as dominating and determined from a single point by inviting us to see also its polycentric and non-hierarchical aspects.

However, these concepts should not be seen as new generalizable characterizations of surveillance. As Haggerty comments in 2006: "I am wary of the prospect of developing a model of surveillance that can usefully be generalized to all or even a considerable number of surveillance contexts" (Haggerty 2006, 39). In this sense he seems to withdraw from the kind of generalizable claim made in *The Surveillance Assemblage* together with Richard Ericson, where they wrote that "We are only now beginning to appreciate that surveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole" (Haggerty and Ericson 2000, 610). The sheer complexity and multiplication of entities and agendas make it very difficult to aim for statements that speak of surveillance as being characterized by a set of features that hold across all instances.

3.5.6 Partial conclusion

Summing up these insights and notions, this study submits that an approach that draws from STS and philosophy of technology and accounts from the insights of surveillance studies is equipped to provide a more fine grained account of the role of technologies in policing. Instead of starting with metaphors of surveillance such as the Panopticon or Big Brother, this kind of analyses pay closer attention to various policing projects, systems, devices and differentiations on their actual uses, providing insights into the socio-technical ensembles of policing. In this sense, the approach announces to produce more nuanced discourses of surveillance in policing, avoiding a priori optimistic or overly pessimistic accounts, providing a better grip on the issues at stake and offering a handle for adequate recommendations and steps to take.

3.6 Positioning this book

There is already a growing body of literature that fuses the insights of STS and surveillance studies into analyses of technologically-mediated policing. This section reviews a number of studies that took this approach and ends with summarising the research areas of the following three chapters of the book.

3.6.1 Similar studies

Already mentioned above is the study of Lynsey Dubbeld (2004). She looks at the operation of CCTV surveillance in the Dutch context, while analysing the implications for privacy of these technologies and practices. She draws extensively from notions developed in STS to produce a more nuanced picture of surveillance in the Dutch train stations. However, she does not depart far from the methodology of the studies that take the panopticon as a starting scheme. While providing a valuable analysis of privacy and of CCTV operation, she starts with the Panopticon as an a priori framing of surveillance. This entails an analysis of the degree of panopticisim of the Dutch railroads video surveillance system.

Rosamunde Van Brakel and Paul De Hert analyse developments in policing in their insightful article on the 'pre-crime society' (Van Brakel and De Hert 2011). They look at some of the consequences raised by 'preemptive policing' while acknowledging the important role of technologies in these practices. For this analysis they acknowledge the insights of STS as helpful for understanding the complex but interactive relation between technologies and human behaviour (Van Brakel and De Hert 2011). However, they remain at the level of analysing various documents on preemptive policing and do not go very far in analysing practices from an STS perspective or in looking at the ways in which technologies interact with policing practitioners or they mediate their perceptions, decisions and actions.

In the introduction to the volume on *Technocrime, Policing and Surveillance*, Stephane Leman-Langlois dedicates a special attention to ANT. After dismissing technological determinism in the discourses on crime and policing, he proposes ANT for painting a new picture. Leman-Langlois provides a short but insightful summary of what an ANT approach could bring to understanding the role of technologies in policing and in 'technocrime'. However, he acknowledges that the authors in the collection "do not follow this view, and were free to adopt any theoretical framework they deemed fit for their particular subject" (Leman-Langlois 2012, 8).

A more substantive analysis that takes an ANT perspective to surveillance, including on a few policing practices and technologies, is provided by Tjerk Timan (2013). In his PhD thesis he looks at several technologies and practices in Dutch cities and includes an analysis of police-worn cameras and control rooms. Timan provides a detailed script analysis of the body camera worn by police officers as they patrol the streets. However, analysing public nightscapes in his thesis, he concentrated much on mobile cameras. Consequently, he minimised the role of other technologies in policing, especially those used in data mining, profiling practices and in geospatial analysis that significantly shape the presence of policing and consequently the landscapes of surveillance. Nevertheless, Timan's contribution provides a technology-respectful analysis, contributing to the enlargement of the body of work that takes a serious and in-depth look at technologically-mediated practices in policing. Bringing more detail on mobile camera surveillance he provides a perspective that steers clear from the tendencies of panoptic-driven analyses.

Francesca Gromme takes a similar STS approach in her analysis of surveillance practices but with a distinctive touch. She looks at a set of pilot projects in a few cities and sites in The Netherlands. Rather than aiming to develop a new generalized model of surveillance such as 'surveillance assemblage' or 'the panopticon', she analyses them as situated practices and provides "an in-depth analysis of the ways in which technologies are involved in the pluralization of surveillance" (Gromme 2012, 35).

For instance, Gromme (2016) looks at data mining practices employed in a pilot project by the community safety department of a Dutch city. She aims to contribute with an understanding of the ways in which technologies are used in these practices of 'zooming in' a population. That is, the community safety department aims to analyse in detail the problem of 'youth at risk'. She draws on Charles Goodwin's notion of 'situated improvisations' to analyse practices that employ data mining technologies. She argues that close views are inherently partial and do not produce a better view of the same object but perform a new object of intervention. In this sense she echoes Latour and Hermant's point in their analysis of 'oligoptica' where they show exactly how the perspective of local authorities in control rooms is framed, mediated and limited by a whole range of human and non-human actors.

However, focusing on neighbourhood level as the pilot did might not be the smallest level of concern to best illustrate this point. There are governmental and policing programs working on problematic youth at individual level, asking many more detailed questions about each person. Moreover, as she notes in her ethnographic observations, the police in this case study did not provide data about individuals to those involved in this project but only provided information about the neighbourhoods that youth lived in. This makes the argument vulnerable, especially as she aims for a general point about surveillance practices and, in this case, about all levels of closeness in police investigations.

In analysing practices of 'zooming in' aimed at understanding youth crime, she comments on the practitioners' discourse. She makes a normative claim about the proper unit of analysis by asking if their approach is creating a better view. However, she does not engage the literature on crime and place studies (Shaw and McKay 1931, Eck and Weisburd 1995, Clarke and Weisburd 1994, Sherman 1995, Weisburd, Bernasco, and Bruinsma 2009), which discusses extensively the subject of the unit of analysis in criminology. Nevertheless, the work of Gromme is thorough and insightful and takes the STS approach to practices and technologies in policing to a new level of detail and subtlety.

3.6.2 Moving forward

This study aims to increase the body of knowledge concerning technologies in policing. By drawing from and combining the insights of STS, surveillance studies as well as of the more recent research in philosophy of technology outlined in the above sections, this study analyses the mediating role of technologies in contemporary policing. It does this by studying socio-technical arrangements in a variety of organizational settings and policing styles and by exploring the role of a variety of technologies in policing practices. These technologies include well known and widespread technologies such as geographic information systems as well as more recent projects where police organizations experiment with new technologies and institutional innovations.

The following chapters of this book explore the ways in which various technologies participate in practices such as geospatial analysis of crime phenomena, in processes of enacting risky or problematic persons, groups or areas, in technologically mediated surveillance or in monitoring for and profiling suspicious behaviour. Instead of focusing considerations on one policing context, the following chapters analyse the mediating role of technologies in a diverse set of sites, technologies and policing situations. These span a broad range of European policing organizations, from local to national, concerned with multiple issues and crime phenomena,

from youth delinquency to road policing, and adopting a broad range of policing models, from community policing to intelligence-led policing and knowledge-based policing.

On the one hand, analysing a diverse set of practices within socio-technical systems helps to chart the networks of relations between police officers, technologies, organizational innovations and the legal frameworks in which they operate. On the other hand, following police officers and analysing the mediating role of technologies in these practices paints a richer picture of how officers perceive crime phenomena, how they act with and react to the output of technologies and how decisions are taken in technologically mediated policing.

The analyses explore in more detail what Bart Simon (2005) calls 'surveillance interfaces'. That is, the local, material sites, such as the computer screen, the camera lens or even the simple bureaucratic form. Extending this notion, the sites encompass all kinds of technologies in control rooms, in the hands of police agents or in the analysts' workplaces. The analyses look at the role they play in mediating police perception of crime, in processing data from incident reports, databases or sensor networks, in generating crime statistics or in running automated profiles. Focusing investigation on these sites can illuminate the processes through which someone or a group becomes a suspect as well as how and what are they suspected of.

The following chapters aim to produce thick descriptions of the ways in which suspicion is constructed in daily policing practices. This implies analysing suspicion as enacted in the networks of relations between police officers, technologies, legal frameworks, organizational arrangements and other factors that emerge in these networks. This means studying indicators and classifications of crime but also strategic and tactical intelligence products that guide where, when and for whom the police look for. This means steering away from discursive claims about neutrality of technology to potentially disclose issues of normative relevance embedded in technology design, in system categories or in risk profiles; it means analysing laws, policies and value statements and the way they are implemented in technology and in organizations; it means empirical substantiation of claims and detailed analysis of phenomena based on interviews and ethnographic observations.

3.7 Methods

This section gives a more elaborate presentation of the ethnographic research I performed in the study that led to this book. The sub-sections present the sites, the time intervals of the interviews and the typical interview structure, the sampling method and sample size, data analysis and validation as well as issues related to accessing sites. The section also discusses ethical issues related to performing research within policing premises and being exposed to sensitive police information and personal data in police systems. Besides the outline presented in this section, each of the following chapters provides additional details pertaining to the particularities of each site.

3.7.1 Sampling

For a study about policing, technologies, surveillance and suspicion I needed a diverse set of sites to analyse the role of technologies in policing practices beyond single systems and particular organizations. In the first phase I employed a purposive sampling of police

organizations that had the needed elements. That is, police organizations that employed certain technologies in their practices, ranging from the well-known (for instance geographic information systems) to the state-of-the-art (for instance sensor networks, social media monitoring and data mining).

The initial plan was to research similar technologically-mediated practices across multiple police sites in several European countries. However, the access was not uniform for all the technologies and practices. It turned out that not all technologies were available at all sites and also that access to these practices was not granted in all cases. In the end I managed to get in-depth access to one local police organization in Romania, two police organizations in The Netherlands and one constabulary in England. In addition, I performed six interviews with officers who worked in other police forces than those I researched primarily. The references to the latter were obtained through snowball sampling.

After gaining access to a site, the sampling of practitioners was done through a combination of selecting key informants and snowball sampling. Typically, an informant would introduce me to several other police officers that the informant knew to be involved in practices related to a particular technology. For instance, road policing units would 'deliver' me from a team to another after their shift ended. Or the head of a unit would present me to the agents in his department and ask them to accommodate my research.

The snowball sampling process also went from lower ranking agents to heads of departments. This happened for instance when I gained access to research a certain technology (e.g. GIS) and during that study I discovered that the organization also employed other relevant technologies (e.g. social media monitoring). In that situation I asked the interviewee to introduce me to the responsible official in the organization that could further facilitate my research access to the newly discovered practice. In this way, the snowball sampling method contributed to the selection of relevant interviews for each policing practice. The following sections include the detailed presentation of the sites, interviewees and technologies that I researched.

3.7.2 The sites

The main sites where I performed ethnographic research were in police organizations in The Netherlands, Romania and England. For practical reasons, I mostly requested access to police organizations in The Netherlands, where the research leading to this book was based. However, I avoided the drawbacks of focusing on only one police system (Jones and Newburn 2002) by covering a broader set of technologies and arrangements across Europe. In addition to police organizations in The Netherlands, I requested access at the premises of police organizations in England and in Romania[7], where I was granted the possibility to study a similar set of technologies and practices. In this way I was able to investigate not only the legal frameworks and procedure documents that specify how things should be but also look at how police officers and agents worked with technologies in their daily routines. I looked at how they interpreted the output of technologies and how these technologies mediated their perceptions, experiences and actions.

[7] On a personal level, researching and writing about this site is also a way of contributing to the society in which the author grew up and of benefiting from knowledge of the language and familiarity with the issues.

3.7.2.1 A Romanian local police

The gathering of empirical data began with a study at a local police organization in Romania. Using my native familiarity with the site and making use of personal connections I learned of a local police organization that employed a geospatial solution that their municipality recently implemented. The municipality is an important economic, industrial and cultural centre of Romania with more than 150 thousand inhabitants (in 2014) and a mixed ethnic structure. These characteristics made the local police organization of this municipality a relevant site for researching a wide-spread technology in policing (GIS) and the way it mediated police perception and action in a multi-ethnic city.

As detailed in Chapter 4, the gatekeeper to this site proved to be the head of the IT department of the municipality. He facilitated my access to the local police for a duration of two months between July and August 2010. Further on, he proved to be on good terms with the head of the local police and he volunteered to introduce me to him. In this way, the head of the local police was one of my first interviewees. He acted as a key informant and helped me to get a first picture of the systems and structure of their organization. Afterwards the head of police offered me a desk in the control room of the local police and he instructed the personnel to 'answer all questions' that I would have for the duration I was hosted there. From then on I spent daily between four to six hours in the local police station, either in the control room, in strategy meetings or during day (and night) shifts with field agents. In total I interviewed a number of four high ranking officers (including the head of the local police) and a number of fifteen field agents (eight males and seven females) and I spent roughly one hundred hours of participant observation among the local police practitioners.

3.7.2.2 The Dutch police organizations

In the Netherlands I first looked for a police force that also employed geographic information systems (GIS). Soon, I learned about a regional police force which used GIS in an innovative way. The municipal agglomeration had more than 300 thousand inhabitants (in 2010) with a diverse set of minority groups, being an important economic centre in The Netherlands with a highly developed industry and infrastructure. Therefore, it became a relevant site for researching GIS and draw contrasts and comparisons with the first site where I researched this technology in policing practices.

I first requested official access to the head of that police force. Still, I was prompted by the management of the organization to first obtain a general research access from the College van procureurs-generaal of the Openbaar Ministerie (i.e. Public prosecution) of the Netherlands. After being granted this kind of access I used it in several organizations where I requested access. In addition, each organization had their own local procedures and I was subjected to several screening processes.

After being granted all the approvals I returned to the regional police organization where I was first introduced to a head of department. He gave me a grand tour of the organization and he further introduced me to several other officers involved in various projects within the organization. In this way, I studied the GIS at this organization between September 2011 and January 2012. Throughout this study I learned about another practice in the organization that involved internet monitoring of youth groups.

Besides geospatial mapping of youth groups, the local police engaged in internet and social media monitoring of these youth. I observed the officers monitoring 'problematic youth groups' not only with GIS but also on the internet with social media monitoring technologies. As

detailed in Chapter 5, I was able to observe practitioners during their work and occasionally ask questions about issues that I found relevant or the practitioners highlighted to me as being important. I studied social media monitoring practices between February and September 2012 with some additional material that I gathered through interviews with officers in other Dutch police organizations. Among these, I interviewed one of the main designers of an innovative technological solution for internet monitoring. The solution was developed initially for internet investigation but was expanded towards more generic internet research for a larger set of governmental agencies and police departments to allow the gathering, storage, time-stamping and retrieval of internet information.

Finally, I studied Automatic Number Plate Recognition (ANPR) technology in the Netherlands, between September 2012 and February 2013, I looked at ANPR related practices in the 'Sensing Project' within the, then, Korps Landelijke Politiediensten (i.e. the National Police Services Agency). In this project, the police advocated an innovative way of combining ANPR and other sensors with profiling, in order to achieve real-time assessment of suspect behaviour. In the project I was able to interview ten officers ranging from high management to low ranking officers involved in the project as well as two police programmers involved in the design of the risk profiles that automatically signalled suspicious behaviour. The period spent at that site allowed me to understand both the principles and philosophy behind a police project that makes use of sensing infrastructures to infer suspicious behaviour as well as to investigate how police officers work with these technologies in their daily routines.

3.7.2.3 A constabulary in England

To gain an additional vantage point I researched ANPR also at a site in England which used the same technology. I chose the constabulary in England for being one of the first to implement ANPR and for having one of the most developed networks of such cameras when their 'ring of steel' was fully operational (i.e. in 2012 when I went there). I gained access to this organization for a shorter period of time (one week in June 2012) but I was still able to have a full program. I was granted the possibility to do participant observation sessions with ten road policing officers during their shifts (~16 hours of driving with them through their areas of responsibility), to interview two control room operators and one of the main analysts of the constabulary. As detailed in Chapter 6, this shorter but intense research period allowed me to contrast some of the practices and arrangements I studied in The Netherlands concerning ANPR. It afforded insights that moved the analysis beyond ANPR, towards the intricacies of the use sensing infrastructures in policing.

3.7.3 Interviews

During the time I spent at each of the several research sites I requested police officers for the possibility to conduct interviews with them concerning their practices. In addition to these, I interviewed designers and experts that were not formally associated to the police organizations where I received ethnographic research access. Instead they were referred to me through a snowball sampling process or approached during events, conferences, peers or personal relations. In total I interviewed more than thirty policing practitioners.

At the beginning of the interviews I asked the interviewee if I can use an audio recorder to record the conversation. I also asked them to indicate during the interview when sensitive information was discussed and consequently if I should turn the recorder off or anonymize the data. In the vast majority of interviews I was granted the possibility to record the interviews. In

a few cases I was prompted beforehand that I am only allowed to take notes. This data gathering method gave me the possibility to concentrate on the interviewee and it gave the participants the opportunity to freely describe their practices and their policing routines.

The interviews I conducted were semi-structured and lasted typically between one and two hours. The beginning of the interview protocol started with basic questions about the practitioners' background, role and tasks in the police organization they worked for. It then moved towards the role of technologies in their daily routines. In the second part of the interview typical questions that I asked were: "how did your policing routines change during the implementation of these innovations?" and "what do these changes mean for the way you do your work now?"

A third structured part of the interview began with questions about the way they perceive suspects and how they act on the entities presented by their systems as problematic, risky or suspicious. Typical starting questions during this part of the interview were: "Could you explain me more about what we see here on the screen?", "What does this indicator mean for you?", "How do you make sense of this crime information?" These kind of open ended question allowed the practitioners to explain in detail how they work with technologies. This gave me the possibility to probe afterwards with more in-depth questions about the meanings and perceptions they associate with indicators, reports, statistics or any output produced by technologies.

Doing in-depth interviews allowed me to investigate the motivations and experiences of officers during their work routines. Complementing a content analysis of policy documents, laws or internal procedure documents about how things should be, this method allowed me to draw inferences about the actual policing practices. These inferences, elaborated in the following chapters, may not align with the ways in which these practices are accounted for in legal frameworks and official procedures. It was particularly important in this respect to speak directly with the officers and agents about their work. This allowed me to address specific topics, such as their perceptions of suspicion and motivations for starting a monitoring procedure. These issues that may not be typically covered in detail in policy documents and could be complemented through observations and semi-structured interviews.

3.7.4 Data analysis and validation

The interviews and observations that I gathered were then transcribed and imported in a data analysis software. I used Atlas.ti, a well-known qualitative data analysis suite. This software solution aided me in the process of identifying key themes and for the discovering of relations between several interviews. During the data analysis process I developed both etic and emic coding. On the one hand, I derived a list of codes from the academic literature on surveillance, policing, privacy or philosophy of technology. As I will elaborate in Chapter 7 this etic approach enabled an analysis that cuts across the empirical material. On the other hand, the emic codes emerged in time by closely reading my field notes and the interview transcripts.

This approach enabled me to explore contrasts and similarities across participants as well as areas of agreement and disagreement between them. The combined coding allowed me to improve the validity of the findings by going beyond the biases that could have been introduced by particular officers and the ways in which they may have steered the interview (i.e. highlighting what they perceived as positive issues or downplaying the perceived negative ones about their organization or practices). At the same time, an emic approach fuelled the analysis

with rich and novel perspectives that transcend the themes from the academic literature on policing and surveillance.

The data analysis process was also fostered by the feedback given to me by various parties. For one, at the end of my research time at a particular site I typically shared my preliminary observations and findings with the officers and management staff themselves. As a way of 'giving back' I invited them to comment on my insights. This step offered very useful validations of my observations. At the same time, it contributed to the police organization through the insights they gained from our ensuing discussions.

Secondly, I presented the preliminary findings of the project in several iterations to the members of the Digideas project and to the members of the philosophy department of Maastricht University. This kind of feedback improved the academic grounding of the field work through refining insights and focusing analyses. The feedback received in these environments helped me to reflect on the validity of my conclusions and it often opened up new avenues of exploration of the empirical material. Also exposing my preliminary findings to other researchers contributed to decrease the influence of my own biases. For instance, having a Romanian background and performing research in Romania and encountering situations related to Romanians generated particular observations and points of view that had to be cross-checked for validity with fellow researchers.

Thirdly, I presented my preliminary findings to the broader audience of several academic conferences. The material developed in the following chapters also featured in papers that were presented to these audiences and published in books. The peer review process of these publications, through the multiple anonymous reviewers that read this material, contributed to improve the validity of these findings and often helped me to refine my insights and sharpen my analyses.

3.7.5 Ethical issues

When dealing with police information technologies that process sensitive personal data, several ethical issues come to the fore. First, the confidentiality of persons whose data I came across during the ethnographic research. Protecting the data of citizens, youth, vehicle owners and others was a precondition of being granted research access. In the accidental cases in which I came across such data I did not record it or I anonymised it from the moment of transcribing it. Second, the confidentiality of policing practitioners was an important concern. Each officer, agent or management official provided me with sensitive insights about their practices and organizational routines. Such details may not always align with the image that the organization as a whole wanted to project. Therefore, these informants could risk sanctions or their position within the organization. The reasonable protection of their identity was a concern for this research. Their names and contextual information that could lead to their identification were therefore anonymized in this book. Exceptions are those experts who explicitly approved of their names being associated with their claims. Third, the confidentiality of police tactics and operational information. When researching daily policing routines with an ethnographic approach I was bound to come across situations where the officers were involved in the surveillance of particular suspects and groups. Not disclosing the explicit details of this kind of information was paramount for the success of the operation and was part of the agreement to be granted research access to the police sites.

3.7.6 Results

The following chapters elaborate on the findings of this study concerning a range of policing practices and technologies. On the one hand, as typical for qualitative research, the analyses in each chapter aim to illustrate, highlight and contrast insights and discover new phenomena; in this case related to the mediating role of information technologies in policing. On the other hand, they withdraw from providing a new overarching model of how policing is structured or from painting a picture of police surveillance at European level. The approach taken in this book goes in line with Kevin Haggerty's concern that contemporary surveillance has become too complex to produce an overarching model that may hold across multiple surveillance arrangements (Haggerty 2006). The findings presented in these chapters do not claim to represent all the practices and all the officers in the host organizations. Instead, the more modest goal of studying particular policing practices, projects and organizations allows for concentrating on the role of technologies in concrete arrangements and for painting a rich picture of the active, constitutive role that information technologies play in contemporary policing.

Chapter 4

ReGIStering suspicion

4.1 Introduction

The previous chapter made an argument for studying technologically-mediated policing. With the growing influence and spread of technologies in policing we need to pay attention to the insights, approaches and concepts elaborated in philosophy of technology, science and technology studies and surveillance studies. In this way the chapter laid the ground for answering the first set of research questions presented in the introduction. What roles do information technologies play in police practices? In particular, how do they contribute to practices of assessing 'suspects' and how do they influence the practitioner's perception? This chapter makes the argument that rather than playing a mere instrumental role – as implied by a large body of policing literature presented in Chapter 2 – technologies actively participate in police decision making processes, rendering suspicion a socio-technical construct.

To substantiate this claim, the chapter analyses practices associated to a wide-spread information technology in policing, geographic information systems (GIS). In particular, it analyses one of the seemingly simplest of these technologically mediated practices, the geocoding and analysis of paper-based reports from field agents. The chapter sets its analysis within the organizational arrangement of a local police in Romania. The organization was open to provide the requirement documents of the system and, due to the novelty of the system in their organization, was able to provide recent insights in the changes and processes of shaping their GIS. The municipality of M city[8] introduced GIS in the local police in 2009 along with a CompStat-inspired management to complement their community policing style.

The analysis in this chapter takes as a starting point a small vignette about the geo-coding and registration of a paper-based suspicion report. The report arrived incomplete from field agents. Despite its incompleteness, the data operator submitted the registration in the system after filling in the missing fields with insufficiently justified data. The operator explained that the system prescribed all fields to have a value in order to finish the registration. Interviewing another agent about the geo-coded suspicion report it turned out to be about a young Roma boy. Asking her opinion about what the system retrieved, the geo-coded registration proved to mediate her perception of the boy, entailing a more alerted attitude.

From the analysis of this seemingly simple and mundane situation, the chapter provides a thick description of police practices, attitudes and arrangements in that organization, in order to understand how this situation came to be and to analyse its potential consequences. First, the chapter provides additional vignettes that illustrate how the system mediated the officer's perceptions. The system aggregated data about past events and displayed it on big screens, influencing the perceptions of officers about crime phenomena and the areas/times/offences/persons that they had to police. The chapter shows how the system fostered a cumulative effect, contributing to the erosion of the presumption of innocence, not only for individual persons (e.g. the suspected boy) but for categories of citizens (e.g. members of the Roma ethnic group). In this light, suspicion appears a socio-technical construct, shaped not only by the sensory perceptions and the informal categories of field agents, but also mediated by the system's design, configuration and output.

[8] To protect the anonymity and confidentiality of officials and police staff, the name of the city has been turned into M city. The same applied to the names of the GIS technology company and police staff throughout the chapter. M city is an important economic, industrial and cultural centre of Romania. It has ~150 thousand inhabitants in 2014 with a mixed ethnic structure.

Second, the chapter shows that although playing an active, mediating role, the system was shaped in its turn by a combination of social and technical factors, intentional goals and unanticipated situations. Upon further research, it turned out that the data introduction arrangement was shaped by the views of the management who wanted to promote the integrity of professional norms by building them into the technological design. However, these goals faced the financial and social challenges of the local police of M city. This process of delegation entailed a situation not previously anticipated by designers. As section 4.5.3 will detail, the analysis demonstrates that technology played an active role in the process but did not determine the outcomes all by itself. The GIS was not the only element responsible for the enactment of suspicion of the young boy but it worked the way it did in a heterogeneous arrangement of technical and social factors.

The analysis in this chapter draws on ethnographic observations I performed during July and August 2010 in the police station of 'M city'[9]. I observed and mapped the relations within the organizational, legal and architectural arrangements and between material configurations such as screens, cubicles and software-enabled entities in the information system. I gathered research data during the course of roughly 100 hours of participant observation sessions in various situations. These included day shifts and night shifts in the control room, street patrolling with field agents, data introduction sessions with office personnel and participating in strategy meetings where police management made decisions based on GIS-generated maps represented on big screens. In addition to these observations, the analysis draws from internal police documents and system requirement documents that were made available to me by the local police management. All these allowed for my close observation of work processes and relations between police staff and the technological equipment they engage with.

The chapter is organized as follows. Section 4.2 provides a more elaborate context of local policing in Romania. It includes a brief overview of police reforms in Romania against recent trends in security policies in the European Union. Section 4.3 presents a set of features of the GIS system of the local police of M city and its relations to the organizational arrangements, such as the data introduction procedure. Section 4.4 analyses how the system mediates the officer's perceptions on crime phenomena and the potential consequences of this mediation. Section 4.5 analyses the factors that contributed to the shape of the local police socio-technical arrangement. Section 4.6 discusses these findings in relation to the discourses of technology designers as well as the management staff and their initial expectations for the system.

4.2 The context of local policing in Romania

Local police organizations in post-communist Romania were established in the mid '90s as municipality services under the authority of local councils. As discussed in chapter 2, they function separately from the centralized national police having as one of their aims to regain the legitimacy of the police, long eroded by the authoritarian 'Militia'. As inspiration for their

[9] For reasons of confidentiality, I gave pseudonyms to the practitioners I interviewed. Those that feature more prominently in this chapter I renamed agent Alexandra and agent Camelia from the data introduction and officer Roxana, the main GIS analyst. Besides these and other agents, I interviewed the head of the local police and the head of the municipality's IT department.

models many municipalities looked for successful community policing organizations in western countries, following a general societal tendency towards western models.

In preparation for entering the European Union and NATO, and especially afterwards, the tendency towards western models implied an increasing synchronisation with new styles of policing and security strategies. As we have seen in chapter 2, over the past several decades, a broad trend in the policing sector worldwide has been the move toward more preventive and proactive styles (Tilley 2008). Although widely adopted, community policing coexists in practice with other police managerial strategies (Tilley 2009). CompStat, as a multi-layered approach, is characterized by both organizational mechanism for promoting accountability and performance among police staff as well as by giving geographic information systems (GIS) technologies a key role in crime mapping and operative activities. The employment of GIS is part of a larger trend in the police sector to benefit from technological developments in information technologies and foster efficient resource allocation at many levels of policing activity: strategic, tactical or operational (Ratcliffe 2008).

In the European Union, the promotion of proactive styles of policing and of information technologies in policing is manifest in security strategy policies, both at the level of the European Commission as well as of Member States. Identifying the cross-sectorial nature of threats, the European Commission calls for strengthened cooperation and coordination between European agencies, Member States and local authorities, as "even seemingly petty crimes such as burglary and car theft, sale of counterfeit and dangerous goods and the actions of itinerant gangs are often local manifestations of global criminal networks" (European Commission 2010b, 4). In Romania, national security strategy documents promote interoperability and interconnectivity of information systems, as they envision security threats to require proactive, anticipative and integrated operations (CSAT 2007, 4). Implemented gradually, these strategies promote the development of integrated information systems at both national and local government levels (CSAT 2010, 18).

In practice, the tasks of local police organizations in Romania involve activities such as preventing and combating street crime during demonstrations or public events, patrolling in parks and neighbourhoods, protecting buildings, monuments and other entities of public interest, identifying beggars or bringing homeless children to child protection agencies. Local police agents are responsible for handling contraventions and minor offences and delegate criminal offences to national policing agencies. In this arrangement, they can exchange information with national policing agencies about suspicious behaviour pertaining to a wide spectrum of criminal occurrences that they encounter in their tasks of maintaining public order. In order to understand the observations I made in M city concerning their practices, the next section presents a set of elements of the GIS design and of the organizational arrangements in the local police of M city.

4.3 GIS and local police arrangements

As outlined in the introduction, the local police of M city embraced a community policing style inspired (as the head of the local police mentioned) by Western community policing styles. Additionally, the local police implemented a CompStat managerial philosophy along with a new geographic information system. The system can generate a range of maps and reports based

on the geo-coded data. These are spatial-temporal data about persons, locations or goods that were involved in incidents.

The system was developed by a local partner of a global GIS corporation in collaboration with the local police organization of M city[10]. A review of M city internal police documents showed (in August 2010) a number of 144 change requests since the initial deployment (in 2008). The requests made towards system developers range in complexity from correcting anomalies and fixing bugs to adding and modifying design features.

For instance, one of the change requests concerned the addition of the category 'suspect' in data introduction procedures, which was not available in the initial design. As one member of the police staff mentioned to me during an informal talk, this was necessary as local police agents can stop a person and ask for identification documents as a preventive strategy, aimed at deterring criminal behaviour. Upon such a stop and identification, the agents have to report the name of the person(s), the location and temporal data of the event, the offence they suspected the person of and what led them to this assessment. This information is noted in a paper-based report and later registered in the system. Afterwards, this data can be exchanged with the national police as part of their inter-institutional protocols.

The approach to stop and identify a person is detailed in police tactics procedures. These specify that "the measure of interception" applies both to those for which "there are clues to have committed crimes" but also to those "assessed as suspect by police agents due to their presence at a particular place and time, their clothing, luggage or behaviour" (Șerb 2006, 68). Thus, the term 'suspect' in the local police information system refers to a person raising suspicion due to behaviour and other identity related attributes and not necessarily to a person connected to a known committed crime.

The national police can potentially use the information exchanged with the local police in solving crimes or providing leads that were otherwise difficult to find. In a typical situation of collaboration, the local police patrol stops and identifies a person whose behaviour or presence at a particular place or time they assess as suspicious. The national police may then benefit from this information if that person turns out to be involved in a crime dealt with by them. Without the data exchange the association with the potential crime would have been more difficult.

4.3.1 The "susp." notes

When I began participant observation sessions, in July 2010, local police agent Alexandra was working in the office as a data operator. She had the task to introduce the paper-based reports from field agents into the geographic information system. One of the first observations I made during these sessions was that many reports arrived incomplete and ambiguous from field agents. Some arrived without the precise address of events while others lacked part of the details of the incident. Agent Alexandra mentioned that the GIS requires a precisely defined location of events in order for her to place a 'pin' on the map in the process of geo-coding: "*Look how sloppy they send the information. Here it's just the street, no number, but the street is quite long. Here it's between number 80 and 120, quite some distance. And here it's "during the night of 28"but the night is quite long, isn't it? Anyway we put it in and for a strategic analysis is helpful.*"

[10] The system is currently advertised as a preconfigured product under a brand name, requiring minimal adaptions of the configuration for other police stations.

One type of reports caught my attention in particular as they contained only the note 'susp.' in the 'details' field, with no other specifications regarding the situation, reasons for assigning this label to a person or the type of offence. During the registration of such a note, after the entry of the date, location and names involved, the system displayed on the screen a drop down list containing types of offences (see Figure 1). After a small moment agent Alexandra chose 'Theft'. Noticing the absence of this detail in the paper-based report I asked agent Alexandra to explain her choice: "*The program asks for an offence to be specified before I can go to the next step. Probably the suspect was searching through the trash bins as an alibi for stealing, probably bad clothing, kind of walking, hair style. What else could he have done in the parking lot at that hour?*" Agent Alexandra then closed the registration of the suspect report and moved on to the next one in the pile.

Figure 1 – Example selection of types of offences in the local police system in Romania

I remembered the name of the suspect. Later on, upon my request, another agent, Camelia, retrieved the data collected about that particular person. We found that he was a young Roma boy, age 14. The system retrieved 5 entries reporting that he was stopped and identified for wandering late. However, none of the entries described suspicion of theft or of any other penal offence except the last one. I asked agent Camelia her opinion about the person given what the system presented. "*Obviously, a pickpocket (tr. pungaș). We've got to be very careful with them, especially when they hang around the touristic parts of the city*", came the response. I understood what her assessment was based on but I tried throughout the field research to understand this situation and its potential outcomes.

To be sure, this vignette depicts a situation representing only a potential first step in a long criminal justice chain with multiple possibilities for correction and adjustment. Moreover,

assigning the attribute ‘suspect’ to a person in the local police system does not necessarily entail the procedure of detaining the person. As confirmed by several officers and management staff, agents are instructed that the local police system may contain ambiguities or plain errors. However, the vignette does show that in daily practice the technological system mediated the agent’s perceptions (Verbeek 2011). As perceptions may influence their informal approach to persons, it is important to understand how did this situation came to be.

The following sections perform a detailed analysis of this short vignette answering two sets of questions. One set concerns the outcome and implications of this situation: how did the system influence agent Camelia’s perception on the young boy? What implications can follow from this kind of technologically mediated practice? What happens when policing practitioners have only the system as their information source? To elaborate the answers, the section presents additional vignettes with situations in which practitioners worked in front of the big screens in the control room, analysing crime phenomena based on the GIS-generated output.

The second set of questions concerns the factors that contributed to this situation: what influenced agent Alexandra in completing the registration procedure? What factors played a role in her choices? Was the technology the only factor determining this situation? What factors influenced the system design? To answer these questions the chapter introduces new observations that I made in the course of field research. They present different aspects related to the development and shaping of the information system in the M city local police. At the end of these sections the reader should have a richer tableau of the socio-technical arrangement in the local police of M city, supporting the main argument of the chapter.

4.4 Mediating the past

After retrieving the data about the young boy from the system, agent Camelia called him a ‘pickpocket’ (tr. pungaș). She looked at the last entry in the system where he was classified a ‘suspect of theft’. It turned out that this entry influenced her view on the other entries in the system. Despite the potential inadequacy of the last entry, the system prescribed agent Camelia’s attendance to the situation. She was inclined to quickly classify him in a category entailing an alerted attitude.

Of course, the situation was triggered by the interview question and it happened in the control room of the police station. However, if the retrieval of past data would have happened in the field, it is plausible that the system prescribed a similar perception of the boy. Still, in the field, the agent would have the possibility to crosscheck the system with the information they acquire on the spot. Despite the influence of the system, agents could see and hear additional details at the scene of the incident. However, what happens with police opinions and perceptions of incidents or of crime phenomena when they only have the system, mediated by the screen of the computer, as the information source?

4.4.1 The work of screens

To explore the active role of technology in shaping police perceptions I will now present a set of vignettes in which police officers met in the control room of the local police in order to make strategic decisions based on GIS information. In preparation for strategy meetings, the main

analyst was responsible for generating all kinds of thematic maps. For example, 'maps with scandals', 'the distribution of beggars' or 'incidents with cars' in a specific day/month/year. In order to identify patterns she compared the maps with those exchanged with the national police. All these practices were meant to provide the police management with suggestions about possible next steps concerning resource allocation.

I sat with officer Roxana, the main analyst, during her preparation of such meetings (see Figure 2 for a similar arrangement). Working in front of her screen, officer Roxana was generally absorbed in intensive screen interactions. She often moved with the pen over the screen, looking at each indicator that produced a brief description of an incident/person.

After analysing the details of each incident she took a broader view on the map of the whole city. She explained me the patterns she identified: "*At the beginning of the year* [2010] *there was a boom in thefts. Probably from the crisis or something, they suddenly increased. Look here, first week a slight increase* [Officer Roxana showed me multiple dots on the map circling them with the pen on the screen] *and then, boom, almost all the city and it stays for several weeks. Then we reacted by sending agents in those areas and did identification just as it was during the time of Ceauşescu: Everyone after a certain hour was identified as suspect. Look here, it's a week with a lot of thefts, nothing before, nothing after. It seems they tried the area but we were already alerted and sent patrolling squads*."

Figure 2 – Officer working with the GIS in a local police in Romania

Afterwards officer Roxana concentrated on a region in the city: "*Look how this area gets formed.* [She pointed with her pen to an area on the screen representing incidents] *You see this hot spot?* [She circled a bundle of dots on the screen with her pen]. *It stays for several weeks until we intervene.* [Then she showed me another map after their intervention] *Look how they*

move after our actions [To illustrate this she produced several maps for consecutive weeks]. *You can see how they cross the boulevard and move into this neighbourhood* [At this moment she seemed to assume that the dots of incidents represent a group or a coherent criminal phenomenon acting in response to police patrol routes]. *These established patrol routes look bizarre but they are not random. You could ask: why would we go at 2 o'clock in the night to this particular location? We decided to deploy patrols based on geo-location analysis showing the tendency of crimes to occur at these particular places and times*".

Officer Roxana made her analyses based on previously recorded data of geo-coded incidents. The quotes show a tendency of hers to rely on the system's output and the previously introduced data. This is suggested, on the one hand, by the vocabulary and the tense of the verbs. She used the present tense to refer to the elements displayed on the screen as if they were direct representations of reality: "they *move*", "look here, *it's* a week of a lot of thefts,", "you can see how *they cross* the boulevard". On the other hand, her reliance on the system is suggested by her vivid interaction with the screen. She pointed with her pen to areas on the screen as if they were the actual streets and districts of the city.

These quotes show that in her practice of interpreting the GIS-generated output officer Roxana 'black boxes' whatever happened in the street as well as the paper-based reports of field agents and the office staff registrations. Their partiality, inadequacy or error become ignored in her practice. This analysis confirms what has been highlighted elsewhere, namely that GIS can often blackbox inconsistencies, misrepresentations or alterations of data (Graeff and Loui 2008, Jenkins and McCauley 2006) that are easily ignored in the daily practice of GIS users. Going about their daily routines, practitioners cannot frequently afford to assess the data quality or question the system's output.

With these maps and analyses prepared, the analyst joined the strategy meeting. Such a meeting typically gathered the chiefs of departments, the head of the local police and the main analyst. All were facing the screen wall, where the analyst presented the previously prepared maps. These contained each type of offence represented by coloured markers. For instance, car incidents in red, begging in black, street nuisance in yellow, etc. A separate map, on a separate screen on the wall, displayed the data that came in from the national police.

The head used these maps to identify broader spatial-temporal crime patterns in order to decide the next steps in resource allocation. At one point during the meeting, the head of police asked: "*Why is that whole neighbourhood empty [of incidents], we used to have much more events there? Has it become so quiet?*" The response from the analyst followed: "*Rather that we're not there so much ... lack of motivation since the reductions* [i.e. Romania implemented abrupt austerity measures in 2010, involving 25% salary cuts and 40% personnel reduction in public administration]." The head responded: "*Yes, that's probably it. Next week we will make a special action in this neighbourhood on every offence* [i.e. in order to compensate for the reduced presence]".

The meeting was focused on the screens, with the head of police asking for all kinds of reports and maps, comparing them with each other and with those of the national police. For instance, he requested a map with the incidents from the same month of previous years in order to try to identify trends over longer periods. At one point he stared for several minutes, mentally being absorbed in the screens, with a silence that got the others stare at each other. "*Show me what happened one week earlier*", said the head of police, breaking the silence. He requested a map

which displayed the events that were geo-coded at the beginning of the same month of the previous year [i.e. 2009]. The analyst quickly generated the new map but did not remember any details regarding the displayed representations of events. The head of police looked at the screens and decided that all strategic orders and patrol routes stay the same.

These situations above highlight new aspects of the ways in which policing practitioners interact with technology. In this case, when the head of police doubts the apparent lack of offences in a certain neighbourhood, he allows the analyst to remind him of recent personnel reductions and demotivating salary cuts, better explaining what the system displays. When this sort of knowledge was not present (i.e. the analyst could not remember additional details from previous years), decisions relied solely on what the system displayed. In these situations, the system invited a particular kind of use, implicitly co-shaping the use that was made of it (Verbeek 2011). The officers' perceptions of crime phenomena is mediated to a large extent by the generated maps. When officers cannot remember other details that would allow them to question the system's output their decision relies on whatever the system displayed.

With the insights of this analysis we can now return to the vignette in which agent Camelia classified the young boy. In a similar manner she assessed the young boy as a pickpocket relying on the information that the screen displayed. The system 'black-boxed' what happened in the street and the translation processes afterwards. In this light, suspicion appears more than a mere social construct. Rather than forming in the heads of agents based solely on their sensory perception, it is also the system that performs what is a suspicious person or what crime phenomena/areas/times need more policing.

This socio-technical asessment of the young boy can have negative implications for his wellbeing when this data is retrieved at a later time. We have seen how the system's output influenced the policing practitioner's attitude and attendance to criminal phenomena. If retrieved in the field, this kind of output can shape the agent's attitude towards the person. If "he's in the system", the suspect is "obviously, a pickpocket". The system can thus induce an alerted attitude towards the person.

When the system blackboxes not only incomplete or ambiguous data but norms with ethical implications for whole categories of citizens, the potential for automated discrimination increases. The next section analyses this potential consequence of technologicaly mediated policing. In this case, some of the color codes for offences encoded generelized viewes about the Roma community in the configuration of the local police GIS.

4.4.2 Accumulating prejudice

As we have seen in the previous section, different colors represented offences on the GIS maps (red for car incidents, black for begging, yellow for scandals). The officer responsible for choosing these colors at the point of configuring the system was officer Roxana, the main analyst. While her choices for most colour codes were apparently random, it turns out that her choice to use a dark colour for 'begging' was not random. Upon asking her, the color code expressed her view that begging, especially by children and youth, is practiced by the 'dark skinned' Roma ethnic group. As she was the officer responsible for configuring the system, her views got inscribed in technology (through the colour code). From that moment on, the officers working with the system did not see only one black dot, as officer Roxana saw at the moment of configuring the system. These multiply in every weekly map with begging distributions

throughout the city. Through the colour codes, her inscription entails a cumulative effect: all begging is done by members of the Roma ethnic group.

I tested this effect by asking one officer his opinion about the way in which 'begging' was represented on the GIS maps. His answer was: "*I have no idea why they made it as it is* [but after a moment]…*probably from the skin colour*…". This answer, although triggered partially by the interview question, shows that the colour code embedded in the system evoked a general perception of Roma. The software-enabled entity of the colour code had the potential to induce an association with the ethnic group, mediating the perception of the officer that worked with the system.

The observation shows that, besides contributing to more efficient resource allocation, technologically mediated practices introduce their specific risks. We have seen in the previous section how the high-ranking officers made decisions based on the maps on the big screen. Both decision makers and GIS analysts presented a tendency to rely on the data displayed on the screens. The system prescribed the head of the local police to decide on the distribution of police patrols when the analyst did not remember any other details. Similarly, the analyst tended to rely on the screen when verifying individual incidents and persons or when identifying patterns.

Through data aggregation, the integrated information system can contribute to a cumulative effect with potential harmful consequences for persons or groups. This effect has been theorized by Manders-Huits (2011) referring also to Van den Hoven (1999) as *accumulative informational harm*. Manders-Huits borrows the notion of accumulative harm from Joel Feinberg (1984) and adapts it to e-government information systems that process personal data. Feinberg explains the notion of accumulative harm as being harm inflicted by a collective through the accumulation of multiple, seemingly harmless acts. For instance, Feinberg's illustration of the concept suggests that one person, walking on the grass, may not wreck the lawn but if enough people were to follow the exact same action, the grass would be unable to recover.

Manders-Huits argues that this phenomenon occurs also in the accumulation of seemingly innocuous bits of information. In the case of e-government information systems, she identifies more ways in which informational harm can accumulate. One way is through incorrect information stored in databases, either by malicious intent or recklessness by the government (e.g. careless implementations/data introduction) and/or citizens (e.g. supplying incorrect information). Another way is through errors of the technical infrastructure (e.g. unintentional effects of algorithmic classifications, loss of data). Through the aggregation of personal data, this kind of information gets combined. For instance, we have seen above how the aggregated information mediates the practitioner's perceptions, influencing resource distribution in the police or the informal attendance of agents.

Manders-Huits argues that this phenomenon contributes to a shift in power balance between government and citizens, rendering the latter more vulnerable. Data subjects are largely unaware of technological design choices and thus unable to consent to information use or to verify data quality. Data in information systems remains accessible to policing practitioners and can be used in different contexts. For instance, when used in strategic analyses, the maps and reports aggregate data both temporally (e.g. data from previous years) and spatially (e.g. begging distribution through the whole city). These maps prescribe decisions on establishing and updating patrol routes and police personnel. This amounts to policing certain areas and

times more than others. When combined with the colour codes, the GIS-generated maps may predispose an association of members of the Roma ethnic group in general with begging. This can reinforce negative perceptions and influence decision makers to delegate more resources towards policing this group.

In the case of the young boy, accumulative informational harm was generated by potentially incorrect information accumulating in the system. Agent Camelia classified him as a trouble maker interpreting the previously registered suspicion report. Still, the attribute 'suspect' in that report was not based on very solid reasons. For such individual cases, the system shaped her interpretation, jeopardising the *presumption of innocence* of the boy, potentially causing harm after the event took place. As we have seen in the above vignettes, when the officers forget or do not know the details of the situation, the system remains the dominant reference shaping their perceptions, giving them both legitimacy and force.

This does not necessarily mean that agents act on all system's suggestions. Some agents showed awareness concerning the legitimacy of the use of the 'suspect' category in the geographic information system. As one inspector mentioned to me, "*this issue of suspicion is one of the controversial issues. Why should you be in our databases because you were wandering late and because you were not from this city?*" The empirical data of this research do not support the claim that the local police of M city decided more policing of the Roma group based on the GIS-generated maps. Also there is no empirical data concerning other agents' attitudes towards the young boy. In other words, it is not a certainty that the system determines the same approach in other agents, as it did during the field research for agent Camelia and the interviewed officers. However, these sections did show that, more than mere instruments, technologies actively shaped the use that agents made of them. Suspicion in these examples was not something that only formed in the minds of practitioners based on their sensory perception but it was at the same time enacted by technology.

4.5 Determining agents?

The analysis so far made the point that technology in policing has the potential to actively shape the agent's perceptions of suspect persons, groups or crime phenomena. The vignettes showed how the GIS-generated output influenced the attitudes of practitioners towards persons or potentially intensified policing of certain areas/times/groups. But was GIS technology determining these effects? Is technology bound to bring about this kind of outcomes in policing? The following sections analyse what factors played a role in shaping the system design and the arrangement in the local police organization? In order to answer these questions, we will go back to the vignette with the introduction of the 'susp. note' about the young boy and analyse the behaviour and choices of agent Alexandra.

4.5.1 "The program asks"

As outlined in the introduction, agent Alexandra filled in data in the system without having details about the type of offences in the paper-based report. So, why did she proceed the way she did? A first answer to this question was provided by agent Alexandra herself. Her decision to select a type of offence was induced by the system design. She *had* to make a choice in order to finish the registration process. On the one hand, the system prescribed her actions in making

a choice concerning the type of offence. Even if the field report did not have the details, she needed to provide some input for this field. This situation is demonstrative of how technical artefacts *prescribe* dominant patterns of action (Akrich 1992). In this case, the '*script'* of the technology defined a framework of action in which agent Alexandra was supposed to act. This resulted in a situation in which she, as a data operator, was compelled to finish the data introduction procedure in the absence of enough data.

On the other hand, it may be too quick to conclude that the technology determined all her choices. The system constrained the data operator to make *a* choice but did not specify which choice should be made. Still, she chose "Theft" without this information being written on the paper file. While her choice could have been an inference from the increase in the number of thefts in the city, none of her assumptions regarding hairstyle, walking style, clothing style or behaviour of the identified person had a reference in the paper report. This observation entailed further questions during the field research: Why was agent Alexandra in a position to act as a data operator without enough data? Why was the system designed to prescribe the making of a choice?

4.5.2 Global corporations, local arrangements

Asking the head of the local police about the introduction of the system, I learned that the GIS induced multiple changes in the working routines of agents and analysts. Field agents received additional tasks when making the paper-based field reports. They had to fill in previously ignored details in order to facilitate GIS analyses. For instance, reports such as what kind of thefts were committed in an area, what kind of modus operandi tended to occur in an hour interval or what age groups were involved in incidents required all these details to be introduced in the GIS. The agents themselves were in the best position to know the details of the situations they attended. Following the Compstat model, the management of the local police required agents to introduce the reports in the system themselves at the end of their shift. So why was agent Alexandra introducing a big pile of paper-based reports?

It turns out that the initial arrangement had to be abandoned (see Figure 3). As the head of the police mentioned, the introduction of the technological system came against the specific challenges of their local police organization. On the one hand, the agents – often having a low level of formal police training – considered the procedure of geo-coding incidents too elaborate. On the other hand, the local police had a limited number of available workstations. No matter how well intended and prepared the agent, the lack of sufficient funding for the local police and the little number of workstations led to long waiting times for data introduction at the end of their shifts. The agents considered the task of data introduction as too tiring. The police management soon decided to delegate the task of introducing field reports in the GIS system to office staff.

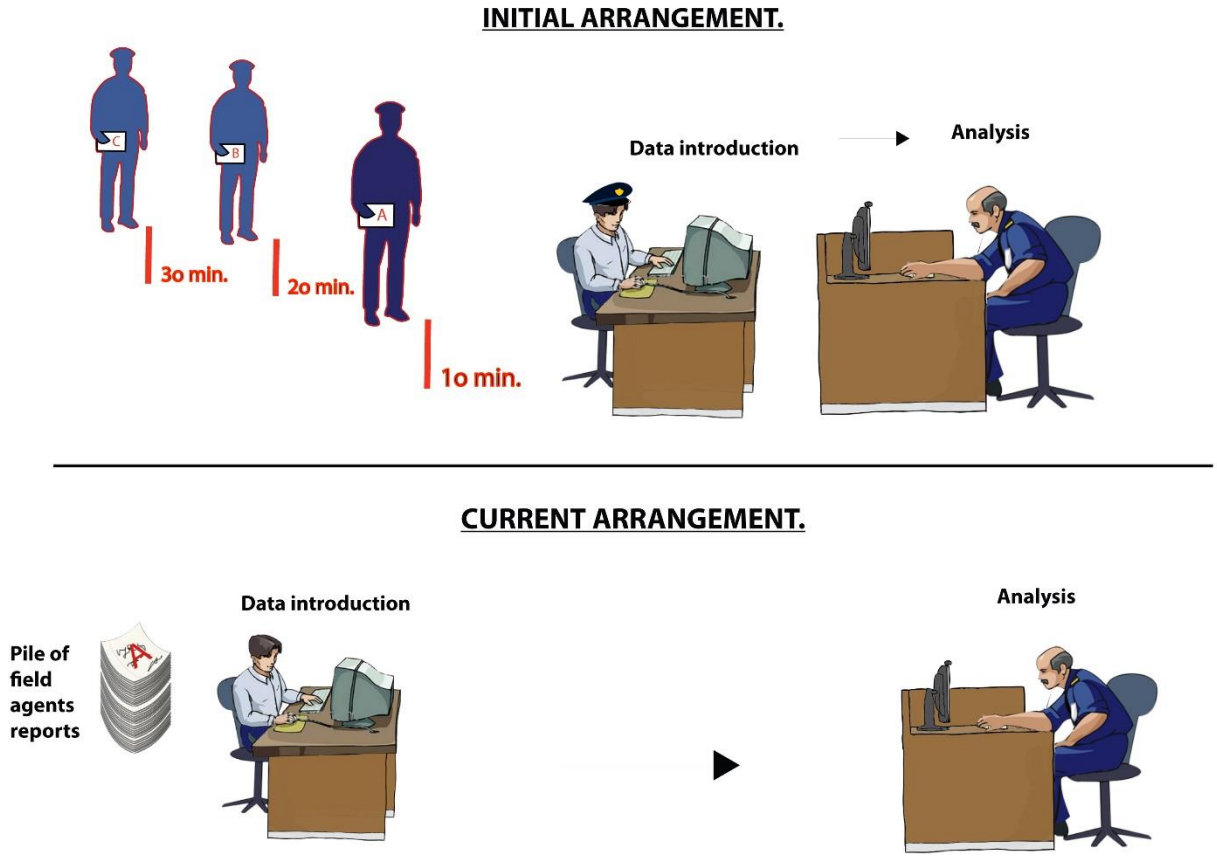

Figure 3 – Data introduction arrangements in a local police in Romania

Given the initial arrangement, the GIS designers anticipated field agents as the system users, endowing them with particular capabilities when *inscribing* predictions about the context of use (Akrich 1992). The specific design anticipated a context of use in which the field agents, with their close knowledge of the field situation were the represented users. As this task has since been delegated to office workers, the paper reports became the only easily available reference (except in situations in which the operators phone the tired field agents to ask for the missing details). At least during the period I was stationed in the control room, neither agent Alexandra nor other data operators requested these additional details. Although she had the choice of phoning the agents for the missing fields of each paper-based report, the socio-technical arrangement did not encourage her to perform this action. It turned out she was more inclined to finish the registrations by inferring a probable motive for suspicion despite the lack of references in the report's details.

4.5.3 Promoting the integrity of professional norms

But why was the system designed in such a way? Why the fields were made mandatory in the data introduction procedure? A first layer of answering this question can be found in the interview with head of the local police: to make sure agents enter all the details that they were required to pay attention to. The local police management requested to the GIS designers to inscribe constraints in the data introduction process, making certain fields mandatory – such as the one concerning the motive of suspicion.

A second layer of answers comes from the interview with the head of the IT department of the municipality. He was responsible with implementing GIS in the whole municipality, including the local police. He explains that the development of GIS occurred against the background of a broader vision to reform their public administration and maintain the integrity of professional norms. In this vision the system should not only increase the efficiency of resource allocation but also discipline the personnel to perform their tasks according to the established professional norms. The approach involved several measures embedded in technology: "*When it is freezing cold, the agents are, of course, tempted to enter a café, a restaurant or any building instead of patrolling the routes that we established. Monitoring them* [through the GPS units] *was in the plan from the beginning. Different forms of constraint are at work to make things turn. Not in the sense that you do something to hurt the persons* [i.e. the local police employees], *but that you determine them to do whatever they are supposed to do, for the money they receive*."

During the interview, he performed the development of this technology in their organization as inevitable, undeterred by individual resistance on the part of agents or by institutional frictions. As he mentioned: "*You know, it is not only the GIS developers that are making the whole thing work. It's also the Special Telecommunications Services* [i.e. the wireless data communication between the agents' units and the back office server was enabled by the infrastructure of STS, a national agency for special telecommunications]. *They* [the STS] *were not particularly glad to participate at the implementation of a system that was not by default part of their duties. But in the end they had to agree as they could have only postponed things. This is the direction, there is no other*".

The vision presented by the IT director to delegate measures for maintaining professional integrity to technology was implemented in multiple areas of the local police system besides the data introduction procedure. For instance, it turns out that the system's capability to track police agents in the field in real-time (both walking patrols and cars) was not only enabling dispatch inspectors in the control room to quickly send the closest units to incidents but also to monitor the whereabouts of each individual agent throughout the city. This was further enabled by the design of the cubicles in the control room. As the head of the local police mentions, these were designed at particular heights such that control room personnel could see the GPS screens from any point in the room.

The system logged the location data of the mobile units and generated histories of their movements. In this sense, the control room acted as a centre of calculation (Latour 1987) for all the data flaws that were gathered. Through the aggregation of these flows, the police management was able to both analyse crime distributions in the city as well as to assess if individual agents follow the established patrol routes and hours. As Officer Roxana mentions: *"In the beginning we did extensive checking of the itinerary of the agents. They did not believe that it is actually possible or that we actually do it. They turned the stations off; some broke the wires in the car units and meddled with the settings. Now we don't check as often as the agents also understood that the system works. After some of them were called on the 'carpet' (i.e. disciplining committee) the acceptance improved"*.

This kind of disciplinary measures did not only concern field agents. The system also monitored the office staff to do their job according to the specified professional norms. For instance dispatch inspectors had to introduce the dispatch jobs in the system as they occurred. That is, the input time of an event should be close to the time the event is reported to have happened. A too long time between the two moments indicated lazy inspectors who quickly note the events on paper and only take the effort to introduce them in the system at the end of their shift.

In a similar manner, maintaining the integrity of professional norms was also implemented in the data introduction procedure. Agent Alexandra acted as a data operator in a framework in which the completion of all the fields in the paper reports was a mandatory task for the local police agents. In this case, the goals of improving local police efficiency merged with disciplinary measures embedded in design and aimed at promoting the norms required by multi-layered geo-spatial analyses.

With the insights of this analysis, we can now understand how a broader set of factors combined and contributed to agent Camelia's assessment of the young boy. Her assessment was indeed based on the system's enactment of the boy as a suspect. However, the system's output was black boxing a broader set of factors built in the system. These included design choices that embedded disciplinary measures and which combined unpredictably with the challenges of the local police arrangement, where agent Alexandra had to make her choices.

Far from exhaustive in describing the socio-technical arrangement, this analysis shows that suspicion in these cases is neither determined by technology nor is it only based on the agent's sensory perception. Technology plays an active, mediating role but not a determining one. In such a technologically mediated environment, assessing someone as suspect becomes a process that combines social as well as technical choices and criteria, intentional goals as well as unpredicted situations. In this case, the combination of factors accumulated, with potentially negative consequences for the young boy and the Roma group. It is therefore important to trace the chain of translations between the discourses on technology of designers and managers and the concrete outcomes of technologically mediated policing. The next section discusses the findings against the discourses of technology designers and the goals they initially set for the local police GIS.

4.6 Discussion

The above analyses – of seemingly simple practices and daily routines related to a common information technology in policing – may seem like hair splitting. Not necessarily representative for all contemporary technologically mediated practices, they concentrated on the GIS system in a local police station in Romania. However, the chapter's focus was to render suspicion as socio-technical constructs. Even if there is no empirical evidence about the young boy being later arrested or discriminated, the chapter shows how the system mediated the perception of agent Camelia who showed a more alerted attitude towards him. The analysis demonstrated how the seemingly straight-forward assessment of the young boy was shaped by several socio-technical factors in the local police arrangement.

One of these factors that turned out to influence the practitioner's working routines to a significant extent were the views of developers and policy makers that were delegated to the technological design. The manager of the IT department (who devised the general IT policy of the municipality), the head of the police (who adapted the Compstat policing model), the main analyst (who configured the GIS), all had a role in shaping the socio-technical arrangement. Their discourses found their way in design choices, influencing the practitioner's routines.

As shown in the previous section, the vision of the IT manager concerning the role of technology in promoting professional integrity translated in all kinds of measures embedded in

the system design. His view about the reformative role of technology was presented against the background of its inevitability: *"This is the direction, there is no other"*. His conception of technological development was strengthened by the optimistic expectations of the others. Not only was the technology inevitable, it was also welcomed enthusiastically by the local police management. As the head mentioned enthusiastically concerning the inspiration for the system: "*We were inspired by the "24" TV series*[11]*. You can't stop watching them, it's really 24 hours watching*". Officer Roxana mentioned that this inspiration drove them to a solution that enables easy retrieval and visualization of information: "*We didn't think we'll reach the same level as we have seen there* [i.e. in the "24" series], *to type a name and get what milk he drank as a child, but setting our standards high got us here. When we first had the system working and saw everything on the big screen, we all said in one voice: Wow! It makes a huge difference to see in one glance a certain crime distribution instead of going through paper reports or even through Excel files*". They view the results of the GIS development as a great step forward in their practices.

However, as we have seen in this chapter, besides improving their practices, the technology actively influences their perceptions of crime phenomena, persons and incidents, with potentially unexpected and undesired consequences. Framing technological development as an inevitable force, following one direction and 'no other' exposes a rather determinist view on the social role of technology. This view found its way in their discourses and further influenced the system's development. As Van der Ploeg (2003) underlines, particular conceptualizations of technology serve different purposes in discursive strategies. In this case, optimistic discourses that highlight technology's inevitable development and undoubted benefits leave little space for contestation and resistance. As it turns out, significant resistance came from local police agents. At the same time, however, this discourse also leaves little room for critical analysis.

As it assumes technology to move forward independently from social factors, this discourse implies that technology determines the structure of the rest of society and culture. We have seen in Chapter 3 that technological determinism generally lacks an adequate conceptualization of the complex distribution of human and non-human agency. As a consequence, it has difficulties to account for problematic outcomes that go beyond mere system (mal)function or beyond training the personnel to 'properly use the system'. Therefore, technological determinism does not offer incentives to continuously identify problematic issues that arise in the dynamic appropriation of technologies in a flexible social context.

On the other hand, analysing technology *in the making* (Latour 1987), with a vocabulary accounting for different distributions of agency between human and non-human actors, allows for identifying chains of translations between the goals and expectations of technology developers and the outcomes yielded within the local police arrangement. As pointed out by Madeleine Akrich, it may be that actors define their own roles, despite the designer's inscriptions. In the case of the local police system, the anticipated actors did not come forward to play the roles envisaged by designers. The arrangement changed in the local police when the management delegated data introduction from agents to office staff, yielding a new situation, not initially anticipated. Rather than developing inevitably, the technology developed under the influences of a heterogeneous set of human and non-human (f)actors that needed to be analysed together.

[11] The action in the "24" TV series is centred in the high-tech hub of a fictional counter terrorism unit, where the staff work surrounded by screens and are able to simultaneously access information from multiple databases.

Pointing only towards poorly-trained agents and their idiosyncrasies and prejudices fails to account for the ways in which their behaviour is steered by all kinds of programs of action, human and technological, conditioned by discourses, procedures, organizational arrangements as well technological scripts charged with professional integrity goals. Pointing only towards procedures and legal frameworks, fails to account for the agency of practitioners to interpret vague regulation as well as for the technological affordances that are able to induce new behaviours and render previous regulation inadequate. Pointing only towards technology for its affordances to quickly aggregate and distribute (possibly erroneous or prejudiced) information fails to account for its appropriation in particular institutional arrangements and organizational contexts in which practitioners are able to use it in novel ways or not use it at all.

This analysis points to the need for transparency and ongoing analysis of socio-technical arrangements in policing. It supports some of the recommendations made by the European Commission in the debate regarding the reform of data protection legislation with respect to data processing by law enforcement agencies. For instance, recommendations from 2010 aim at ensuring that "different categories of data should be distinguished in accordance with their degree of accuracy and reliability, that data based on facts should be distinguished from data based on opinions or personal assessments, and that a distinction should be made between different categories of data subjects (criminals, suspects, victims, witnesses, etc.), with specific guarantees laid down for data relating to non-suspects" (European Commission 2010a, 14).

These recommendations are indicative of the risks that technologically mediated practices in the areas of police and judicial cooperation in criminal matters can have for citizens. The recommendations suggest the extension of the application of the general data protection rules to "include processing at the domestic level" (European Commission 2010a, 15). While taking into account the specific nature of policing activities, the right of access to personal data of citizens to be able to correct information should find particular emphasis in the data protection reform. In this sense, the argument of this chapter – that information technologies in policing play an active, mediating role in shaping the perceptions of practitioners about suspicious persons or behaviour – supports policies that recommend organisations to "clearly describe their subject access procedures" and "provide explicit protocols for submitting an access request" (Norris et al. 2015, 3).

Empowering data subjects to effectively exercise this right becomes even more relevant in a context in which security strategies emphasize the need for interoperable and integrated information systems to enable efficient operative activities (European Commission 2010b, 4). We have seen in this chapter how a local police organization was involved the classification and geo-coding of suspicion reports. The practitioners worked in an arrangement that allowed them to exchange data with other law enforcement agencies in order to help in preventive strategies or in criminal investigations. While not necessarily representative for all local police organizations, the findings of this chapter show that these arrangements and combined practices can yield problematic situations for individual persons and categories of citizens when data is interpreted in a remote context as a direct representation of reality.

4.7 Conclusion

This chapter focused on the geographic information system of a local police station in a city in Romania. It followed the policing practitioners in their daily routines. Through vignettes developed from observations gathered during participant observation sessions and interviews, the chapter highlighted partial and ambiguous registrations of suspicion (i.e. the vignette about the insufficiently justified suspicion of the young boy) as well as the work with colour coded offences on GIS maps (i.e. 'begging' coded with black dots on maps).

The analysis showed how the information in the system influenced the agent's interpretation of crime phenomena. This influence fostered a more alerted attitude towards particular individuals on the part of other agents who used the system. During strategic analyses, the GIS influenced decision makers in their resource allocation towards policing certain places/time/offences. In this light, 'suspicion' appears more than a social construct, generated by the culturally shaped categories and opinions of patrolling agents. Rather than forming only in their minds, based on hunches, local knowledge, justified facts, laws or prejudice, a suspect person or a suspicious group is also what the screen enacts as such. In this sense, suspicion can be distributed in technology, embedded in code, logged in classifications and displayed on screens.

At the same time, rather than solely determining outcomes, the technological system of the local police was shaped within a heterogeneous set of technical and social factors. For instance, the colour codes of offences were configured by the main analyst at the moment of setting up the GIS. Her views got inscribed into the technology. In this way, the socio-technical ensemble prescribed a generalization about the 'begging' practice of the Roma ethnic group, eroding their presumption of innocence and rendering them more vulnerable during encounters with agents.

In another situation, the management's vision to promote the integrity of professional norms among the local police personnel translated into multiple disciplinary measures inscribed in technology. The design of the data introduction process, which made the fields mandatory, was part of this broader vision of the municipality management. However, they did not fully anticipate how the system would be appropriated in the context of the local police of M city with its insufficient funding and personnel. These factors contributed to a situation in which the paper-based suspicion note about the young boy was registered without sufficient grounds in the GIS.

The chapter argued that evaluating individual factors separately fails to account for their complex intermingling in socio-technical ensembles. Therefore it makes a plea for transparency of design decisions as well as continuous analysis of the use and configuration of information technologies in policing. In this sense it supports the European Commission's recommendations that promote safeguards for different categories of data subjects as well as policies that empower the data subjects to make effective use of the right of access to personal data in police information systems.

Chapter 5

Sorting (out) youth

5.1 Introduction

In the previous chapter we have seen how technologies in policing play an active role in shaping the perception of officers concerning crime phenomena. The chapter built around the case of a young boy and showed how a classification in an information system performed him as a suspect and legitimised the views of police officers about him. This chapter takes the argument further. It asks what do technologically mediated classifications entail for police action? While the previous chapter focused on the case of a suspicion report about a young boy, this chapter explores a more systematic approach to the policing of youth. It argues that technologies mediate not only the perception of officers concerning problematic cases but in an alignment with policy and organizational factors they mediate police action, entailing intensified surveillance of large numbers of youth.

The chapter analyses data in The Netherlands where the prioritization of the issue of 'problematic youth groups' in 2010 on the Dutch government agenda entailed a proactive crackdown approach to sort out the problems generated by these youth[12]. While the analysis in the previous chapter discussed common place technologies and practices in policing (GIS are a familiar sight in many contemporary policing organizations), this chapter expands the analysis to new technological developments in policing. These developments are related to the exuberant rise of social media, especially among youth (i.e. Facebook, Twitter, Instagram, etc.). Social media monitoring technologies and associated practices are emerging preoccupations in many police organizations. At the same time, The Netherlands has one of the highest internet penetration rates, providing an adequate setting for studying social media monitoring by police organizations.

The chapter draws on ethnographic research that I performed throughout the year 2012 mainly at a Dutch police organization, which I name in this chapter Dutch Urban Police (DUP)[13]. There I was granted access to interview officers, agents and analysts involved in mapping classified youth groups with geographic information systems and in monitoring them with internet/social media monitoring technologies[14]. I gathered data in the course of sessions of around three hours with practitioners from the youth policing department, with some additional material from interviews in another police force. These sessions were participant observation sessions with me sitting in the vicinity of practitioners and able to observe their routines and ask questions throughout the session. Additionally, I interviewed one of the main designers of a dedicated police solution for internet and social media monitoring.

This chapter is structured as follows. In section 5.2 I give a broader introduction to the issue of policing 'problematic youth groups' in the Netherlands. The section includes a presentation of the method to classify problematic groups into 'criminal', 'nuisance' and 'annoying' depending on the gravity of their offences (Bureau Beke 2010). Then I make an inventory of the technologies with which the DUP organization and other partners gather information about groups. Besides geographic information systems and the multiple databases of the partners

[12] 'Problematic youth groups' is a term in Dutch policy making to designate groups of youth (considered between 12 and 25 years of age) that the police have associated to street nuisance and criminality.

[13] The DUP police operates in one of the biggest municipalities in The Netherlands. The city has more than ~200 thousand inhabitants. It is an important economic centre in The Netherlands with a highly developed industry and infrastructure.

[14] To protect the confidentiality of interviewees and of youth registered in police systems their names are made generic in this study. Officers and agents are renamed alphabetically (Anna, Bart, Cees, Dirk and Erwin).

involved in interventions (e.g. police, municipalities, public prosecutor, and child protection agencies) these technologies include internet/social media monitoring. This is because the proactive crackdown approach promotes the gathering and exchange of information about problematic youth groups in addition to classifying and mapping them.

To understand the policy context in which these technologies mediate police action and contribute to more surveillance of youth, I review an evaluation report of the crackdown approach. The report, published in 2013, assessed the proactive approach as generally being on a good track. Drawing on the drop in numbers of shortlisted groups it promoted extra emphasis on 'quick and effective crackdown' on the less problematic 'annoying' and 'nuisance' groups to prevent them 'slipping down to the status of a criminal group' (Van Burik et al. 2013, 21).

In order to show the mediating role of technologies in police action, we need to re-establish their role in mediating the perception of Dutch policing practitioners concerning these crime phenomena. Section 5.3 analyses in more detail a vignette that illustrates how a local police system enacted the reality of 'problematic youth' in an area and influenced a police analyst's perception of the phenomenon. In this situation, an automatically-generated statistic report showed a graph indicating a significant increase of 'nuisance youth'. The analyst was about to issue the report during the interview. Upon questioning him to explain the spike, the analyst retrieved the database records. He found that agents in the field classified 'youth that go through the gate without a valid ticket' as 'nuisance', designating a higher level of criminality than would be appropriate for free riding. This proved to be a repeated classification problem and consequently a counting issue. The automatically generated report mediated his perception on the phenomenon, performing it in a category that entailed the need for action and more intense monitoring. However, the above situation does not capture the monitoring actions that the police have eventually taken.

Section 5.4 draws on participant observation sessions with police agents practicing internet monitoring of youth groups. First, I show how the classified groups in the system mediate the start of the internet monitoring procedure. Although only classified for street related offences problematic groups are also monitored online. The police legitimizes its internet monitoring policy by interpreting street related activities of youth groups through the notion of crime displacement. This notion assumes crime as a constant phenomenon that shifts to other times and places. A low profile of youth groups on the streets becomes an argument for the police to include the internet among these places which fosters data gathering about youth groups from internet sources.

Second, I show that once engaging with internet monitoring, practitioners encounter new youth relations and new forms of groups. What becomes here a suspect situation, person or behaviour is mediated by metrics and features specific to social media: how many followers for the declared age, the clothing in a profile picture, etc. Not only are these indicators unrelated to street nuisance, but the very notion of youth group is challenged by these kinds of online relations between youth. Even if these indicators for suspicion are unaccounted for in the classification method that was used to select a group for more intense monitoring, they mediate police action, reinforcing incentives for monitoring.

Third and finally, I show that the incentives for data gathering are exacerbated with the merging of these practices with technologies for social media monitoring. These technologies partially automate the labour-intensive surveillance practices of police agents but also increase the scope and amount of data that is gathered as part of internet monitoring of problematic youth groups.

Concluding, I highlight in this chapter how technologies mediate police action but not by themselves. In an alignment with policy and organizational factors, they engender a translation of the issue of 'problematic youth groups' into an information problem, fostering proactive surveillance of a large number of youth. This socio-technical arrangement surely plays a part in explaining the yearly drop in numbers of problematic youth groups but at the same time it has an active, mediating role in enacting the very reality of this phenomenon.

5.2 The issue of 'problematic youth groups'

For decades, the issue of 'problematic youth groups' has been addressed by the police in the Netherlands. These youth have been a major source of irritation for many Dutch citizens due to their association with criminal activities, street nuisance, graffiti, loud noise and disrespectful and intimidating behaviour. The terminology and definitions, however, changed over the years. Terms, such as 'jeugdbendes' or 'gangs', were sometimes used but avoided at other times. When avoided, they were criticized for not capturing the variety of behaviour and for not being adequate for the Dutch situation, bringing too much reference to stereotypes of American gangs (Van Gemert 2012). Over time, the definitions also had consequences for policies, influencing the view on the statistics and approach to the phenomenon. For instance, Spergel writes: "Definitions determine whether we have a large, small, or even no problem, whether more or fewer gangs and gang members exist, and which agencies will receive funds" (Spergel 1990, 177 as cited in Van Gemert 2012). In the past decade a more neutral definition of 'problematic youth groups' has been adopted in official reports (Bureau Beke 2009).

The so-called shortlisting method is the result of the collaboration between the police and Bureau Beke, a Dutch consultancy bureau specialised in providing advice for policies on crime and safety issues. The method enables the police to have a more fine grained characterization and classification of youth groups, depending on their street related behaviour and activities. Youth groups are characterized by whole set of criteria such as their type (criminal, nuisance, annoying), the location(s) where they are seen by officers (who usually give the group a name based on this location), composition (size, ethnicity, age range), daily activities, risky habits (alcohol and drug use) and recent criminal behaviour. All this information is fed into forms by the officers on the beat. To shortlist a group, the method specifies that there must be repeated nuisance on the street, caused by more than two members, and the groups must be more than 'virtual groups, active on the internet' (Bureau Beke 2009, 18). New members or youth that are seen together with the group are registered as well upon encounters with officers. Once sorted, the police begin registering their activities with geospatial technologies in order to maintain a view on the phenomenon.

According to the shortlisting method, 'annoying youth groups' are groups that are seen to hang around the neighbourhood, are occasionally noisy or have accidental small arguments, which are usually finished quickly. Some of the members engage in mild violence and property crime. 'Nuisance youth groups' are groups with somewhat more pronounced, provocative behaviour (e.g. insulting bystanders). They may vandalize things more regularly and may not shy away from violence. They engage in minor crime and make an effort to ensure they do not get caught. The last category, 'criminal youth groups', contain youth who (at least in part) have committed more serious crimes (e.g. burglary, robbery, pimping). They often come into contact with the

police and are not afraid to use force. They usually commit crimes not just for status but also for financial gain (Bureau Beke 2010).

5.2.1 Approaching 'problematic youth groups'

Since 2009, all regional police forces in the Netherlands are required to centralize the statistics on shortlisted groups in their area. Still, early 2011, the Dutch Ministry of Security and Justice put the issue of 'problematic youth groups' high on the agenda. The ministry argued that these groups needed a dedicated focus with an intensified crackdown approach. The 'seven-step approach' (Bureau Beke 2010) went beyond mapping and classification to involve comprehensive interventions at group level as well as at individual group member level. A broad set of partners from the criminal justice chain and the child protection chain were involved in this approach (e.g. municipalities, public prosecutor, child protection agencies and the police).

Depending on the group classification, cases are handled in different ways. For instance, municipalities take the lead role in interventions for the 'annoying' and 'nuisance' groups, while the public prosecutor takes the lead for 'criminal' groups. Therefore, depending on the analysis of information about each group member, a juvenile offender may be subject to supervision and social reintegration measures but also face investigation, prosecution, trial and sentence execution (Borst 2013).

In either case, an important step in the approach is building a common understanding between the involved partners in order to get a clear view of the group's composition, relations and activities. In this step partners consult with each other and have to agree on which measures they need to take in each case. To inform these decisions, they share and use information brought forth by the police. This information varies from details about the street activity of youth to the inner motives and hopes of a group member. For example – as a police poster mentions – officers need to get the most complete picture possible on the person guided by a wide range of questions such as: 'What motivates a person? What are his/her dreams/talents/competencies? Is X active on the internet? Digital identity/ profile? Does he/she have multiple identities on the Internet? etc.' (see Figure 4)

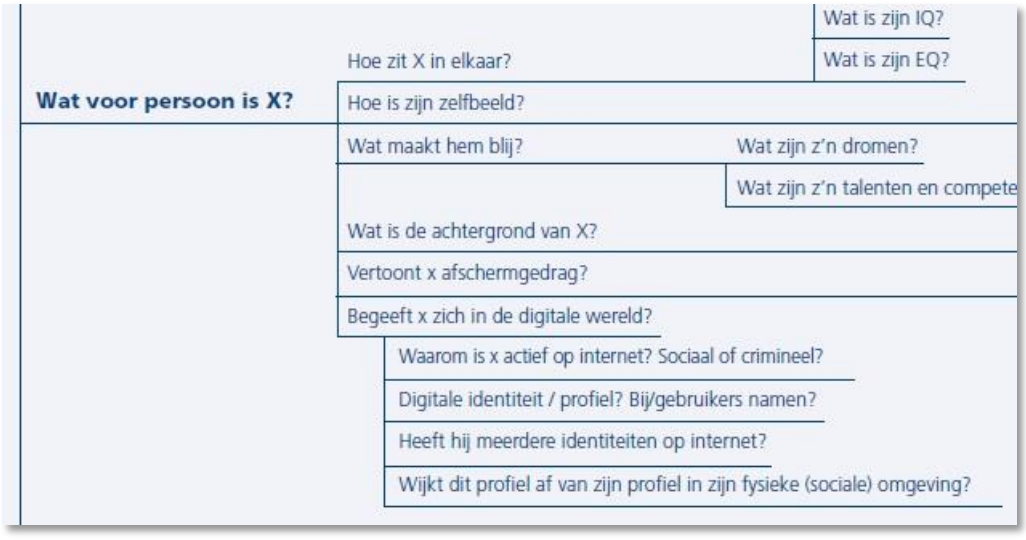

Figure 4 – Crop from a Dutch police poster on the person oriented approach

Partners look at information from geographic information systems, police databases, partner databases, the internet and social media (Bureau Beke 2010, 9). In this context, local police organization dedicated agents to the task of monitoring youth on internet and social media. These agents work in collaboration with other officers in the youth policing department.

5.2.2 Technologies for policing youth groups

In terms of technologies, the Dutch police organization where this study has been performed uses a geographic information system to map the incidents in their area. The system draws from data registered and stored in police databases and allows for plotting the output in several forms with the help of an intermediary operational database. Among others, it enables the policing of juvenile delinquency through the registration and visualisation of both youth groups and the individual members related to them.

The system allows the analysts to select a period of interest and generate maps with events involving the listed youth groups. Analysts can click on group icons to open a list of group members that have been registered at each particular encounter with field agents. The system enables analysts to correlate the youth group registrations with hotspots of crime, potentially producing a picture of the phenomenon that relates crime with a group's activity.

Concerning the internet activities of the youth groups, the DUP organization developed an extension of their geographic mapping solution to allow the registration of relations to internet and social media. That is, the registration file of each person in the system received an additional set of fields called 'internet identity'. In these fields, police agents register aliases, social media accounts, messages or relations. This feature enables the police to relate internet activity to shortlisted groups.

Regarding internet and social media monitoring, the DUP organization engages various approaches. For instance, officers set their own accounts on social media, trying to stay up to date with the activities of youth groups. Since a lot of information on social media is made deliberately public, police officers use it without the need to make a social media account (e.g. Twitter). When the information is not openly available, they try to obtain it by making fake social media accounts, allowing them access to more social media information.

The DUP organization also used social media monitoring technologies. These are software solutions that enable automatic gathering of information from multiple internet resources (e.g. forums, blogs, social media providers). Police officers employed them for monitoring the presence on social media of certain groups, movements, crises, locations, persons, etc. There is a wide array of providers for these solutions, freely or commercially available, competing through their features or packages.

In real-time mode, these solutions allow police officers to monitor social media for particular terms of interest. For instance, officers can visualize threads of discussion based on names of groups, persons, cities, regions, neighbourhoods, street names, and so on. Moreover, these solutions enable all kinds of metrics (for instance, how often a certain term is present in a social media discussion, from which key influencers or whether the discussion tends to have a positive, negative or neutral approach to a certain topic). All these real-time features can be used by officers in combination with off-line analyses to enable targeted internet monitoring practices concerning particular events, groups or persons.

5.2.3 Evaluation report of the approach to 'criminal youth groups'

At the beginning of 2013, a report commissioned by the Ministry of Security and Justice (Van Burik et al. 2013) evaluated the crackdown approach on criminal youth groups. It concluded that the multi-level approach is generally on a good track. Drawing from the annual statistics (Bureau Beke 2013) it reported a decrease in the number of youth groups that were listed as problematic.

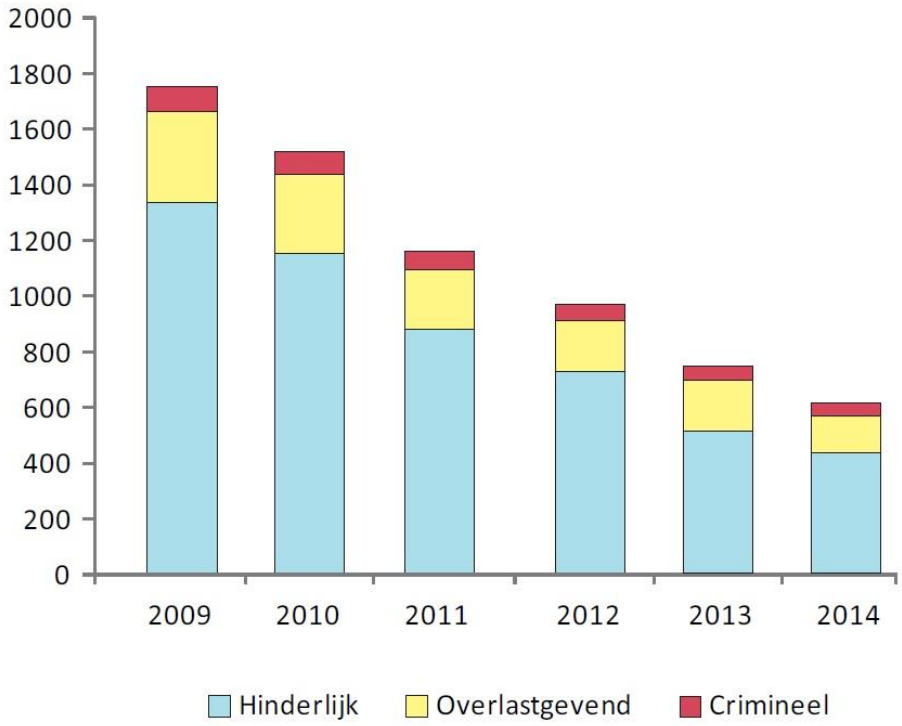

Figure 5 – Evolution of problematic youth groups in The Netherlands by number and type. ´Annoying´ in blue, ´Nuisance´ in yellow and ´Criminal´ in red. From Bureau Beke's yearly reports.

As Figure 5 indicates, the report shows a continuing drop in the number of cases in all categories of youth groups (Bureau Beke 2014). The report recommends further measures to be taken concerning 'annoying' and 'nuisance' groups to prevent them from 'slipping down to the status of a criminal group' (Van Burik et al. 2013, 12), because 'criminal' groups are harder to dismantle than 'annoying' and 'nuisance' groups. These figures also show that for each year the 'annoying' and 'nuisance' groups are the largest categories at the national level. For instance, in 2012 'annoying' groups formed 731 out of all 976 shortlisted youth groups. In 2014, 427 groups were 'annoying' and 163 were 'nuisance' out of all 623 groups. With group sizes varying widely between 10 and 100 members (Van Burik et al. 2013, 5) this is a total number ranging, for instance in 2012 between 10 and 100 thousand youth in these two categories.

The report also identifies challenges faced by the approach. It notes a lack of resources and personnel as a main challenge, affecting the capacity of the police to keep up with the dynamics of the phenomenon. Moreover, it notes the lack of a shared sense of urgency among the partners in prioritizing the approach, leading sometimes to late actions. The evaluation notes also that "a growth or drop in numbers of shortlisted problematic youth groups does not necessarily imply that the actual number of groups has grown or dropped." (Van Burik et al. 2013, 3). Analysing possible causes of inaccuracies, the report identifies the lack of expertise of police

officers working with the shortlisting method or the "increased police attention [which] may, for example, well result in more groups being identified" (Van Burik et al. 2013, 43).

Although the evaluation report raised many special points of attention, it did not have as a focus to evaluate the role of the technologies used in the approach. For instance, the role of technologies in the classification and geographical mapping; in the information gathering process, in the internet and social media monitoring process. In the report, technologies are largely taken for granted or mentioned very briefly. For example, although it notes possible inaccuracies in statistics, the report does not account for the way in which these numbers are locally produced, how the groups that get counted are created, visualized and classified in a category or another.

Another example of the way in which the role of technologies evaded the scope of the report concerns social media. They are mentioned (once), only as one of the factors contributing to the formation of criminal youth groups: "In the forming, disappearing and transforming of criminal youth groups, three factors or processes seem to play a role: […] (3) spread of 'gang culture' by (social) media." (Van Burik et al. 2013, 10). Although the approach includes a dedicated step for information gathering practices, including collection from internet and social media, the evaluation report neither addresses their role in generating statistics nor in the approach itself.

5.3 Practices of classification and mapping

In this context, this section looks more closely to the role of technologies in classification and mapping practices. To illustrate the mediating role of technologies in police action, we need to re-establish their role in mediating the perception of Dutch police officers. The section draws from interviews and participant observation sessions with two officers – renamed Dirk and Erwin – in their daily routines. The section illustrates the mediating role of the entities they work with on their computer screens. Although the icons of youth groups and the generated reports are the outcomes of a translation from 'groups hanging on the street', they mediate the officer perception and their focus of intervention.

5.3.1 "The probable perpetrators"

During one of the first interviews in the DUP organization I asked officer Dirk about his background and his tasks. He explained that he used to work as a field agent and that he often dealt with youth groups on the street. He used to engage them in discussion every time he encountered them on the street, trying to gather information about their plans, activities or composition. At the moment of the interview he was working in the office with the information system, trying to form a broader view on the phenomenon. He explained how youth groups are represented in their systems:

"Everything a police officer sees is always bound to a location.[…] So when I go to a group [Officer Dirk points to a group icon on the screen], *what the system shows is the location, the last location known, that the agents on the beat put in. Then I know that mostly they hang out at this location. [...] So the data they put in is shown here: the name of the group, the sort of group, whether they are criminal or annoying or nuisance". "To view it in the mapping system*

you have to have 'a group', 'a location' where the group hangs out with this particularly code 'hangp'. That's the place where they hang out. So I have to put it here, the location, this is the street and they [i.e. field agents] *have to put in a number, from 1 until 100 or whatever. Otherwise it doesn't show."*

Officer Dirk selected a period of interest. The GIS displayed a map with icons representing events with listed groups. He also generated a map with hotspots of crimes. Based on this combination he derived a picture of the phenomenon and related it to the group's activity:

"After a while we also identified the group here [Officer Dirk pointed to an area on the map designating another department], *in the neighbourhood of some bars and we saw a pattern of vandalism from here to here in the same time that they normally gathered here* [Officer Dirk pointed again with his pen to various areas on the screen to illustrate the connection]. *So, by identifying the group here and here and knowing the timestamps, we could also identify them as the probable perpetrators of this vandalism trail... Without any other analyses, we saw that it could probably be the group responsible for that trail".*

Working in front of his screen when drafting his analysis, Officer Dirk needed to rely on the information put in by other field officers, 'always bound to a location', and on maps produced by the system. As we have also seen in the previous chapter, what he visualized are coded entities on his screen. Their mapping is contingent upon a set of factors that need to be aligned.

Officers on the beat translate whatever they see on the street into program fields (e.g. 'hangp' designating the usual group location). When they encounter an already registered group they need to link it to the previously defined name and location (e.g. the Keiserstraat group), even if the group composition and possibly the name has changed. Because they 'need to have a group' they render it as a stable entity reinforcing its registered characteristics. Highlighting this process shows that the phenomena in the street are translated into other, software-enabled, entities visible on computer screens.

5.3.2 "Do we have a problem with nuisance here?"

As it turns out, this process faces a set of challenges that give a good glimpse in the technologically mediated character of this work. The following quote is taken from a participant observation session with Officer Erwin. Officer Erwin was working as an analyst and needed to report on the situation of problematic youth groups in his area. During the participant observation session he was about to issue a report showing a spike in 'nuisance'. The report was built around a statistic generated by the system based on the previously registered data.

[Before concluding the report I questioned Officer Erwin on the probable reasons for the spike. At first he hypothesized about possible causes (more parties, gang culture, the warm season). However, at some point he took the effort to search and read the database registrations to try to understand the automatically-generated graph. To both our surprize, he found that many registrations were categorised as 'nuisance' when other codes were more fitting, designating lower offences]

"It's good that we looked into that. Now we know. […] *They are all registered as 'melding overlast jeugd' (youth nuisance). It's the same. You see? He went without a valid ticket* [in public transportation]. *The problem with this kind of thing… I bet it's the same* [the officer checks another set of registrations]. *It's the same. So that's really a big issue here. So then in*

fact you could say: 'do we have a problem with 'nuisance' here?' No, I don't think so. Because all the registrations are about the tickets, that they don't buy a ticket.

[Officer Erwin got really engaged in this discovery] *I just want to check the other ones for 2011.* [The officer checks the set of registrations for that whole year]. *This is another one: 'Young guy was sitting with his feet on the opposite chair'. Not allowed. So they have to find another incident number to put this in the system, because this is really screwing up the numbers like crazy. […] So this really changes our view on nuisance. Same. […] Oh my God. This means in fact that I can throw the whole analysis down the drain".*

Officer Erwin needed to discard the report. However, the quote highlights more than mere challenges in working with police systems. This situation highlights some of the contingencies involved in the socio-technical ensemble of the police. It illustrates how systems enact certain realities. In this case, the report showing a significant increase of 'nuisance' in that area classified 'people that go through the gate without a valid ticket' as 'nuisance', which designates a higher level of criminality than would be appropriate for free riding. As Officer Erwin mentions, this proved to be a repeated classification problem and consequently a counting issue. This mediated his perception on the phenomenon, performing it in a category that entailed the need for more intense monitoring.

Without inferring from this reduced set of examples that national statistics are flawed, this section does remind that what we often classify and count are software-enabled entities. These classified entities, prone to partiality and ambiguity (Gerson and Star 1986) are built into our infrastructures and procedures, embodying a highly normative charge (Bowker and Star 1999, 4). Statistics based on these classifications also have normative consequences when taken up in policy making and translated into action as descriptions of reality.

This situation is illustrative of the point of John Law (Law 2009), who argues for a performative understanding of social science methods. That is to say, rather than merely describing reality, the methods through which statistical knowledge is produced also *enact* these realities into being. Instead of only reporting on phenomena, the methods make them into 'realities'. For instance, in our case, the police are the ones filling in the forms that entail sorting youth groups in one category or another and, at the same time, they are the ones responsible for sorting out problematic behaviour. Their classifications and conceptualizations produce in a way the phenomena, while the aggregation of numbers about these classified entities performs them at that level. And it is these entities that mediate intervention and monitoring.

5.4 Practices of social media monitoring

The internet monitoring procedure in the DUP organization specifies that 'having a group' in the GIS is the starting point of internet monitoring. Agent Anna, working in front of her computer screen, is responsible for monitoring 'problematic youth groups' on internet and social media (i.e. Twitter, Facebook, etc.). She explains her role and tasks: *"Being youth agent and [at the same time] surveying the internet is a great combination to have. To gain some value from what they put on the internet. The main objective of internet surveillance is being [there] before the criminal offense happens. That's why it's not called internet investigation but surveillance. To gather information. You don't have to have criminal offenses, but use it as an information source".* Therefore, the necessary condition to begin her monitoring tasks is that

she has to "*always have the group, like this* [she points to an icon of a group on the screen]. *We always start with a group that's already in the system".*

This shows the central role played by the notion of 'group' in the police procedure to begin the process of monitoring. 'The group', defined as a case in the system, becomes an obligatory passage point in these working processes (Latour 1987): necessary to begin monitoring but also sufficient, in the sense of legitimizing further data gathering.

5.4.1 Building legitimacy through displacement

However, in order to legitimize an internet monitoring policy the police needs to establish an additional argumentative step. While the internet monitoring of youth groups is a legal practice in The Netherlands, its legitimization builds on the idea that a form of displacement is at work. The hypothesis of this notion is that crime tends to shift or move to other places and times, either upon police actions or due to changes in the societal structure, but remains the same in volume.

Crime displacement can be largely classified into five types: 'temporal', meaning that the intended crime is committed at a different time; 'spatial', referring to the intended crime being committed in other places; 'tactical', which implies the commitment of the same crime but in a different way; 'target' which is about a different target then the one originally planned and finally 'type' displacement, referring to another kind of crime from that initially intended (Hakim and Rengert 1981).

This idea came to the fore in an interview with Officer Bart, the internet strategist of the DUP organization. He explained that with the rise of social media the police is not anymore encountering the groups on the streets. Still, not seeing the groups on the streets is not a reason to let them pass without surveillance. He argued that even if they are off the street, they merely changed their way of setting up whatever they used to do and this requires more effort in monitoring them on the internet:

"*That's what you get on the internet. You do not see that many youths hanging out on the streets anymore. Normally it was brewing: okay, they sit at the bench, talk, and then [do the problematic activity]! And now there's nobody at the bench. But they're still making contact, trying to communicate. And that's the different thing. Normally, we used to know the group by seeing them: okay, there they are. But now, where are they?"* [Officer Bart makes an assumption here that group members continue their problematic behaviour as they spend time on internet and social media, even if they keep a low profile on the streets].

The idea is known in informal police circles as 'waterbed effect' or 'balloon effect'. The quote of Officer Bart is indicative for the way in which the displacement hypothesis is sometimes taken up at the operative level. Not encountering a certain phenomenon (in this case youth hanging out at the street corner) made the officer more prone to translate the absence into the shifting of criminal activities to other places, times, tactics or types. The quote performs youth groups as still 'out there', setting up their activities, which continue to be of a criminal nature. Thus the underlying assumption of this theorization of crime dynamics is that crime among these youth remains a constant. In this way, it becomes an argument to increase the distribution of resources towards monitoring these youth on internet and social media.

5.4.2 New cases, new incentives

Once a group is selected for monitoring, the practice influences the monitoring of each of the members associated to it in the police system. This is because, engaging with the monitoring of a group translates into following its individual members. As agent Anna explains:

"Two things are important here: I look for individuals on the internet because they are a group [in our system]. But on the internet, they're not necessarily a group [i.e. a Facebook group]. They can be friends and that can be a group, but I'm not looking for a group called 'Berg group' or something. So I'm following the individual members, not necessarily a group."

During the internet monitoring practice, she interprets various indicators specific to social media in order to infer suspect behaviour. This practice often leads her to new cases and new situations loosely related to the initial group. For instance, in the following situation, agent Anna read several Twitter messages, pictures and accounts leading one to the other. She described a situation generated by a picture of a boy holding a pistol that incidentally came to her attention. Agent Anna traced the picture through various social media accounts to find the original account. The account proved to be related to a boy that used the picture to threaten his girlfriend. Given the content of the pictures and the reported threatening message, she decided to recommend to her colleagues that they bring the young boy to the station again for questioning:

"I follow one group on Twitter. And one day there was this message about a boy being arrested for threatening his ex-girlfriend with a weapon. It was retweeted many times. […] I found it looking into his followers on Twitter. And then somebody had this picture of a weapon [Agent Anna points to a picture with a boy holding what appears to be a pistol]. *I went to his Twitter and I found more pictures with weapons. So, on his account I found these pictures.* [Agent Anna points to more pictures with the boy holding pistols]. *I called the department and said 'Look what I found. We have to interrogate him again because of what I found here'. And we should confront him with that.*

When we brought him in he was this little boy crying that he's sorry and that didn't know it was wrong to have it. But if you take pictures like this, you're very well aware of that."

Interviewer: So he's dangerous now?
"*Well, he's not dangerous, but...he deserves the attention, for sure*."

On the one hand, this example shows that social media definitely play a central role for many youth of this generation. The quote performs the boy carelessly uploading even pictures with him holding weapons, failing to anticipate that the police was able to see them with very little difficulty. On the other hand the quote performs the police agent monitoring youth for social media related activities. The boy was brought in again not so much for additional offences committed on the street but for pictures he posted on his social media account.

During multiple sessions of participant observation agent Anna constantly assigned suspicion based on new kinds of behaviour, criteria and entities. Departing from the risky activities specified by the shortlisting methodology (e.g. graffiti, alcohol and drug use, and street nuisance) she interpreted pictures, social media relations, status updates or numbers of 'followers' for the different cases she was monitoring. Occasionally, she inferred suspect behaviour from these new entities with their specific normativity: too many retweets, high

numbers of 'followers' for the declared age, too many messages on a topic, the clothing in a profile picture, etc. These kinds of behaviour and activities were not necessarily problematic according to the shortlisting method, based on which the group was included for monitoring in the first place. Still, departing from a case legitimized the expansion of these internet monitoring practices.

5.4.3 Questioning the method

However, unlike the case of the young boy, the activities of many monitored youth are not related to criminal activities. Throughout this research, it became apparent that youth don't always continue their problematic behaviour when spending more time online. They also change their behaviour. Spending time on social media is part of this shift. They engage in gaming, picture sharing, sending messages, status updates and chatting *instead* of spending time on the street. As agent Anna documents as well.

"They put everything on here. 'Eating soup'. 'In a moment there will be the match', they put it in there. 'Ready with internship'. This one's obviously sick, because he says: 'being sick is the most awful thing', but then with a bad word, there it is. They say they buy things, so it gives me information about what they do".

This shift in behaviour from street nuisance to online gaming is also signalled by reports of other police forces[15]: For instance, the police in the city of Arnhem noticed a sharp drop in street nuisance and they linked this change to the increasing time youth spend on social media and online gaming. They note an experience they had during the release of a new computer game when street nuisance disappeared "like magic". They report that the nuisance by youth groups in the Arnhem streets have declined significantly. "It has never been studied, but we have the strong impression that the rise of social media has something to do with this" said the Arnhem coordinator for youth nuisance, Hans Klein Rouweler.

These observations are also in line with several critiques of the crime displacement hypothesis. Multiple studies show that, upon successful prevention programs, displacement does not necessarily occur (Clarke and Weisburd 1994, McLennan and Whitworth 2008). Other authors in police studies such as Barr and Pease (1990) argue that the notion is inadequate in the first place, as not all crime prevention results in crime being displaced. They propose the notion of 'deflection', which encapsulates the idea that crime can also be prevented even if it may translate in other forms of crime.

Agent Anna comments as well critically on the very shortlisting method used by the police. Not only do youth change their behaviour when engaging in online activities but the very notion of group fails to adequately account for this change:

"We're thinking that maybe we are running behind [with the shortlisting method]: In some situations we are saying: 'we cannot find our youth on the street. The groups are not there anymore. How is that possible?' And then she quickly answers herself: "*There is much more contact on the internet. They play a Playstation game, all that kind of stuff, online. They play*

[15] Wegwijzer Jeugd en Veiligheid, a Dutch portal on youth and safety, http://www.wegwijzerjeugdenveiligheid.nl/nieuws/details/article/jeugd-gaat-liever-gamen-dan-hangen/. Retrieved December 2012.

against each other from their own homes. And they also make more contacts [with other groups]. That's what I want to show: the groups are mixing…"

She argues that the police shortlisting method fails to account for the dynamics of youth behaviour. Once engaging in social media monitoring, she notices that the classifications of youth groups begin to dissolve. Groups seem to mix and this renders the distinctions made in the police system as not maintaining an adequate representation. In the following quote, agent Anna questions the size of a group, as registered in the system, by checking its associated members on social media:

"When they were in a group [on the street] *they usually stayed for a longer time, the changes were not that big. But now, if I check Twitter, for example, I look at the Keizerstraat group, 35 people are in* [the system] *as contacts of each other. I say: 'I do not believe that they are really contacts in the sense of friends'. So I will go and search for those 35 people on the internet and see if I can find whether they are really having contact through the internet and whether I can say, because of the messages they are sending, that they are friends. I dare to say that there are up to 10 people of that group that are really in contact with each other – and it's a real maximum".*

This quote forcefully illustrates the mediating role of the entities in police systems. A difference of more than 70% from the initial group size indicates a significant decoupling of 'groups in the system' with the online relations between youth. In this light, groups appear loosely defined and unstable, whereas the shortlisted groups fixed and too rigidly constructed. Although the procedure needs to start from 'a group' in the system, social media monitoring practices show multiple connections with other shortlisted groups and a mix of relations that is not accounted for.

"They often change more in the way they are constructed as a group".

"Then I saw the retweet and the retweet led me to him. And he is not part of that group but he belongs to a different group."

"I believe that this group is... [she stops to explain] *you have 'hinderlijk' ('annoying') and overlast ('nuisance')... it's one of these two. The group I follow is called Koningstraat, that's this one* [she points to an icon on a screen]*. And they are members of Hoogstraat group"*

"So the groups we had in the past, I think it's changing. And we cannot say in a short amount of time that this is that group, depending on that location. They are less location-dependent and the loyalty is different because of the contact through the internet."

"I think they are dissolving in a way that they are not that loyal to each other as they were when they were on the streets."

These quotes perform a much more fluid notion of group, compared to the one produced by the shortlisting methodology, which treats the group as much more fixated through name, location, or category. These 'dissolving' relations of youth in online environments have been also highlighted by other analyses of surveillance of young people on internet (Steeves 2012). These studies suggest that not only do internet surveillance practices perform youth differently but youth change their online behaviour over time, in part due to awareness of police monitoring.

In both situations, these new relations challenge the definition of groups and their classification. From the above quotes, we can see how a big set of group identity attributes – as defined by the shortlisting method – are performed differently by social media monitoring practices. The size of the group, its composition, kinds of relations, their stability or their relation to location are enacted differently, indicating significant transformations of the police notion of youth group.

This has implications for the aggregated statistics that are based on these groups. More mingled relations may mean fewer groups. Thus, the underrepresentation of social media relations in the shortlisting method leaves room for misunderstandings when reading numbers in statistics. This is especially relevant for the higher number of cases of 'annoying' groups. As the evaluation report shows (Van Burik et al. 2013), they remain proportionally the largest, but at the same time the least problematic category. Their characterization, according to the method, can easily encompass large numbers of youth that 'hang around the neighbourhood, are occasionally noisy or have incidental small arguments, which are usually finished quickly'. Their reinforced enactment as 'problematic' entails the need for their further monitoring. In its turn, this practice is gaining significant breadth and depth when amplified by the technological developments that afford increasing automation of this process.

5.4.4 Automating social media monitoring

As mentioned by Officer Bart, the police engage with real-time monitoring afforded by internet and social media monitoring technologies. Depending on the task at hand, practitioners see them as powerful tools to automate the labour intensive, time-consuming processes of information gathering. These solutions allow officers to program automatic alerts on certain events, crises, persons or groups, and to analyse the data even after it has been removed from the servers of the social media provider. Officer Bart described such a technological solution for social media monitoring that was purchased by their police force from a commercial vendor[16]. The solution is able to automatically monitor a broad set of social media providers, internet forums and websites for persons, groups or events:

"*They* [the commercial social media monitoring service] *make a super database. So if you say something on Twitter: "I'm going to kill X" and then a day later you think maybe that was not wise, I'm going to remove it. It will be in the Coosto database. They just download it. Coosto keeps everything. So they have 380.000 websites in Holland* [at the moment of the interview 2012]. *And that's a lot.*

For example, if there is an author that's very interesting, I make a search for everything the author said. [Or I can ask the program to] *give me a signal whenever he's talking 'house party'". Or I can say: give me everything this guy ever told on the internet. If he says something: "I'm going to kill the queen." I add this name to my search and know everything this guy said about the queen and any message of this guy. So I can play* [with these search criteria].

Or I could do a project about Hells Angels[17]. [For instance] we had a meeting of Hells Angels that had to be forbidden. The week before the meeting it was very important for us to know what

[16] Coosto is a Dutch based social media monitoring company, whose solutions enable "monitor[ing of] social media, including Twitter, blogs, forums and Hyves. More than 380,000 sources are visited daily and indexed. Coosto gives rapidly a clear answer to the questions: who, what, where and when? The results of Coosto are always available", Coosto website, retrieved September 2013.

[17] An international motorcycle club often known for riding Harley Davidson motorcycles.

are they doing, what are they talking about? So, we can make projects and organize our results so we can get them back".

With such a large amount of internet resources stored in a database the power to automate the search and analysis is interesting for the police. But the license to use the commercial service, Officer Bart explained, was expensive for their local police force and it also posed a security problem as they needed to send their queries of interest outside the police domain, to the servers of the provider.

In part for these reasons, the Dutch police chose to develop an internet monitoring solution themselves with similar functionality. Initially aiming for investigative purposes, the scope of the solution expanded to enable more generic research by a larger set of governmental agencies and police departments but only related to defined cases. Officer Cees, from the national police agency explained that the solution is set to allow gathering of information, storage, time-stamping and retrieval.

"The first approach was especially for investigation purposes, but now it´s broader, it´s more generic research for government agencies in general to gather information from the internet, analyse it, be intelligent with all the information. Don´t just look at a large pile of information, but try to find the semantics between it, the entities and the relations.

As soon as you suspect that you want to investigate possible incidents related to bike gangs or whatever, you have a case and you have defined it as case, even if it's not related to picking up people and everything else. It's just mining information and analysing information related to a possible incident or whatever. So it's a case, it's always a case.

If it's not related to a case, we are not allowed to keep it […] it should be gone after 24 hours."

Officer Cees explains that the solution that enables the police to monitor the internet is limited only to cases and does not give them a blank check to gather all social media information, compared to commercial social media monitoring solutions. In this light, the practice and design of the notion of 'case' becomes a crucial factor regulating what information is legally stored and what's not. The way a case's scope is defined has far reaching implications for the amount of data that is gathered. This is because only data not related to a 'case' qualifies for deletion on a short term basis ('24 hours'). The information that is gathered as part of a case ends up stored for longer periods and potentially this is exposed to the scrutiny of officers. When I asked the designer to give more examples of cases, these issues became clearer:

"Right now we're testing on the topic of the Olympics [the interview was taken in 2012] *to see what it is doing with all the information related to the Olympics. I can assure you that's a lot, even based on a few keywords. All the information related to the Olympics is stored as a history. But it's always case related. We don´t store the information that is not related to it."*

Admittedly, the action to gather of a large amount of information was done in a test. Nevertheless, the quote illustrates how the police has the capacity to define cases in a loose form and store a large quantity of information in relation to such a case. Moreover the issue of case design and its flexible boundaries becomes evident in the following quote:

Interviewer: What if in the course of a case and its development, the boundaries of the case are changing because you acquire new insights?

"That's very flexible, because the investigators in control can always, at any moment in time, add new information or add new searches or add new source material of which they think: hey, we know something."

Thus a case's scope and its technological translation can be loosely defined. Larger or smaller amounts of information end up legally stored as part of a case at hand. This aspect is regulated by users and procedures. Police officers can define and redefine cases as small or as large as they need. While the notion of case is traditionally associated to reactive policing and to aspects such as committed crime, the case's scope, case (re)definition, and case closing, these features are significantly transformed or lose their ground when they are translated in software code and employed in proactive monitoring practices.

With this insight we can return to the issue of policing youth. Being based on 'cases' for monitoring, this technological solution is compatible with the practice and procedure of monitoring problematic youth groups. This is because shortlisted youth groups are already defined as cases in the crackdown approach. Each shortlisted group is analysed and prioritized, with some getting selected for closer monitoring. This implies intensified internet surveillance with social media monitoring technologies as police departments extend their technological solutions in this direction (for instance the DUP organization acquired and used a commercial social media monitoring solution).

Several points can now be brought together. Internet and social media monitoring practices perform new forms of groups and new ways of inferring suspicion. In a policy context which recommends '*getting the most complete picture possible on the person*' (police poster), and an organizational context lacking resources (as analysed in the evaluation report), automated solutions predispose the police to delegate more 'cases' to be monitored with automated technologies. Even if surveillance is announced to be only case-based, as opposed to monitoring all social media activity, this does not limit the expansion of their number or loose definitions of cases.

This section highlights the pivotal of the notion of 'case' in mediating proactive surveillance practices. The aspects in which case definition plays an active role include their scope (what belongs to a 'case', how and who expands it), their lifecycle (how is it redefined, when is it closed) and their translation in technological implementation (what data can be gathered as part of a case). Given their capabilities to increase the scope and depth of data gathering it is important to critically assess the method through which youth groups get classified and enter the scope of automated surveillance. Otherwise, once enacted as a problematic group, the youth have a hard time invalidating the conditions for which they were placed under monitoring; even when the reasons for which they were selected in the first place are not present anymore.

5.5 Conclusion

This chapter analysed practices and technologies involved in policing 'problematic youth groups'. In line with the evaluation report (Van Burik et al. 2013), analysed in section 5.2.3, it showed how classifications and aggregated statistics on shortlisted groups do not simply mirror the dynamics of the phenomenon. That is, a variation in the number of groups reported by the shortlisting method may not necessarily mean that there are in fact fewer or more groups from a certain category. Rather technologies and practices play an active role, mediating the ways in which youth groups are performed as 'problematic'. Practices of classification produce the entities that are counted. This insight points not only towards difficulties in the method but proves relevant for the amount of resources allocated to monitoring.

Proactive policies promote enhancing information exchange and early signalling on the larger sets of 'annoying' and 'nuisance' groups (Van Burik et al. 2013). Against the background of a broad adoption of social media by youth, police officers tend to use the notion of 'crime displacement' to explain why they see less groups on the street and why they are still justified to monitor their internet behaviour. Once engaging with social media monitoring, police agents encounter new youth relations and new forms of groups. At the same time, they define new indicators for suspicion. What is a suspect situation, person or behaviour is mediated by metrics and features specific to social media: how many followers for the declared age, the clothing in a picture, etc. Even if these are unaccounted for in the shortlisting method that was used to select a group in the first place, they predispose the police to find more cases and thus reinforce incentives for monitoring.

The chapter showed how these incentives are exacerbated with new technological developments for social media monitoring. These developments enable the automatic gathering of a large quantity of online data. In this way they promise to reduce labour intensive monitoring processes. The police designed their own solution and announces to use it only on 'cases' that require it, as opposed to monitoring all social media activity. However, 'problematic youth groups' are already defined as cases. This quickly expands the scope and depth of their monitoring and easily integrates in organizational procedures and technological designs. The norms shaping this arrangement are not only to be found in legal provisions and policy documents but hidden in the details of technology implementation. Therefore, particular alignments of technological, organizational and policy factors mediate police action, fostering automated monitoring and data gathering. These factors together engender a translation of the issue of 'problematic youth groups' into an information problem, fostering automatic (social media) monitoring of a large number of youth.

Chapter 6

Sensing suspicion

We have seen so far how various technologies mediate police officers' perception and action and that these technologically mediated practices entail outcomes that are often charged with a high moral load: increased risk for discriminatory actions towards ethnic and racial groups; intensified surveillance of already labelled persons, groups or areas; breaching the privacy of large numbers of people, eroding the presumption of innocence of communities and groups during encounters with the police. With limited possibilities for the police officers and agents to anticipate and change the output of the technologies they use, the later actively influence their perceptions and actions.

In this light, the design of policing technologies becomes a process a process of doing ethics through design. That is, the code enabling programs and algorithms partly shapes the concrete choices of police officers in action. When developers and programmers acknowledge this insight and take responsibility for the outcomes of technologically mediated practices, developing technologies becomes a process filled with ethical choices. We have seen for instance in the previous chapter how the Dutch police sought to restrict the use of their social media monitoring technology to previously defined cases in order to limit mass surveillance of internet users. Technology, in this case, was designed to incorporate legal restrictions and to mediate police action towards minimizing unjustified surveillance. Most social media users, who do not fit the criteria of cases and profiles, would not have their data collected. The process was therefore aiming explicitly at translating legal norms and moral values in technological design. But what values and norms were at stake?

6.1 Introduction

This chapter investigates the building of values in design and asks how developers of police technologies explicitly build values and norms in the design of policing technologies and what are the ethical implications of this practice? As the following sections will detail, the chapter analyses police efforts to embed privacy protection in design. The chapter expands the scope of the analyses of the previous chapters by accounting for data gathered from sensors pervasively distributed in the environment. In particular it focuses on road surveillance technologies (Automatic Number Plate Recognition, ANPR) in England and the Netherlands and discusses initiatives to implement the idea of 'privacy by design' in police sensor networks. The chapter argues that the right to privacy can be protected by design but in combination with organizational arrangements, legal provisions and a privacy protective mind-set of policy makers and developers. However, without such concerted efforts new ethical issues continuously arise in these practices due to the dynamic, situated and mediated character of suspicion in an environment pervaded by ubiquitous sensing technologies.

To support this argument, the chapter analyses a police project that spent a significant effort in explicitly aiming to reduce the impact of privacy invasion while performing their policing tasks. The chapter draws on ethnographic research performed in the Sensing project within the, then, Dutch national police (KLPD). In this project, police officers engaged sensor networks together with profiling as a way to identify suspicious behaviour in large flows of data (Schakel, Rienks, and Ruissen 2013, 179). In particular the project gathers and processes live data from the road traffic in The Netherlands with ANPR technology as they regard ANPR as one type of sensor amongst others (e.g. of internet traffic, railways, waterways). The difference that sets this project apart in terms of privacy protection is that it selects profiles of suspicious behaviour

before storing all traffic data. Profiles are built through knowledge sharing between multiple branches of the police and not through data mining and a priori bulk collection of data.

To contrast the promises and challenges of this kind of projects, the chapter uses some additional material from a constabulary in England[18]. At the time of the study (2012) this constabulary had one of the densest networks of ANPR cameras in the UK. With its ANPR 'ring of steel' fully operational the system was storing traffic data in bulk for several months. Still, the UK Information Commission Office (ICO) ruled the system unlawful and argued that the ANPR 'ring of steel' was a serious breach of the right to privacy as it stored data of traffic participants for long periods of time and from an abundant network of cameras (Cambridge News July 31st 2014). While the UK constabulary temporarily turned off part of its ANPR cameras in response to sustained criticism of its mass surveillance practices, the Dutch police started to explore innovative ways of engaging ANPR, promising to protect people's privacy by design while simultaneously performing their policing tasks (Hellemons et al. 2013). While both police services employ a similar ANPR system, purchased from the same vendor, they differ in the way of engaging this sensor network.

In both organizations, I performed semi-structured interviews with members of the ANPR teams to understand how technologies mediate their perceptions of suspicion and action on specific vehicles. There were ten in-depth interviews in the Netherlands with the lead designers of the Sensing project and multiple police officers involved in ANPR operation and 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 both settings for more than 50 hours taken together. For one, these included participant observation sessions in control rooms to understand how the system mediated their operative decisions. Additionally, I participated in actions with road policing units with marked and unmarked police vehicles to understand how police officers worked with and talked about technology and how it contributed to the enactment of suspects and of suspicious behaviour. Instead of assuming deviance and suspicion 'out there', ready to be discovered, this study investigated the ways in which suspicion was enacted. That is, it looked at suspicion as both actively described and produced within these practices.

Tracing the enactment of suspicion in technologically-mediated practices is especially relevant for understanding the ethical implications of implementing privacy enhancing technologies in sensor networks. That's because these technologies are often regarded as the solution to achieve both crime control and privacy protection. For instance, a vision document of the Dutch police sees technologies as the solution to "prevent an unnecessary infringement on the privacy of people who are not under any suspicion" (Hoogewoning 2006, 79). In other words, suspicion and the way it is enacted in policing becomes a 'gateway' to the revocation of privacy. Preventing 'unnecessary infringement on the privacy of people' through technological design can also be read from the other direction: who *is* under suspicion can have their privacy rights legally lifted.

While strategies to operationalize 'privacy by design' (Kroener and Wright 2014) provide ways in which privacy by design should be practiced, this chapter looks at the ways these technologies work in practice. Although multiple studies took an ethnographic approach to study technologies and surveillance in policing organizations (Norris and Armstrong 1999,

[18] To protect the confidentiality of the individual police officers the name of the organization is not revealed in this study. Exception is the Dutch national police force, which is one for the whole country. Still there, the names of individual officers were made generic.

Sanders 2006, Manning 2008) few of them, as of yet, analysed the more recent attempts of policing organizations to practice privacy protection by design.

The rest of the chapter is structured as follows. Section 6.2 provides a background of the idea of privacy by design and its contemporary legal status in the European Union. Section 6.3 gives a brief introduction to ANPR technology and shows the mediating role of ANPR in policing practices. Sections 6.4 explores profiles in action and contrasts ANPR practices in the two policing organizations. Section 6.5 discusses the designing of profiles and the ethical issues that persist. It analyses situations that span the use of ANPR profiles to the setting up of the profiling process, including the programmer's approach to profiling suspicion. Section 6.6 discusses the findings in the context of an array of visions about ubiquitous sensing technologies and their use in police surveillance. Section 6.7 concludes the chapter with a summary of the findings and arguments.

6.2 On the right to privacy and technology

Privacy concerns have been discussed for decades in a wide range of academic, technology, legal and lay public forums and in relation to a plethora of information and communication technologies. More recently, concerns triggered by the rise of social media, cloud computing and ubiquitous sensor networks have been raised from the highest policy making levels (European Commission 2010a, 2009a, Moraes 2013) while revelations about their use in mass surveillance practices by law enforcement and other governmental agencies renewed and intensified a global debate on the right to privacy (Lyon 2014).

6.2.1 Protections and exceptions

Privacy is a complex topic with multiple definitions and often encapsulating differing meanings and interpretations across jurisdictions and cultures. Still, in terms of legal protection, the right to privacy is protected by the legislative frameworks of many countries throughout the world. Their laws often draw inspiration from the Universal Declaration of Human Rights which reads at Article 12 that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations General Assembly 1948). While clearly articulating the scope and goal of privacy protection, the formulation of Article 12 does not imply that this right is absolute. 'Arbitrary interference' leaves room for non-arbitrary exceptions in the exercise of this right.

In a European context, the European Convention on Human Rights makes these exceptions more specific. While point 1 of Article 8 reads that "everyone has the right to respect for his private and family life, his home and his correspondence", point 2 reads that there are exceptions to this right when it is "necessary in a democratic society". The list of exceptions includes "the interests of national security", "public safety or the economic well-being of the country", "the prevention of disorder or crime", "the protection of health or morals", and "the protection of the rights and freedoms of others" (Council of Europe 1950). The article provides a clear right for the respect of private life and correspondence but it also leaves room for interpretation and a long list of encompassing exceptions. Taken together and in conjunction

with new developments in the area of information and communication technologies, these exceptions have given rise to many concerns about the effective protection of this right.

This is because conceptualizations of security risks, public safety, or criminal phenomena have been continually changing and often expanding. We have seen examples of this phenomenon in the previous chapters concerning the definition and classification of suspects, suspicious criminal behaviour or of problematic youth groups. In these examples, the changes were related to technological developments which actively mediated how much data was collected about the suspects that fit the scope of the exceptions.

The relation between technologies and privacy infringement is also attested to by the wealth of theories and approaches to privacy protection that were developed and refined in the past decades along the emergence of information and communication technologies. In the face of – and sometimes anticipating – the spread of information and communication technologies, legal scholars and philosophers have continuously defined and updated conceptual frameworks in defence of the right to privacy. The development and refinement of new conceptual responses such as informational privacy, location privacy, online privacy, contextual integrity and so on (Flaherty 1997, Fulda 2000, Gutwirth 2002, Koops and Leenes 2005, Solove, Rotenberg, and Schwartz 2005, Nissenbaum 2009) attest to the ways in which the right to privacy has been shaped along the co-evolution of technologies and social practices.

In this context, regulatory frameworks turn out to require continuous adjustment in the face of new technological possibilities and changing social practices. For example, in the context of policing and law enforcement, Vedder showed how data mining technologies are able to produce new knowledge from existing data (Vedder 2001). Data mining technologies can yield new inferences from already gathered information such as medical data, drug consumption or criminal records. In this way, processes such as automated knowledge discovery and data mining highlight the inadequacy of regulations that concentrate solely on data protection. With data subjects largely unaware of the kind of data processing that is performed by multiple interconnected organizations, the defence of privacy protecting principles, such as informed consent, data minimization or purpose specification, proves to be very difficult through legal means alone.

6.2.2 A brief introduction to ‘privacy by design’

A particular approach that received significant impetus for tackling these concerns is ‘Privacy by Design’. This is a conceptual framework which advances the idea that privacy protection cannot be assured solely by compliance with legislation and regulatory frameworks but needs to be embedded in technologies (Cavoukian 2009). Championed by Ann Cavoukian, the privacy commissioner of Ontario, Canada, ‘privacy by design’ proposes a proactive rather than a reactive approach to privacy protection. That is, privacy implications should be considered throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. Moreover, privacy should not be compromised in a zero-sum approach (e.g. privacy vs security) but protected in a positive sum approach in which both ends are achieved through creative solutions that combine elements of IT design, physical infrastructure and organizational arrangements.

The concept has been embraced with particular emphasis by the European Union institutions (European Commission 2009a, 2010a) and features in the new General Data Protection Regulation (GDPR). The GDPR is set to replace the 95/46/EC Data Protection Directive

currently in force. The directive was enacted in 1995 and does not fully account for technological developments such as social networks, data mining, cloud computing or global sensor networks which were not significantly influential and developed at the time of the enactment of this legislation. Therefore, the European Commission proposed in 2012 a draft GDPR aimed as a legal framework that better protects the privacy of European citizens in this new context (Albrecht 2012).

Among the several legislative innovations that the GDPR proposes, one of them includes 'data protection by design and by default' principles. The Article 23 of the draft GDPR proposes that "data controllers shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing" and "personal data are not made accessible to an indefinite number of individuals" (Albrecht 2012). While specifically targeted at data controllers, and not equivalent to Cavoukian's proposal for privacy by design, the article specifies these principles as obligations for data controllers and not as mere recommendations.

However, both 'privacy by design' and 'data protection by design and by default' have been criticized for their vagueness and lack of explanation of how to translate their principles into concrete guidelines for implementation (Gürses, Troncoso, and Diaz 2011, Kroener and Wright 2014). How many individuals would be able to access data and still comply with an article about 'indefinite numbers'? How should programmers and engineers interpret privacy? What is an adequate level of security for the mechanisms that engineers should implement? There is no binding obligation in the GDPR for data controllers to implement particular solutions over others when considering these principles. Despite the attempts of several scholars to propose strategies towards operationalization (Kroener and Wright 2014, Hildebrandt and Koops 2010) there is often not a straightforward implementation of these concepts in concrete projects.

In this context, some policing agencies took up the idea of 'privacy by design' and proceeded to make their own implementation. In the face of criticism or anticipating it, they promise to engage sensor networks in ways that both protect people's privacy by design while simultaneously delivering security. Unlike some police organizations who had to scale down their systems after sustained criticism(Cambridge News July 31st 2014), these organizations look for innovative approaches to their engagement with sensing technologies in order to proactively protect privacy while simultaneously delivering on their policing responsibilities (Hellemons et al. 2013).

6.3 Mediating perception

Before exploring the design of technologies in these privacy protective practices we need to re-establish the mediating role of technologies in the case of sensing technologies. What held for GIS in Romania and social media monitoring technologies in The Netherlands may not hold for sensor networks. Even if previous chapters demonstrated the mediating role of technologies in police processes, this section illustrates these phenomena in the case of ANPR technology in the UK and in the Sensing project. Are ANPR systems actively mediating police perception and action? We answer this question first before analysing how designers explicitly build in privacy by design. The section begins with an introduction to ANPR and then shows the active mediation of perception and of action concerning suspicious vehicles.

6.3.1 A brief introduction to ANPR

ANPR stands for Automatic Number Plate Recognition. It is a technology enabling the identification of number plates of cars in traffic. In short, ANPR systems comprise a chain of video cameras and communication infrastructure and processing software components. The video surveillance cameras face the lanes of highways or roads and sense the movements of vehicles. The way of interconnectivity between cameras can vary but the fixed ones are generally wired while the mobile and temporary cameras are connected wirelessly, all communicating data in real-time to a central back office system.

The role of the software components is to automatically read and recognize the registration numbers of vehicles. These components process the images captured by the cameras. In real time they isolate the plates within those images, recognise the plate characters in the images with optical character recognition technology and translate them from pixels into a string of computer characters (Parker J.R. and Federl 1996). Once digitized, number plates can be stored in databases, searched, compared, aggregated and in general processed in conjunction with other data from databases and sensor networks.

ANPR is not a new technology. Dating from the late ‘70s in the UK, it slowly gained a reputation of an accurate technology with high reliability levels. Although some older versions had low reliability levels, newer algorithms claim high efficiency levels in correctly identifying licence plates in traffic (Parker J.R. and Federl 1996). Since its introduction, ANPR technology has been deployed in parking lots, entrances to areas, highways, roads, in marked and unmarked vehicles (see Figure 6) and in general in arrangements that need to monitor road traffic in a way that uniquely identifies all the vehicles (Cohen, Plecas, and McCormick 2012).

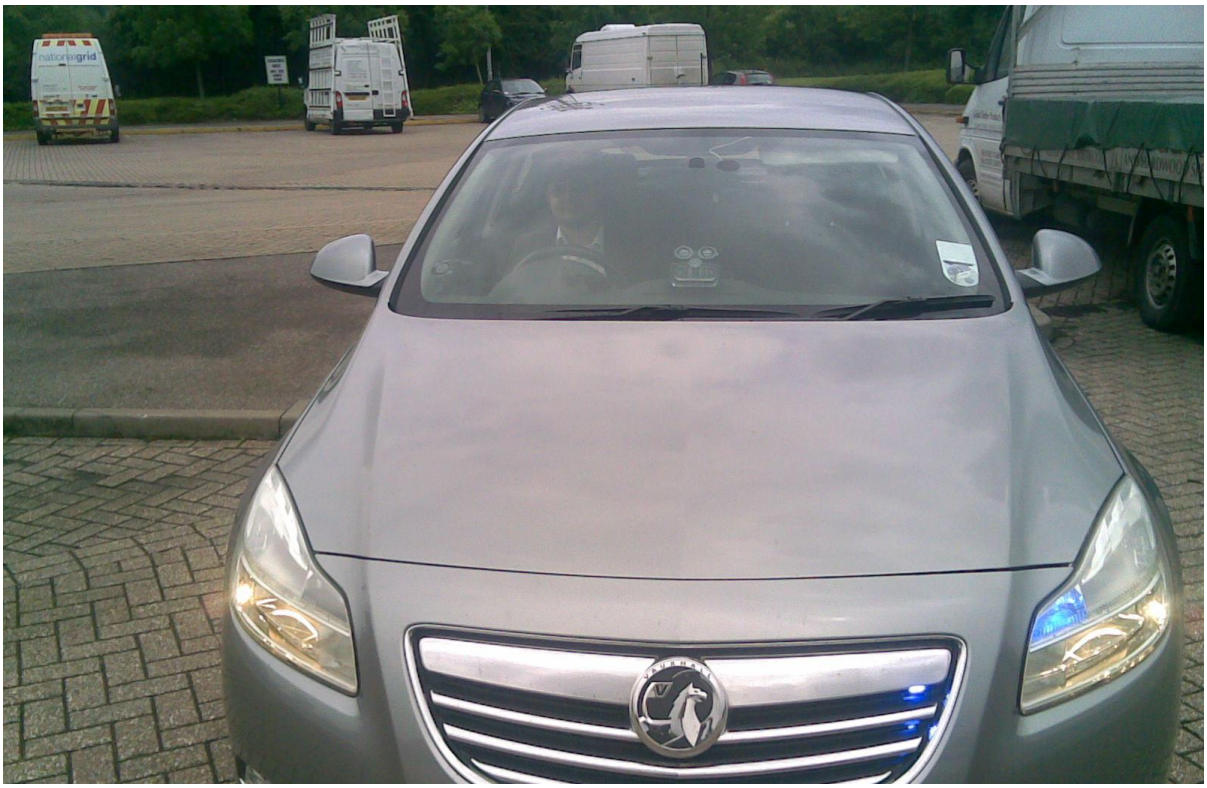

Figure 6 – An unmarked ANPR police vehicle in a constabulary in England. Notice that the ANPR gear in the vehicle is hardly visible.

6.3.2 Lists and ANPR

The most common way of using the ANPR technology is by comparing number plates in real-time with reference lists. These lists of numbers have come to the attention of the institution running an ANPR system: road administrators, tax authorities and in our case police organizations. Monitoring the traffic is done for instance 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 (Police.uk 2014).

If the system finds a match in one of the lists, it returns a so-called 'hit'. The hit is accompanied by additional information about the location (in case of mobile units or identification of the fixed camera), date and time of the hit and additional intelligence that may prompt further actions. Additionally, the hit triggers system operators or mobile units through visual (colour markers) or audio (alert sound) indicators. These indicators are displayed on the screens positioned in front of the police agent, as illustrated in Figure 7.

Figure 7 – A mobile unit of the Dutch police equipped with ANPR hardware and software. The bigger screen displays real-time information of ANPR hits.

The police uses ANPR for many purposes. They engage it in finding stolen vehicles, tackling uninsured vehicle use, catching drivers with unpaid fines or finding wanted criminals as part of a legal procedure (Police.uk 2014). In all these practices, the police know the number plate of the suspected vehicle and introduce it in a reference list. From that moment on the system gives a 'hit' whenever that number plate is recognized in traffic and notifies system operators of that

encounter (see Figure 8). Each number plate in the flow is assessed against the list but in principle the system need not store 'non-hit' data for this practice.

Figure 8 – A typical ANPR workstation during police actions.
The screen displays real-time data on the flow of vehicles passing in front of the intelligent cameras.

6.3.3 "It's not a problem in the end"

This section presents a situation with one of these most common uses of ANPR: checking traffic against predefined reference lists. Using ANPR with lists is a practice encountered in all the police organizations using ANPR. This section illustrates it by drawing on data gathered in England with one of the road policing units. In the constabulary where this study has been performed the police made use of a large network of fixed ANPR cameras together with a fleet of mobile ANPR cameras mounted in marked and unmarked police vehicles.

At the beginning of the field work, 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, through the roads in the county. One of the first 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 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 given 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 determine the actions of 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 who were bound to react on what the system displayed (as they could only check the picture of the car captured by ANPR), 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 did mediate 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. In this case officers interpreted it as a reinforcement of their initial suspicion. 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. 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 police officers enacting him as suspicious.

6.4 Profiles in action

Criminal phenomena often involve cars that are not a priori known to the police. Therefore they do not feature in any list. There may be thousands of vehicles involved in major organized crime that pass under the sensors without generating any hit. One of the ways to tackle these phenomena is to build intelligence by analysing the 'non-hit' reads. This means the police store all vehicles passing by cameras in the network. Depending on the number of cameras, this can amount to tens of millions of reads a year as is the case with UK ANPR system. Storing data from cameras distributed across the road infrastructure is kept for up to two years and can be accessed for analysis and investigation provided authorisations by senior officers (Police.uk 2014).

In the previous section we have seen how officers assessed the hits through certain 'lenses'. The ANPR system, acting within a socio-technical ensemble, mediated their attendance to the situation shaping their behaviour. In this section we will see that these formal and informal profiles that frame their attendance to the situation are mediated by profiles at the strategic and tactical levels of policing. The section draws on data both in England but also from The Netherlands.

6.4.1 Types of profiles

It is important first to distinguish that the term 'profile' often refers to both the practice of applying them to a population but also to the process of their making (Hildebrandt and Gurtwith 2008). For instance, group profiles refer to categories of people that share common features, characteristics or behaviour and who may or may not form a community. For instance, Romanian drivers on the roads in England. When the characteristics of a group profile are specific enough to designate a single entity they become individual profiles. Owen Dumitru from Newcastle, owning a Volvo with a particular number plate.

Concerning the way they have been made, one type of profiles are those that are directed, in which the correlation is previously hypothesized and then applied and tested on a population. Another type of profile is the one generated with data mining techniques, in which unexpected knowledge is produced, previously not hypothesized. This distinction helps to show that data mining – while an important feature for building profiles – is not to be confused with profiling. Profiling can be done without data mining.

In the context of the Sensing project, Schakel, Rienks, and Ruissen (2013), following Marx and Reichman (1984), define profiling as a method "to correlate a number of distinct data items in order to assess how close a person or event comes to a predetermined characterization or model of infraction" (Schakel, Rienks, and Ruissen 2013, 6).

6.4.2 Strategic group profiles

In the following quote, taken a few days later in the same constabulary in England, one of the analysts explained the ways in which she programs various kinds of profiles using logical operators. The system allowed her to process the stored data and combine identity attributes to generate a profile with the desired characteristics:

Officer Julia: *"Basically [we are] looking at eastern European individuals. But it is very difficult because in the systems there's no classification for 'Eastern Europe'. We know what Eastern Europe involves but you couldn't just go "only tell me eastern Europe". So* [the system] *enabled us to list all of the different possibilities, whether it's victims of eastern European crime, or offenders, or particular eastern European countries, whatever. And have the 'AND' and 'OR' functionality and pull them all off in one go, rather than having to look at every crime, look at every offender […] And then literally all you do is you click it and it goes away and it looks at all of the ANPR and it finds just the ones that fit those criteria, and it will bring them all back."*

The analyst demonstrates how the capabilities of the system enable the police to process large amounts of data to find correlations between crimes, events, vehicles and people. Since all the traffic data is stored in the police database, both 'hits' and 'non-hits', they can further aggregate this information to single out potential suspects and groups. The availability of stored data, combined with data mining techniques offers the police analysts a flexible way to profile vehicles and groups and find leads of suspicion.

At the same time, the amount of data in conjunction with the search capabilities contribute to a powerful system in which vehicles are registered and analysed wherever they would go through the country. Once a group of people is profiled as problematic, this infrastructure available to the police easily reinforces predetermined categories of suspicion. In this light, analysing the action of officers on the street level cannot be properly understood without the mediating role of strategic profiles. This is where identity attributes feature in practices of categorical suspicion. These practices can translate into action through alerted attitudes of officers in the field towards particular categories of road participants. The risks for breaching the privacy of these groups is heightened as the actions of officers in the field may induce more intense scrutiny (e.g. opening the trunk, asking for more information from the back office) and in general more policing and surveillance of certain groups compared to others.

6.4.3 Lessening privacy invasion with behavioural profiles

Another way to tackle criminal phenomena without necessarily storing all traffic data, relies on designing real-time behavioural profiles. Rather than bulk collection of data, automated rules select suspicious behaviour from sensor data before collecting and storing it in the police system. In this approach, it is not the 'Eastern European' that is a suspect but 'the one that conducts a theft', whatever the nationality or ethnicity, that the police is interested in detecting with sensing technologies.

This approach, employed within the Dutch police, implies the building of crime models that they translate into indicators. As they argue, 'knowing how to recognize a criminal in action may include the identification of a number of indicators' (Schakel, Rienks, and Ruissen 2013, 6). In this way, police knowledge of the criminal phenomenon becomes actionable. These

indicators of suspicious activity are then delegated to real-time profiles in order to catch criminals 'red-handed' (Schakel, Rienks, and Ruissen 2013, 1). Because it would be practically impossible to monitor locations all the time with mobile patrols, let alone infer behaviour patterns, models are translated into automated profiles. In this way, the police can detect suspicious behaviour when those vehicles were not included in any police list.

The models capture various aspects of the criminal phenomena such as locations, times, social networks or modus operandi. The lead officer of the 'Sensing project' within the Dutch police 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:

"*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".*

For one, the officer suggests that this way of working involves sensor data and need not involve persistent databases. The data correlated in such a profile comes 'in an ideal situation, from sensors that are seamlessly integrated in our natural environment' (Schakel, Rienks, and Ruissen 2013, 6). The real-time profile triggers an alert only when the combination of indicators matches. The police needs only to process ephemeral data only for computing the rules of the profile algorithm, discarding the rest of sensor data.

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, this 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. Still in many situations they can provide good indicators for illegal behaviour.

An example of successful behavioural profiling is the profiling of so-called 'canvas cutters'. These are thieves that steal from the trucks stationed in parking places along highways. Their particular modus operandi is to hop from one parking place to another in search for unattended trucks. When they find one they cut their canvas in search of valuable goods. 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 programmed a real-time profile that triggered an alert only 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 mining databases, 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 hypothesized suspicious behaviour. After knowing what behaviour to look for, they translated it into measurable indicators.

This way of engaging ANPR is different from the list-based one. That's because automated profiles run on real-time data and select from the traffic only suspicious behaviour for further

actions, discarding the rest of traffic data. This way of working is also different from the one building knowledge from data mining. Instead of storing all traffic in a database it works with ephemeral data streams. Therefore, the police officers in this project argue that this way of working "reduces the impact of privacy invasion" (Schakel, Rienks, and Ruissen 2013, 7). The data of most traffic participants is not stored in the police databases or quickly deleted. Any potential further investigation, whether unauthorised searches, discriminatory profiles, curious officers of celebrity whereabouts and more, would not have the data to start with in the first place.

6.4.4 Building in revocable privacy

Still, Galindo and Hoepman (2011) argue that the process of using profiles does require the temporary storing of all traffic data for the duration of computing the profile rules. For instance, to assess if a vehicle is used by a 'canvas cutter', the system needs to assess traffic data at multiple parking locations in a short interval. Any license plate needs to be stored for a duration of time to assess if it goes through multiple parking lots in a short amount of time. Even if it may be deleted soon after, 'non-hit' data, that is data of most traffic participants, is stored in police databases.

In this context, Galindo and Hoepman (2011) argue that ANPR data stored for computing the profile may still be used by the police, allowing for more possibilities to gather information about people after the fact. Promising to discard it is only a procedural solution. They argue that the limitations must be ensured through "technical means, in the architecture and design of the system" (Galindo and Hoepman 2011, 2).

They propose the concept of revocable privacy (Galindo and Hoepman 2011). In short, this concept proposes that for the time needed by the profile to assess risk or suspicion, ANPR data should be kept encrypted in a unidirectional way. This is technically achieved with mathematical 'hash functions' which uniquely map the strings of characters (representing the number plates) to elements in a set. Unidirectional here means that from the 'hashed' output in the set one cannot retrieve back the initial string (i.e. the number plate).

All licence plates are first processed with hash functions while the receiver (in this case the police system) is only able to 'decrypt' them "if a minimum number of different senders encrypt the same plaintext" (Galindo and Hoepman 2011, 2). In other words, only if several parking lots detect the same number plate then the data is revealed to the police for consultation and further action. The system uses for comparison and computation of times and locations the unidirectional-encrypted form and not the number plates.

Therefore, any potential attempt by the police to use ANPR in an unlawful way would not be able to retrieve the actual numbers. Hash functions make it computationally impractical to retrieve the initial string of characters given the 'hashed' output. Without the actual number one cannot perform searches and aggregations with other databases and sensor networks. In this way, potentially illegitimate use by police operators would be unable to infer the locations of vehicles, for instance of their lovers, spouses or other privacy infringing uses of the system.

The concept of revocable privacy was further developed and expanded (Koops, Hoepman, and Leenes 2013) but its core tenet remains that "no personal information is available unless a user violates the pre-established terms of service. Only in that case, his personal details (and when and how he violated the terms) are revealed to certain authorized parties" (Galindo and

Hoepman 2011, 2). In this way, privacy is a default which is lifted only when certain conditions are met.

This section showed that in order for the police to deliver on the promises to detect suspicious behaviour while protecting privacy and minimising the risks for discriminatory actions more conditions need to be met. The police needs to build profiles through knowledge sharing and not through the use of persistent databases, they should restrict themselves to behavioural profiling and not involve identity attributes and they should implement revocable privacy robust enough to account for a variety of criminal behaviour that can be modelled and delegated to real-time profiles.

However, the following section shows that this process has its own risks for the very values it aims to protect. During interviews and observations, it became apparent that the need for continuous design of profiles is fraught with a whole set of implications for privacy, non-discrimination and identity. Building knowledge about behaviour also requires the use of persistent databases while profile design criteria can include new identity attributes.

6.5 Behavioural profiling 'in the making'

The argument for behavioural profiling as a privacy protective practice starts with the assumption that the profile is a finished artefact. In the above examples it is assumed that knowledge rules are ready to be delegated to automated algorithms. In other words, only after police officers know that canvas cutters behave the way they do can the indicators be delegated to sensing technologies in conjunction with revocable privacy technologies. However, this section looks at a stage in the knowledge production process in which the officer working with the sensing technologies did not yet know how to model a certain criminal phenomenon.

6.5.1 Setting up profiling

The following quotes are taken from interviews and participant observation session with Dutch police officers strategizing before a new police action. The action was aimed at using sensing technologies to tackle a criminal phenomenon that uses a large number of vehicles in performing their actions. In the following quote, the lead officer explains that the start of this action implies a large list of number plates that he proposes to be monitored. Knowledge and 'wisdom' about how to refine this number comes later through the use of sensing:

"*We start and after a while we gather more and more intelligence and we will all become wiser from that. We will learn how to use sensing, we will learn how to work with it.*" […] "*These [number plates] have been put into a separate database and I can tell you they are quite a lot: it´s not just a few registrations, no, there´s thousands of them. [...] We have to refine this top X and go deeper into it to get a real top X*".

Therefore, in order to study crime patterns and hope to derive at some point the knowledge that would to be delegated to a profile, the police needed to monitor a large number of vehicles for a certain period of time. Still, to put this practice in perspective, these vehicles have been selected, so they did not start with monitoring all the traffic in bulk even if the list contained

'thousands of vehicles'. Nevertheless, the quote shows that the police do need to further refine the list to get to 'a real top', a process that involved persistent databases and monitoring.

6.5.2 The presumption of innocence

A second issue of this way of working concerned the risks for the presumption of innocence. The better profiles get in detecting criminal phenomena, the more they tend to induce reliance for the officers working with them. However, the profile designer in the Sensing project was well aware of the potential that profiles falsely identify criminals.

"*So it is not 100% safe. It's not fool proof, but 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… we miss*".

The designer admits that the hits produced by the profiles can generate both false positives and false negatives. In other words, he knows that profiles are not delivering certainty. Still, when it came to action in the field, his uncertainties tended to become black boxed. The following situation happened during a participant observation session in a special action coordinated from the control room of the Dutch police force. The action was part of a concerted effort to tackle a large scale criminal phenomenon in which a lot of vehicles were potentially used.

It was a particularly busy day in the control room of the Dutch national police. 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 ANPR 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. His expectations seemed rather high:

"*I think that when [the sensing project] 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.*"

The quote shows that the officer in the control room expected real-time profiles to deliver more than a mere indication but a near certainty. His way of talking about it (i.e. the use of the interjection BAM) indicated that the potential for the profile alert to influence his behaviour. He would have otherwise be inclined to perform an extra check but (with the sensing fully developed) he would be inclined to delegate his trust to the profile rules. In conjunction with the high-pitch audible alerts, the profiles would induce an alerted attitude if not the suggestion to his colleagues in the field to proceed for swift action.

Admittedly, the hit from a profile does not necessarily lead to an arrest. Still, the quote highlights that the officer in the control room tended to have a significantly different level of expectations from a profile. Contrasting, the profile designer was more aware of its potential flaws. The profile acted as 'boundary object'(Gerson and Star 1986) between the officers. These are artefacts that have meaning across multiple disciplines or practices and potentially improve that coordination between different branches of the police.

However, (Schakel, Rienks, and Ruissen 2013, 6) also acknowledge that "to prevent boundary objects from becoming static and detached from practice, both models and profiles need to be

subject of constant debate, stimulating the exchange of lessons learned, the creation of new intervention strategies and tactics, and the formulation of actionable hypotheses that can be tested in policing practice" (Schakel, Rienks, and Ruissen 2013, 6). Profiling therefore implies continuous redesign.

6.5.3 Behavioural profiling and identity attributes

Still, during the process of redesigning, new issues of behavioural profiling come to the fore. Despite advertising a lack of identity attributes in the process of behavioural profiling, identity attributes can creep back in whenever a redesign is necessary. The following quote, from an interview with a police programmer in the project, shows that the practice of profiling does include identity attributes.

The programmer was responsible for redesigning a profile. The profile should give a hit when a set of known number plates were performing a certain behaviour: returning to a problematic location. In other words, a profile hit would indicate to the police that 'the old boys are back in businesses'. The police programmer explained that he equated a profile hit to a minimum threshold of points calculated with indicators in the profile:

"*I made two indicators. Each one of them has 'a camera part' and 'a name and time part'. I'll explain. They get 20 points for passing by the camera* [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]".

The programmer explained how the threshold of the profile can be obtained by both spatial-temporal behaviour but also by matching on the name. Still, as he later explained the 'name part' may not be as efficient as he would want it to be:

"*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"*.

This dialogue shows that even if the profile is meant to assess behaviour it also requires an inquiry to the vehicle registration database for the name and address of the owner. The algorithm needs to provide the number plate from the first read to assess the subsequent reads and assess if the vehicle is performing a suspicious behaviour. Therefore, we observe that in practice designers inscribe rules on indicators regarding other identity attributes. In this case they process the name and the address besides only the behaviour. This phenomenon is further illustrated in the following interview with the lead designer:

"We connect to RDW (Dutch vehicle registration database) and we get all the information about the car, the make, the colour, the fuel type that it uses, but also on the owner of the car. In this way, we can, for instance, say we want to stop all the cars which are very expensive, newer than 3 years and the license plate holder, the owner, is younger than 27 years old. We find it interesting that someone who is quite young still has a brand new car or almost brand new car that is so expensive. Where does he get the money? So we make a profile on this and

check if this is a new car, if it is so expensive, and if the owner is younger than 27. If this is all true, then we say: you give a hit".

This quote highlights the use of identity related attributes combined with ANPR in an aggregated profile. What it also shows is that once connecting to persistent databases, behavioural profiling loses its advantages with respect to privacy and non-discrimination. While age is not a particularly sensitive identity attribute in many contexts, the threshold of 27 years old in this context would effectively put under surveillance a whole category of young, successful entrepreneurs who can afford that kind of cars at 27 years of age.

The examples in this section render the profile design as a locus of analysis for morally acceptable discrimination. They show that the ethical evaluation of profiles depends on particular values given to parameters in the profiles. The translation of identity attributes into profile rules can be fraught with a high normative charge. When is someone old enough to be out of suspicion for owning a particular kind of car? Which nationalities are part of a suspicious profile and which not? Through connections to persistent databases and other sensor networks, profiles can request identity related attributes such as name, age and nationality. The mere combination of identity attributes may put under close surveillance whole categories of people.

6.5.4 Picking up the pieces

We can see from these examples that behavioural profiling faces difficulties and challenges. ANPR is not a flawlessly working surveillance machine that only selects the perpetrators from the innocent, the bad from the good. Its accuracy in enacting suspicion depends on a whole set of socio-technical factors that needs to be aligned. Building behavioural profiles only works with many branches of the police collaborating and continuously developing the algorithms. The new way of working is not delivering actionable knowledge at a push of a button. As another officer mentioned some months later from the start of building profiles:

"[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*".

On the one hand, the quote illustrates the difficulties in building knowledge for profiles and shows that new sensors are not being installed in the absence of this knowledge. On the other hand, the officer did mention a camera to be installed in order 'to see what kind of cars are passing'. When they face difficulties in building knowledge, monitoring becomes the fall back option. The officer tended to rely on technology when he perceived the organizational arrangements and new ways of working to fail. As he later reinforced:

"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 that knowledge-based policing is far from an automated discovery in which data mining algorithms would give the police the interesting associations at a push of a button. The process involves trial and error. While the focus may be on producing new policing practices in which technology plays a more significant role, 'old habits' seem to die hard. When 'the availability of technology is not the problem' monitoring seems to be the default option

without concerted efforts to promote imagination in using sensing technologies as well as privacy protective measures.

This section highlighted additional conditions for claiming knowledge-based policing to 'reduce the impact on privacy'. As it turns out, behavioural profiling may offer better privacy protection *after* profiles become finished artefacts, ready to become operational and inscribed in algorithms. Until then, the knowledge that can be used in building profiles is still made through monitoring. Profiles based on behaviour may minimize unfair discrimination but, as this study has shown, profiles can still aggregate a variety of sensors providing information pertaining to socio-economic status, nationality, age and other identity related attributes. These can create new categories of suspicion and enhance the incentives for discriminatory police action towards them. Once engaging in a proactive approach to catch criminals red-handed, the police officers are bound to continuously change profiles. This is done for adapting to changes in criminal behaviour but also to prevent the erosion of the presumption of innocence of a rising numbers of false positives caught in their net.

6.6 Discussion

We have seen so far how police organizations understand and use ANPR as a sensor providing data flows along other sensors, such as radio frequency identification to cover not only roads but 'railways, waterways, or cyberspace' (Schakel, Rienks, and Ruissen 2013, 12). Unlike other sensor networks, ANPR is already in place. Sensing the movement of vehicles on the roads, police organizations engage ANPR in a variety of practices. It provides thus a timely opportunity for understanding policing practices in relation to ubiquitous identification infrastructures.

Significant investments are made and visions are projected for a world in which ubiquitous sensors and devices are networked and connected with each other and to other (online) services. These visions, referred to with umbrella terms such as Ambient Intelligence, Internet of Things or Ubiquitous Computing, announce information infrastructures in which ubiquitously present sensors are embedded in the environment (International Telecommunications Union 2005, European Commission 2009b). They identify entities – both people and things – and communicate information about them. These developments announce to have applicability in multiple areas such as intelligent dwelling, environmental protection, transport infrastructures, etc. As there is no orthodoxy about which technologies should enable these infrastructures, a heterogeneous set of technologies and architectures features in these visions: radio frequency identification (RFID), Bluetooth, ZigBee, and more (Aarts and Marzano 2003, Gubbi et al. 2013). They enable tracking and localization, as well as interconnection at any point in time with accurate identification, reliable communication and intelligent processing of data. Depending on the application, these technologies sense physical phenomena (e.g. temperature, the presence of a unique identifier), trigger effects on the physical environment (e.g. display alerts and other information) and be equipped with data organizing capabilities. When combined with data mining and profiling they become very interesting for policing and law enforcement agencies.

ANPR has a whole set of characteristics used to describe Ambient Intelligence, Internet of Things or Ubiquitous Computing visions: pervasive, invisible, ubiquitous, adaptive, wireless, reliable and intelligent. Cameras are spread in large numbers across wide areas, they are

practically indistinguishable from other cameras that do not have ANPR, they transmit data wirelessly and their algorithms are able account for variations in many factors such as weather conditions, lighting conditions, types of number plates and others. It is thus relevant to discuss ANPR policing practices as this may increase our understanding of issues related to policing and Internet of Things and the best privacy protective strategies to promote in that setting.

On the one hand, this chapter showed that, provided certain conditions, behavioural profiling based on knowledge sharing and inscribed in real-time algorithms can protect privacy and non-discrimination 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; they restrict themselves to behavioural profiling – and do not involve identity attributes; and they implement revocable privacy robust enough to account for a variety of criminal behaviour that can be modelled and delegated to real-time profiles. Concerning organizational arrangements, the storage and processing of data should be done locally (e.g. at each parking lot) and only centralised when a set of predetermined rules are breached. Otherwise, storing all traffic data for long periods of time in a centralized place endangers the privacy protective advantages of knowledge-based policing.

On the other hand, the relations between criminal behaviour, ubiquitous sensors and organizational factors are not always clear – they are increasingly unpredictable even as attempts are made to prevent potential privacy harms. Although technical solutions intend to reduce the risks associated with ANPR as a surveillance infrastructure, at the same time these practices may create new ones. It is clear that we cannot simply rely on 'hard-coding' privacy protection (Koops and Leenes 2014). 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).

What I showed in this chapter is that the enactment of suspicion and the action taken upon suspicious entities are dynamic and nuanced policing practices. They depend upon a wide range of actors that are involved. These include the police officers with their formal and informal attendance to the situation, the ANPR software and its visual and audio interface, databases, political processes, legal provisions, profiling algorithms and more. The intention of this work is not to suggest that practicing privacy in design is pointless or not fruitful. Rather it aims to enable critical engagement with these practices with a vocabulary that allows us a more flexible conceptualization of how privacy is mediated. By continuously tracing the enactment of suspicion in technologically mediated policing practices we can hope to counter more adequately some of the harms and risks to the right to privacy raised within current and emerging forms of digitally mediated surveillance.

6.7 Conclusion

Towards fulfilling their crime control targets, police organizations have multiple ways to achieve their aims. One option to control crime is to emphasise reactive policing. With a focus on solving as many crimes as possible, the police may build intelligence about suspect persons or groups by systematically analysing recorded data. However, in the process, traffic data is stored in bulk, becoming easily accessible for further searches and further processing,

potentially linking names, age, nationality, location and other identity attributes, reinforcing categories of suspicion and fostering infringements of privacy.

Another option is to aim at catching criminals 'red-handed'. In this approach, police organizations do not necessarily need to store data for weeks or months but design profiles and apply them on ephemeral data flows. Combined with organizational arrangements and cryptographic solutions, this approach announces to concentrate on suspicious indicators and discard most of traffic after brief analyses. Compared to solutions that require the storage of all traffic data for months, this way of working does not in principle require the use of identity attributes. As such it lessens the risk for discriminatory actions by police officers in the field.

Acknowledging the privacy invasive potential of sensor networks, a project in the Dutch police looked for ways to engage sensing technologies while improving privacy protection by design. In the absence of legislative provisions they proceeded to make their own implementation of the idea of privacy by design. Still, we have seen in this chapter that certain problems persist. First, while inscribing privacy in design, new (and older) forms of problematic discrimination still remain (i.e. profiling not necessarily based on ethnicity or race but also on nationality, age or income). Second, new forms of identity are being performed (i.e. enacting someone or a group as suspect based on algorithmic processing); third, new ways of eroding the presumption of innocence (i.e. the strong audible alerts and visual symbols of a profile hit are prescriptive for the actions of officers. They increase incentives for immediate action and decrease the incentives for cross-checking the adequacy of information, contributing to higher numbers of false positives). Fourth, profiles deliver their best results only after the police have learned what suspect behaviour to look for. Until that point, the process often resorts to the collection of large quantities of data to enable data mining in order to inform the profile design process. Finally, the new way of working is undermined by the more practical aspects of work, specifically the difficulties in changing old ways of working. When the police fail in knowledge sharing processes, they tend to resort to the storage of data for longer time.

The chapter rendered the process of building suspicious behaviour profiles as a locus for ethical reflection in the context of current and planned expansions of sensor networks. The analysis offered a vocabulary to trace how suspicion is enacted in these technologically mediated policing practices. In this way it places us in a better position to understand how privacy is mediated in ubiquitous sensor networks and how it can be better protected; not by a priori framing technology as a threat to or an ally for privacy but by continuously analysing how suspicion is produced within the materially and discursively heterogeneous relations between various kinds of actors, including police officers, technological artefacts, organizational arrangements, legal manoeuvres and others.

Chapter 7

Synthesis, conclusions, recommendations

7.1 Introduction

Digital technologies have become pervasive in our environments and are increasingly relied upon in many policing practices. From intelligent video surveillance and geo-spatial information systems to profiling algorithms and sensors distributed in the environment, information technologies are steadily becoming constitutive of contemporary policing. In the previous three chapters we have seen technologically mediated policing at work in a diverse range of situations and in various police organizations throughout the European Union. Without claiming to represent the host organizations, the analyses of this qualitative research aimed to answer questions related to the role of these technologies in policing practices.

The ethnographic research I performed at these settings looked at practices of classification, profiling, surveillance and preventive action concerning suspicious, risky or problematic behaviour, persons, groups, vehicles and so on. The analyses concentrated on the ways in which police agents, officers, constables, analysts, strategists and programmers engaged with a range of technologies – from the low-tech paper-based reports, registered in geographic information systems, to social media monitoring and more sophisticated sensing technologies and algorithmic profiling.

The book demonstrates the active role of technologies in mediating policing practices. The evidence from this sample of situations is that in all these diverse settings artefacts played active roles within the complex socio-technical ensembles in which they featured. They incorporated a highly normative charge and have significantly influenced the outcome of policing practice. Much more than neutral tools, technologies proved to mediate the perception, experience, decisions and actions of practitioners. Ranging from the day-to-day routines to the situations in which they produced inadequate results, they influenced the outcome of policing processes, with significant consequences for many of those implicated.

This chapter summarizes the answers to the research questions in Chapter 1 and discusses the findings on a set of issues that tie the empirical material together. The role of technology in policing practices forms the thread that links issues of suspicion, surveillance, community, identity, values and design. First, the chapter discusses processes of performing suspicion in contemporary policing against the background of a proliferation of digital technologies. So, how were 'suspects', 'suspicious behaviour', 'fishy situations', 'wired vehicles' or 'problematic groups' featuring in practices that rely on proactive surveillance, automated geo-spatial analysis, or sensing technologies? What is the relation between suspicion and surveillance? Section 7.2 answers these questions and argues that a paradoxical '*solidification*' effect of suspicion is associated to technologically-mediated policing practices, fostering *a cycle of suspicion-surveillance*.

Second, the chapter discusses how this 'solidification' effect impacted police-minority relations and how information technologies influenced police relations with various communities and categories of citizens. How did algorithms and classifications come to perform the identities of various groups as problematic or suspicious? How was community policing being influenced by the merging of pervasive sensors with proactive policing styles? Section 7.3 answers these questions and shows how the solidification of suspicion combined with a process of *sedimentation of prejudice* that influenced police relations with communities and minority groups on an infrastructural level.

Third, the chapter discusses more generally the relation between technology design and moral values in policing. We have seen how prejudice can trickle down in infrastructures and foster discriminatory actions. We have also seen in previous chapters how privacy was explicitly built into the design of some policing technologies. What other values were at stake? How can we design policing technologies that account for multiple values with equal moral importance such as non-discrimination, trust or transparency? What recommendations can be made to policy makers and designers of policing technologies? Section 7.4 answers these questions and argues for *an uptake of Value Sensitive Design* methodology in daily policing, albeit with a pragmatic twist. At the same time, it proposes a '*sedimentology of infrastructures*' to dig-up potentially explosive '*pockets of prejudice*' that may have formed in our smart environments and information infrastructures.

7.2 Suspicion, technology, surveillance

Assessing persons, groups, vehicles and many other entities – and inferring problematic or suspicious behaviour – are some of the typical activities of policing practitioners. Whether we are talking about scrutinizing people on the street or monitoring internet behaviour, vehicle flows or data flows, police agents and officers assess activities, people, groups or situations in society. They make these assessments according to norms defined in the context of police work and look for behaviour that deviates from these norms. They then interpret some of these deviations as indicators of criminal behaviour or at least suspicious activity that could be related to a crime and warrants further surveillance.

This kind of normativity in police work is highly contingent on a whole set of factors in which policing practice takes place. For instance, strolling through a parking lot may be considered 'quite normal' in the middle of the day but the same behaviour can be assessed as 'suspicious' by a police patrol by night. Not only are these norms dependent on police knowledge of criminal phenomena but also on a whole set of environmental, social, legal and political factors. For instance, a spike in street nuisance on a graph may be considered 'abnormal' if analysed in isolation but 'quite normal' when corroborated with changes in weather conditions (e.g. a heat wave may keep people outside later at night). The word 'riot' in a social media post may refer to a party between friends or it may call for politically motivated street disturbances. Distinguishing between innocents and criminals, normal and deviant, order and disorder are, of course, some of the main tasks of policing practitioners, with which we invest them to enable crime control and keeping our societies safe.

Still, being invested with a monopoly on the use of power requires that practitioners and police organizations perform these entities – 'suspicious', 'abnormal', 'criminal' – in such a way that they protect the members of society from both crime and their own potentially erroneous, prejudiced and disproportionate interventions. We have seen throughout this book that this line is often thin. Policing practitioners can sometimes miss the actual criminal and they can also pick on innocents; they often make decisions on poor data; or they can inadequately interpret the output of systems. Of course, issues such as false positives or discriminatory practices are not new in police studies. What may need extra attention though is the role of technologies in these practices.

A lay understanding of technologies is that they are means for human ends, useful but neutral tools that do not bear responsibility for the outcomes: "We can't take a knife to court".

However, what we have seen in the previous chapters is that artefacts employed in day-to-day practices do much more than being neutral tools. Whether by shaping the attitudes of police officers towards crime phenomena or towards individual suspects (see Chapter 4) or by influencing police action concerning 'problematic youth groups' (see Chapter 5) or vehicles (see Chapter 6), technologies actively mediate policing practices. That is, practitioners decide to police certain persons, groups, areas or criminal phenomena more than others (or with different degrees of intensity, prejudice, justification and force) based on software-enabled infrastructures that influence the outcomes of socio-technical processes in policing. So in what ways do these technologically-enabled entities influence police work?

7.2.1 Solidifying suspicion

One insight of the mediating role of technologies concerns the influence they have on perceptions of reality and truth. Despite being aware of notoriously erroneous police databases – which many policing practitioners and scholars are – the evidence produced by the chapters of this book supports the argument that technologies tend to 'solidify' suspicion. That it, they induce a perception of objectivity about the entities they represent as suspicious, problematic or risky. In other words, the very presence of a 'suspect' label into a technological infrastructure strengthens the officer's state of alertness concerning the represented entity.

Of course, this does not mean that officers cannot and do not doubt the output of technologies or that this phenomenon occurs with every police officer and technological artefact they work with. Neither does it mean that suspicion implies arrest or conviction. Still, we have seen in the previous chapters that technologies tend to 'black box' design decisions with normative charge or erroneous representations. As users, the police officers generally do not have access to and information about the criteria of design choices. In this way, these norms tend to become invisible, further 'solidifying' the police officer's perception of suspicion.

We can recall, for instance, the vignette analysed in section 4.3.1 in which the local police agent in Romania performed an alerted attitude towards the young boy upon reading the 'suspect' registration in the information system. Agent Camelia was not aware of the superficiality of the last registration in the system and she tended to take it for granted as an adequate indication of the character of the boy: "*Obviously, a pickpocket*" was her assessment, based strictly on what the screen displayed. As she was in a difficult position to question the validity of system output, she took what was on the screen as a representation of reality, investing it with a high degree of objectivity. The last entry – the one where the boy was labelled as a suspect of theft – solidified her overall assessment.

We can also recall the situation described in section 5.3.2, when the Dutch police analyst was working with a statistic generated by the system concerning 'nuisance youth' in his area. He was just about to issue the report to his superiors, noting a 'spike in nuisance', when the interview question happened to require him to do additional investigations in the database registrations. The additional investigation found that the statistic report on 'nuisance' was based on a systematically inadequate classification of youth offences. Without this contingent situation, his report would have produced a solid indication of a rise in the phenomenon in their area.

A similar kind of solidification of suspicion we can find at the operational level of policing, as analysed in the situation in section 6.5.2. The Dutch police agent in the control room was working with the ANPR system. When I questioned him about the expectation he had from

ANPR profiles he expressed high expectations about their capabilities to indicate suspicious behaviour: "*I think that when fully developed, it will be easier because I won´t have to check it. It´s just BAM - the hit comes - ok people: check it, it´s weird.*" His reliance on the technology to produce solid indications of suspicion is illustrative of this phenomenon. If one 'is in the system' it can become justificatory for reinforcing assumptions and inducing higher levels of alert. Simultaneously it can decrease incentives for additional justifications ('*I won´t have to check it*').

Many information technologies in policing mediate the experiences and perceptions of practitioners in this way. With their assertive representations and powerful symbols, such as bright red icons for 'criminal youth groups', black dots for 'beggars', flashy alerts and high-pitched sounds for 'weird vehicles', technology often tends to be trusted. Police agents and officers work in these environments in which their behaviour is steered and nudged by a plethora of technological artefacts. These mediate the officers' experience in the background or mediate their perception when officers embody artefacts in their practices. In these ways, technologies tend to induce a sense of objectivity and need of immediacy concerning the people and groups they perform as 'suspicious'.

Of course, many times, technologically mediated suspicion turns out to be justified. The represented entity could be indeed the perpetrator. Still, we have seen throughout this book that suspicion can sometimes be vague, partial or insufficiently justified. The analyses in this book started from a set of reports of suspected entities in police systems and took the time and effort to further investigate how the socio-technical ensemble of policing supported their assessment. We have seen in this way how 'suspicion' was often insufficiently justified, despite being mediated by technology. Even if 'suspects' or 'problematic' entities were performed as such in flawless, attractive graphic interfaces or by strong, assertive sound alerts, they did not properly justify the police interest. However, the tendency of practitioners to rely on technology fostered their assumptions and predispositions. When they placed a lot of trust in technologies and they were not able to question their output, agents were more likely to act on these representations of suspicion.

7.2.2 Legitimizing surveillance

But in what ways did technologically-enabled suspicion mediate police action? After all, suspicion does not imply conviction nor does it justify arrest. Policing is guided by legal provisions that make agents and officers aware of the status of suspicion in criminal justice procedures. Still, the label, once associated to an entity, does justify intensified surveillance and elevated levels of police interest. We can recall here the vision document for the Dutch police that sees technologies as the solution to "prevent an unnecessary infringement on the privacy of people who are not under any suspicion" (Hoogewoning 2006, 79). This formulation also implies that who *is* under the slightest suspicion can be legitimately monitored with the help of high-tech solutions. These solutions are 'expected to become increasingly important' for the 'surveillance of the infrastructure, or rather, of the flows of people, goods, money and information' (Hoogewoning 2006, 78).

And we have seen throughout the previous chapters that these solutions are already here, not only in organizations based in the Netherlands. Classification of suspicion based on algorithmic processing of data from sensors pervading the environment induced elevated levels of police interest, alerted attitudes, automated profiles, and monitoring of categories and groups. In all

these situations, the performance of suspicion, deviancy, or problematic character became justificatory for intensified surveillance.

This was the case, for instance, when the two constables of the road policing unit in England took further actions in their searching of the stopped vehicle, once the system displayed the nationality of the owner (see section 6.3.3). Officer Morris justified the extra checking of the vehicle once he learned the owner was '*a Romanian from Newcastle*'. Even if nationality was not a category associated per se with suspicion in this context, the officer associated the categories of 'Romanian and Eastern Europeans' with 'a lot of problems' and applied the category to the situation at hand. This was made possible by an arrangement in which the ANPR system displayed the nationality of vehicle owners on the screen in the police vehicle. When these categories are considered problematic at higher levels of policy making and also incorporated in the technical infrastructure they become sufficient incentives for the field officers to intensify their surveillance. Even if it turned out 'it was not a problem in the end'.

We have seen another example in Chapter 5, concerning youth groups in The Netherlands. These were monitored on social media once they were labelled as 'problematic' in the police information system. We can recall here the justificatory phrase of agent Anna in the Dutch police, concerning the monitoring of these youth: "*Being 'youth agent' and [at the same time] surveying the internet is a great combination to have. To gain some value from what they put on the internet. The main objective of internet surveillance is being [there] before the criminal offense happens. That's why it's not called internet investigation but surveillance"*. 'Gathering information', 'gaining value', 'learning what they do' are actions of policing practitioners legitimized by the classifications of groups 'in the system' as 'problematic'.

As surveillance does not imply arrest, it was also not perceived by agent Anna as a harmful action towards these youth. In this sense, it contributed to relaxing the need for more justifications to engage in surveillance (*"You don't have to have criminal offenses, but use it as an information source"*). Fair to say here that the possibility of the police agent to easily gather information was also fostered by the habit of youth to "*put everything* [online]". In this situation, not only surveillance but 'quick and effective crackdown' became a suggested action towards the less problematic but much larger 'annoying' and 'nuisance' youth groups. This suggestion, in the evaluation report, to prevent them 'slipping down to the status of a criminal group' (Van Burik et al. 2013, 21) illustrates that classifications in police systems can legitimize not only 'soft' surveillance measures but also swift and decisive interventions.

These situations above, and more throughout the book, illustrate the point that labels in police systems concerning 'problematic', 'suspected' or 'risk' entities are not only necessary but often also sufficient justifications for proactive surveillance practices. What we have seen though is that, in their turn, surveillance increases the chance for encountering problematic situations with people in these categories (compared to other categories). Entering *a cycle of suspicion-surveillance* solidifies incentives for intervention and makes it difficult for the enacted entities to invalidate the reasons for which they raised police interest. Whereas in reactive policing surveillance can work to invalidate the suspicion-surveillance cycle, in proactive approaches it tends to foster it.

In the criminal justice vocabulary, the quality of being 'suspect' is maintained throughout the criminal justice chain until it is changed, either by new evidence or by a court of law (f.i. into 'convicted' or 'acquitted'). In the criminal justice systems of democratic countries, where the burden of proof is on the prosecution, preserving this distinction enables the principle of

protecting the presumption of innocence. The protection relies on allowing a significantly higher level of flexibility in changing the state of being 'suspect', compared to the situation in which a person has been 'convicted'. That is, new evidence, facts or indicators can change this quality much easier than it could be possible after a person is convicted.

The insights from this section raise awareness of the paradoxical effect of technologically mediated policing to bring about a 'solidification of suspicion'. On the one hand, software offers vast possibilities to capture the flexibility needed for the category 'suspect'. On the other hand, software-enabled entities in policing, with their powerful processing capabilities, shiny interfaces and assertive symbols tend to induce practitioners to rely on what is displayed on screens. Especially in proactive approaches, this phenomenon fosters a cycle of surveillance-suspicion that people have a hard time invalidating.

7.2.3 Conclusion

What we have seen in this section is that technologies play an active role in how and who the police look for. Not only do police officers assess suspects with their eyes and their minds, acting on the cultural assumptions they are making, but suspicion can be embedded in software code, delegated to technologies and displayed on screens. Important but not singular factors in performing suspects, suspicious behaviour, situations, vehicles or groups are software-enabled artefacts. These entities play important roles in the socio-technical arrangements in which police work takes place.

One effect we have seen that they have is to *solidify suspicion*. Once a suspect in a proactive policy is 'in the system' it becomes much more prone to have this status maintained and strengthened. Even if police officers consciously know that they should not take the 'suspect' category as proof of crime, in practice officers often tend to rely on what they see on the screens as indications of criminal behaviour. Relying on the corrections that can occur along the criminal justice chain, some policing practitioners, especially field agents and constables, tend to take technologically mediated suspicion as incentives for alertness or surveillance. Perceiving surveillance as a non-harmful action, relaxes the need for further justifications. In these conditions, the slightest suspicion becomes a sufficient condition for engaging in surveillance.

Of course, surveillance is one of the typical police actions. It often turns out to be justified as the entity placed under surveillance proves to be the actual culprit. Still, we have seen throughout the chapters of this books that suspicion remains prone to partiality and inadequacy, also when it is mediated by technologies. Rather than being adequate representations of reality – justifying surveillance or supporting prosecution in the criminal justice chain – technologically mediated suspicion appeared here quite questionable, partial and vague. Through their 'solidifying' effect, technologies can further foster unjustified surveillance and erroneous interventions.

7.3 Community, technology, identity

The argument so far supports the idea that technologies play an active, mediating role in policing practices, influencing police perception, decision and action. Rather than being neutral tools, they can solidify suspicion when they are used by officers and agents, and foster intensified surveillance of persons, groups or categories of citizens. Technologically mediated suspicion can be based on strong indicators of suspicious behaviour but also on traditionally sensitive attributes such as ethnicity, race, gender, age or nationality (see Chapter 4, Chapter 5 and Chapter 6). When these identity attributes get built in infrastructures in the context of design, technologies in policing can contribute to eroding the presumption of innocence towards categories of citizens, groups or communities, rendering them more vulnerable during encounters with the police. This section shows how the *solidification of suspicion* combines with a process of *sedimentation of prejudice* that influences police relations with communities and minority groups on an infrastructural level.

7.3.1 Policing and discrimination

Police forces have often been associated with discriminatory practices that have been documented in many reports. For instance, the Scarman report in the UK noted that a major cause of the hostility of young black men towards the London Metropolitan police included racially prejudiced conduct (Scarman 1982). More recently, a 2013 report of the Independent Police Complaints Commission (IPCC) in the UK found that "people of different racial, ethnic or national background are in fact treated in a discriminatory way, unfairly or poorly. In some cases, this is intentional. In others it is unintentional, as a result of subconscious negative racial stereotypes that inform or influence behaviour or attitudes" (IPCC 2013, 6). Or, concerning local policing in Romania, the 2014/15 report of Amnesty International found that "Roma continued to face systemic discrimination". The report notes the concerns of the Council of Europe Commissioner for Human Rights "over reported cases of excessive use of force by police during searches" (Amnesty International 2014, 303).

Community policing, we recall from Chapter 2, is a style of policing that was initially aimed at regaining the mutual trust between communities and the police. Despite the vagueness of the term 'community' (Skogan and Hartnett 1997, Tilley 2008, Wisler and Onwudiwe 2009), this style of policing has been characterized by measures seeking the cooperation of communities in solving local issues and devising priorities. Opening up of small police stations in neighbourhoods (Skogan and Hartnett 1997), forming neighbourhood patrol groups and diversifying the police force to employ members of minority groups were some of the measures in this direction.

In this sense, promoting or reaffirming the continuing importance of diversity in policing (Jones and Rowe 2015) is, indeed, a necessary process in many policing organizations. For instance, the London Metropolitan Police initiated *The Romanian Community Confidence Project*. As Chief Superintendent Taylor declares for the Romanian Journal the program is aimed at improving the Romanian community's confidence in the local police and also at "attracting the members of the Romanian community in the UK to apply for jobs in the Police". As he further mentions, "the police are willing to demonstrate their commitment and ability to treat the Romanian community fairly and to mediate impartially between the interests of different communities in the borough." (http://www.romaniajournal.ro/exclusive-the-met-in-london-

runs-project-to-make-romanians-in-uk-apply-for-police-jobs/). Concentrating on diversifying the work force of the police towards incorporating staff with backgrounds from minority communities, such measures may prove successful in combating forms of prejudice.

Still, in the absence of a unitary doctrine, community policing initiatives vary widely, spatially and temporally, as well as in their tactics and measures. New generations of community policing as well as new initiatives in local police organizations bring innovations that change the way in which police organizations interact with communities. Under the banner of community policing we have seen that one of the trends that characterizes these changes is the acquisition and employment of new technologies, to the point at which "local police departments now have access to surveillance tools more powerful than those used by superpowers during the Cold War" (Podesta, Pritzker, and Moniz 2014, 49). In this context, a question that calls for critical reflection is how are technologies employed in community policing contributing to regaining the trust of communities in the police?

On the one hand, information technologies certainly contribute to a more efficient policing by speeding decision making processes. They often provide precise information about criminal activities that are going on in communities and make possible big data analysis to enable efficient resource allocation at a local level. On the other hand, we have seen throughout this book that technologies can also play a role in reinforcing discriminatory practices towards various groups, areas and communities. That is, the potential prejudice of policing practitioners towards minority groups is not only stemming from their implicit views and attitudes but the technological infrastructures they work with can influence these assumptions.

A similar point is raised by Simon Cole concerning the effects of automatic fingerprint identification systems (AFIS). He shows how the automation and spread of fingerprint identification "allowed law enforcement agencies to create criminal records for ever pettier offenders" (Cole 2001 258). The merging of technological affordances with practices of identification entailed a further increase in the likelihood that already marginalized groups get selected for arrest. The effect of AFIS technology tended to be highly prejudicial to "those who live in neighbourhoods targeted by police or who have an appearance – skin colour, dress, and so on – targeted by the police" (Cole 2001, 258).

'Suspicion', we have seen, can be more than a social construct, produced by the culturally shaped categories and idiosyncrasies of agents. Rather than forming only in their minds, 'a suspect person', 'a suspicious group' or 'a dubious activity' is also what the screens enact as such. When prejudiced views are embedded in code and logged in classified artefacts they tend to trickle down in infrastructure and become invisible. In this way, they sediment and implicitly and effectively affect the communities at stake. The measures towards diversification of the police force may not be adequate for dealing with prejudice that got incorporated in the very technological infrastructures.

7.3.2 Sedimentation of prejudice

In this sense, I propose to understand this phenomenon with an analogy from geology. Borrowing a metaphor from this discipline, we might call this a 'sedimentation' process that takes place in the context of design. In geology, the term sedimentation is used to describe the gradual deposition from a solution (e.g. water), which results in settling and accumulation into sedimentary rock (e.g. on the river bed). Particles that form a sedimentary rock by

accumulation are called sediment. In the context of policing I want to suggest that technological infrastructures can entail a gradual disappearance from attention and scrutiny of classifications, categories, algorithmic steps, architectural decisions or identity attributes. Getting 'buried' into infrastructures, prejudice can accumulate, harden and acquire a character of objectivity. At times, it rises to the surface, becoming potent and effective in mediating police action towards the enacted entities.

We have seen this phenomenon in the situation of the community policing in Romania. In the local police system the representation of 'begging' was coded with black dots (see Chapter 4). The views of the police officer who happened to configure the system got built into the technological infrastructure and trickled down further in the practices of the other officers who worked with the system. Her views concerning the begging practices of Roma ethnics generalised in the technological infrastructure through the GIS representations. From then on, they accumulated and acquired new strength and spread. Not only was the GIS displaying one black dot on the screen but these automatically multiplied in every weekly map with 'the beggar distribution' throughout the city. As the other interviewed officer confirmed, the software-enabled maps evoked a cumulative effect. All begging was done by Roma ethnics. Irrespective of the statistics on the matter, the technological infrastructure induced a uniform perception of the phenomenon. At the same time, without the interview question, the interviewed officer was not aware of the origins and action of the software-enabled artefacts of the colour codes. In this way, 'the past' sedimented in technological infrastructures and carries on prejudice into 'the future'.

In cases such as this one it may not be sufficient to have a diverse workforce with respect to the staff's background, covering multiple minority communities. Once classifications and stigmatisations are translated in infrastructures they tend to disappear from scrutiny and affect those communities implicitly. When these technologies incorporate prejudice it does not matter that much how well intended the officers, as the socio-technical ensemble fosters the discriminatory actions. No matter how diverse the police staff, they work with technologies that actively mediate their perception and action.

7.3.3 New sensors and the spreading of suspicion

I have discussed so far the way in which technological infrastructures can contain '*sediments of prejudice*' regarding an old set of criteria. Ethnicity, race, nationality are known as sensitive identity attributes that are associated to discriminatory policing practices. Especially debates about police-minority relations are often dominated by these criteria. This section raises awareness concerning the 'diversification' of suspicion criteria with new categories that may get buried in infrastructures. As pervasive sensing infrastructures – enabled by developments in the areas of 'Internet of Things' or 'Smart Cities' – produce a staggering amount of personally identifiable information and as police organizations access or develop algorithms to process this data, new groups and new categories of people may enter the scope of proactive police surveillance.

We can recall here the situation analysed in section 6.5.3 where a planned police profile was using intelligent surveillance cameras (ANPR) to survey expensive vehicles whose owners had 'under 27' years of age. In this way the profile would place under surveillance not only 'suspected drug dealers' but also a whole category of successful young entrepreneurs who could afford such vehicles at that age. The situation shows how automated profiling can enact new groups that can enter the focus of police surveillance at the change of a single algorithm

parameter. The profiling of this group was not based on concrete cases nor on ethnicity or race. Instead *age* became an identity attribute that was enrolled in a new police profile.

We can also recall the criteria for problematic behaviour concerning youth groups (see section 5.4.3). The label 'annoying' was associated to these groups rather loosely, summoning a large number of youth under its scope. Moreover, we have seen that youth interactions on social media were playing an active role in making the delineations between groups quite fluid. What a youth group was on social media became dissociated from 'the youth group' as defined in the police system. Still, the police organization maintained these software-enabled entities in the system, giving them a fixed name and identifying them through this reference. In this way the policies and interventions they developed, were implicitly and effectively reinforcing the problematic character of these youth.

The analyses point towards new forms of identity and new communities that are being performed within infrastructures and police practices. That is, policing practitioners assign a problematic character to a person, a group or a category based on algorithmic processing of identity attributes and not only on behavioural patterns. The criteria of suspicion may yield situations in which new groups and communities unjustifiably enter the scope of surveillance. In this way they become vulnerable during encounters with the police.

Still, the practice of categorical suspicion is not illegitimate per se in the context of police work. Categorical suspicion not necessarily implies mass surveillance of whole categories of citizens. When multiple sensors are aggregated from 'railways, waterways, cyberspace' (Schakel, Rienks, and Ruissen 2013) they can also produce more accurate, contextualized and situated suspicion. As police organizations gain legal access to a variety of non-police databases and information infrastructures, they mine these data and combine information into automated alerts and profiles. Not everyone needs to be under surveillance but only those that simultaneously satisfy multiple criteria related to a case.

For instance, only those that simultaneously were 'in a red vehicle' AND 'were young' AND 'were black' AND were driving in the vicinity of 'a particular location'. If a profile combines multiple identity attributes with behavioural profiling the scope of surveillance is contained and the risk of prejudice towards whole communities is minimized. However, this implies that profiling criteria and technologies need to be made transparent as their values, their algorithm and their logical operators become the loci of distinguishing between legitimate and illegitimate police surveillance and action. A mere change in the software code from an AND to an OR drastically increases the scope of a profile. Even when running such an algorithm at a local, community level, its scope can significantly increase to include large numbers of members of the communities.

Therefore, we need to continuously scrutinize the underlying lithology of infrastructures and gather data and evidence on the nature and depositional conditions for sediments of prejudice. The investigations need to span both depth and spread to derive information on the types of sediments, their distribution and dynamics. This may mean periodically reviewing the code of risk profiles, probing the output of surveillance technologies against dynamic changes in the environment and expanding the scope of investigations when police profiles aggregate multiple sensors and databases.

7.3.4 Conclusion

Almost two decades ago, Janet Chan, a researcher in police-minority relations, argued that "changing police culture requires changes not only in the cultural assumptions held by police officers but also in the political and organizational conditions of police work" (Chan 1997, 28). Drawing from studies of police practices in New South Wales, she concluded that a combination of factors is necessary for improving police-minorities relations. Not only strategies such as cross-cultural awareness training and community-based policing but also "appropriate structures of police accountability and legal regulation, as well as social reforms" (Chan 1997, 28).

This section strengthens the argument that technology should be included in this list of reforms. Besides organizational, legal and cultural reforms in policing, technology design should be scrutinized as well if confidence in the police should be increased in communities. New technologies are not a guarantee for mutual trust but should be questioned as well as they can deposit 'sediments of prejudice' in the strata of infrastructures. The sedimentation process combines with the solidification effect on a new level. With the growing expansion of information infrastructures in our cities and communities, critical reflection needs to be extended towards technologically mediated policing, excavating in loci such as the profile criteria, the limits of cases or the classifications of entities. Engaging infrastructures in this way could expose problematic ways in which values with moral importance got to be encapsulated in technological designs. While we may need to broaden the diversity agenda beyond the terms of race and ethnicity (Jones and Rowe 2015) we may also need to deepen it, analyzing processes of sedimentation where 'pockets of prejudice' may have formed.

7.4 Values, technology, policing

In an influential text on 'the policing of the future', John Alderson listed a set of objectives (Alderson 1977). Policing – he wrote four decades ago – should contribute to liberty, equality and fraternity, it should 'help reconcile freedom with security', 'protect human rights and help achieve human dignity', 'create trust in communities', 'strengthen security and feelings of security' and 'curb public disorder'. Taking this reference only as a backdrop, we can see even at a cursory reading that these objectives are dominated not so much by managerial goals (e.g. curbing public disorder) but by values with moral import – 'freedom', 'security', 'trust', 'dignity', 'equality' and other human rights.

This is, of course, no surprise. The police as an institution is pervaded by moral values both in its education, policy and practice. However, what we have seen in this book is that contemporary policing cannot be properly understood without an account of the role of information technologies in guiding or informing its practices. Whether by making adequate or inadequate contributions, technologies influence to a significant extent individual practitioners and policing processes in general. If we would project today the goals that Alderson set for policing four decades ago, we cannot ignore the ways in which technologies embody normative charges in their design. Technologies have value(s). To account for them in policing we need to understand values as empirical categories and analyse the ways in which they are translated in the technological designs that enable day-to-day police work.

This section discusses the explicit and implicit ways in which values got built in the designs of policing technologies. It starts with a summary of the 'privacy by design' attempts of the police projects analysed in the previous chapters. Then it presents Value Sensitive Design and makes an argument for a broader uptake of this approach in policing as a way forward to accompany the growth of technologically mediated policing in a world of ubiquitous sensing infrastructures. It ends by qualifying this suggestion and links up with the argument for a sedimentology of infrastructures.

7.4.1 Doing 'privacy by design' in policing technologies

We have seen already in section 6.2 that privacy is not only a value discussed in the realm of philosophy but it is stipulated in legal frameworks that further aim to enforce its incorporation into technological designs. The European General Data Protection Regulation (GDPR) with its article 23 on 'Privacy by Design and by Default' already acknowledges that values cannot be protected merely through laws but they need to be taken into account throughout the whole engineering process. Still, we have also seen that there is no binding obligation in the GDPR for data controllers to implement particular solutions over others when considering the principles of 'privacy by design'. In this context, some policing agencies took up the idea of 'privacy by design' and started to explore innovative ways of protecting people's values while simultaneously aiming to perform their policing duties.

For instance, we have seen in Chapter 5 how the Dutch police designers considered 'privacy' an important value for their mission and made several attempts to translate it into the design of an internet monitoring technology. We can recall here the solution analysed in section 5.4.4, aimed to enable police forces to gather, store and analyze information from the internet. In the words of the officer/designer, restrictions should be built into technology to account for privacy protection: "*You can´t get a big net on the internet, 24 hours a day, and just pull all the information in and keep it for 20 years. You can't do that. You will violate privacy; you will violate all legal restrictions. I strongly believe you shouldn't do that"*. We can see from this quote that there is an awareness, at least among the interviewed police officers, that consequences of technologically mediated actions cannot be adequately understood without reference to the value choices made in the design of these policing technologies.

To further strengthen the point, the officer/designer reminded of more restrictions that they planned to build into the technology to prevent the exposure of data to a wide range of officers [at the time of the interview the police were still waiting to work with the solution]: *"Their legal profile [will] decide whether they have all the widgets or just a few. So you can expect a policeman to have more legal possibilities than a tax investigator or somebody at a lower government. [The technology will] let user A only look at public Facebook profiles and user B, because he has a lot more possibilities from a legal point of view, get behind the front door of Facebook".* These specifications of 'legal profiles' that limited the system's affordances depending on each type of user in the police, were attempts of the designer to translate privacy into a technological solution. This is demonstrative of the ways in which police designers can resist the temptation to understand technologies of surveillance in a determinist manner and proceed to engage technologies as (f)actors for improving privacy protection.

Similarly, for the ANPR technology, Dutch police designers looked to incorporate 'privacy' by combining profiling with cryptographic techniques. Their engagement of sensor networks (among which ANPR cameras were seen as one type of sensor) were seen promising not only for identifying suspects in large flows of vehicles but for being 'protective of privacy' at the

same time. Profiles were defined through knowledge sharing between multiple police branches (and not so much through data sharing), to select suspicious behaviour (and not categories based on identity attributes) and to protect the privacy of those who do not match the criteria of the profile (and whose privacy was not revoked).

Not only were individual designers conscious of the need to protect privacy but police documents accounted for the importance of this value for the police mission. We can recall here a vision document for the Dutch police, according to which technologies were the solution to "prevent an unnecessary infringement on the privacy of people who are not under any suspicion" (Hoogewoning 2006, 79). In all these situations, designers and policy makers made it explicit that privacy is a value that they stand for and they wanted to make sure it would find its way into the infrastructures that enable and influence police work.

7.4.2 On Value Sensitive Design

Of course, many moral values are translated and enacted in the legal domain. Values such as privacy and non-discrimination are not only discussed and debated but are incorporated in concrete laws and broader legal frameworks. Still, the analyses of the previous chapters often highlight that many social, political and moral values choices that designers could have been aware of, escaped their attention during the design of technologies. Merely considering one value may not be sufficient to simultaneously protect other, equally important, values (Van den Hoven 2007).

Analyses in this book showed that values such as non-discrimination, autonomy, transparency, consent, trust, personal safety or dignity played important roles in many situations. When they are overlooked in design processes, the technologies that end up being used by officers in their day-to-day work can incorporate problematic charges. These in turn can induce unjustified surveillance, foster privacy erosions and affect the personal safety and human dignity of people during encounters with the police. In this light, designing technologies is a moral endeavour fraught with moral value choices.

A promising way forward to account for multiple values during design comes in the form of Value Sensitive Design (VSD) in developing policing technologies. VSD is a particular approach to the development of technologies that aims to explicitly account for moral values throughout the design process (Friedman, Kahn, and Borning 2006, Van den Hoven 2007, Friedman, Kahn, and Borning 2002). Initially an umbrella term for a set of unaffiliated projects, VSD has become a term designating "strategies and techniques to help researchers and designers explicitly incorporate the consideration of human values into their work" (Davis and Nathan 2015, 1).

The growing set of case studies available in the VSD literature shows how this is possible in practice. For instance, (Friedman, Smith, et al. 2006) developed "a workable privacy addendum for an open source software license that not only covers intellectual property rights while allowing software developers to modify the software (the usual scope of an open source license), but also addresses end-user privacy" (Friedman, Smith, et al. 2006, 194). This example illustrates how it is possible to integrate in design the value of informed consent with developing privacy protections for ubiquitous location aware systems.

In the VSD approach the word "value" is defined broadly, as what a person or group of people consider important in life (Friedman, Kahn, and Borning 2006). The approach builds on the

insight that values and norms are always at stake, either implicitly or explicitly, during design processes. Therefore, if we make the effort in design to reflect on values, technologies can be shaped in advance in more ethically informed ways. Friedman, Kahn and Borning (2002) propose VSD as "a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" (Friedman, Kahn, and Borning 2002, 1).

This means that designers and researchers that take a VSD approach iterate through three types of investigations: conceptual, empirical, and technical and they aim to integrate them throughout the design process (Friedman and Freier 2005). A conceptual investigation means identifying what values of stakeholders are at stake in a particular design choice and researching the existing philosophical literature about how are those values conceptualized and what criteria have been used for their assessment. An empirical investigation delves into explorations of human-technology relations and the larger arrangements in which these feature. This may involve interviews with stakeholders and users, observations of practices or analysis of relevant documents. For example, in a VSD project Azenkot et al. (2011) "interviewed blind and deaf-blind people" and "surveyed public transit drivers". In this way they learned about the "patterns, challenges, and important values related to public transit use by blind and deaf-blind people" (Azenkot et al. 2011, 1). Third, technical investigations concentrates on the features, properties, design choices or performance of the artefacts themselves. These analysis can identify ways in which the values play a role and they can be projected on the design of a new technology or system. The iteration through these three types of investigations ensures that each investigation influences the additional investigations on the dimensions throughout the design process.

A particular characteristic of VSD implies the consultation of both direct and indirect stakeholders. For example, in a computerized medical records systems the direct stakeholders are users, such as doctors, nurses, insurance companies, or hospitals while indirect stakeholders, no less important for the design of such a system, are the patients (Friedman and Freier 2005). Their values and interests are relevant for the design of the system even if they don't directly use its features. In this sense it is relevant to mention that VSD is an interactional theory, meaning that values are viewed "neither as inscribed into technology (an endogenous theory) nor as simply transmitted by social forces (an exogenous theory). Rather, people and social systems affect technological development, and new technologies shape (but do not rigidly determine) individual behaviour and social systems" (Friedman and Freier 2005, 361). Therefore, VSD is compatible with the approach argued in Chapter 3 and taken throughout this book and could be a way forward for many technological developments in the area of policing and law enforcement.

VSD has also been proposed in military projects, an area one might not initially associate with such an approach. For instance, a VSD study was proposed in the development of a military cruise missile (Cummings 2006). The conceptual investigation built around the value of human welfare, but also drew from the theory of just war, and the principles of proportionality and of non-discrimination. Borning and Muller add, concerning this project, that "one can also imagine VSD analyses for military applications for direct use by combat soldiers or other warfighters that implicate additional values, such as courage, honor, discipline, loyalty, and accountability. This domain does not fit comfortably in the usual values discussion in the human-computer interaction community – but (unless one believes there should be no new military systems) it makes sense to consider military systems from a VSD perspective and to design them well, so these philosophical traditions and values are certainly relevant" (Borning and Muller 2012, 5). In a similar vein, it also makes sense to consider VSD in policing.

7.4.3 Argument for VSD in day-to-day policing

The VSD literature provides a growing set of case studies and success stories (Borning, Friedman, and Kahn 2004, Kahn et al. 2008, Friedman, Kahn, and Borning 2006, Friedman, Kahn, et al. 2006). Still, VSD had so far a limited uptake in industry. Part of this limited spread had been the criticism concerning the presentation and relation to values (Borning and Muller 2012). VSD took the position that certain values are universally held even if "how values play out in a particular culture at a particular point in time can vary" (Friedman and Freier 2005, 370). VSD presented them as predetermined lists that "should have a distinctive claim on resources in the design processes" (Borning and Muller 2012, 4).

Considering multiple values as universally held can often create difficult problems for designers that need to reconcile them with the each other and with the commitment to consider the values of direct and indirect stakeholders. On the one hand, we have seen throughout this book that broadening the set of values to be considered in day-to-day design of police profiles, algorithms and classifications is often a relevant goal. On the other hand, the question remains how then to overcome these problems if VSD should be more broadly taken up in the design of policing technologies?

Concerning the validity of this goal, the argument is easier to make. Policing itself aims to be a highly moral service in society. Many police documents attest to the plurality of values that police organizations uphold themselves. For instance, we have seen above Alderson's account of the values that the police should serve. Or we have seen in the previous chapters the vision document for the Dutch police, which understands the police mission as being "supported by a set of values. Internal values form the ethical compass for the police service and its people. […] External values are values crucial to the environment in which the police operates" (Hoogewoning 2006, 33). Therefore, the plurality of values that the police should account for is explicitly acknowledged here as a valid mission of the police.

The issue of universality of values remains more contentious. How can technology designers reconcile, for instance, the perpetrators' value of autonomy with the victim's value of personal safety or with the social value of security? The goal of reconciling stakeholder's values in design has been one of the drawbacks for a large uptake of VSD (Borning and Muller 2012). However, this goal may become less demanding if we consider a recent trend in VSD. Alan Borning – one of the early founders of VSD – and Michael Muller acknowledge that "the theory and at times the presentation of VSD overclaims", meaning that VSD takes the position that certain values are universally held, which is "enormously problematic" but also "more sweeping than necessary" (Borning and Muller 2012, 5).

In this sense, they suggest "tempering VSD's position on universal values" and contextualizing lists of values as heuristics for consideration (Borning and Muller 2012, 5). This means that VSD researchers should refrain from demanding a particular set of values and commit only to "just those values that make VSD work": namely pluralism, inclusivity and transparency (necessary to involve direct as well as indirect stakeholders) (Borning and Muller 2012, 5). At the same time, this take on VSD does not imply 'anything goes'. Borning and Muller (2012, 5) argue for making more visible the position of the VSD researchers/designers and their own values. This visibility allows for evaluating the ways in which they uphold different values and how they resolve value conflicts within a VSD project.

The shift towards pragmatism in VSD may mean less demands for police designers when considering and incorporating large sets values in their technologies. We don't need to reconcile all values of all stakeholders but we can do a much better job at including more values and more stakeholders' values in design. We have seen already in this book several police projects that explicitly implemented 'privacy *and* security by design' in their technologies. Despite their drawbacks, these projects demonstrate that it is an attainable goal to explicitly consider and implement multiple values in the design of policing technologies. VSD expands the scope of design by informing how multiple values may be at stake in the design of policing technologies. In the context of a still emerging legislative framework to regulate novel police practices and technologies, a VSD approach can bring awareness in the design context of technologically mediated policing.

For instance, a VSD approach while implementing social media monitoring technologies could have made engineers aware not only of 'privacy by design' but also of new (and older) forms of problematic discrimination that were being hidden (i.e. profiling was not necessarily based on ethnicity or race but also on nationality, age or income). These values are equally important in designing information infrastructures as it is already apparent in a set of publications that aim to reconcile privacy and discrimination in data mining police practices (Kamiran et al. 2012, Mancuhan and Clifton 2014).

Similarly, a VSD approach could have made designers aware of new forms of identity that were being used in algorithmic processing for assigning the character of someone or a group. For instance, owning an expensive car may be for some a way to perform their identity. While 'showing off' with one's vehicle may be a matter of taste for many, it is certainly not a sufficient justification to be included in an automated profile that selects these vehicles in surveillance practices (see section 6.5.3).

Finally, a VSD approach could have made designers aware of new ways of eroding the presumption of innocence while protecting the integrity of professional norms (see section 4.3.1). The colour choice for 'begging' could have been easily changed if there was awareness about non-discrimination at the time of configuring the system. In the absence of this discussion – that a VSD process could have elicited – the views of one officer was generalized in software and trickled down in prejudice towards a whole group. Once police organizations acknowledge the need to take seriously the normative charge of technologies, they may need to consider a much larger set of values in their design.

Value lists as heuristics could inform the designers in dialogue with the policing practitioners in identifying issues at stake, creating a cognitive link between social and technical considerations. If developers of technologies aim to prevent the accumulation of prejudice in infrastructures they may need to account for the way in which technologies promote or erode values with moral import. A possible path forward is to bring to the surface the latent ethical concerns of the designers. The approach can have a significant role in the emergence and evolution of alternative development paths by rendering more visible the elements of the decisions in front. A broader uptake of a more pragmatic take to Value Sensitive Design could contribute to steering technologies in an iterative approach throughout the design process as contrasted to a one-time impact assessment.

Still, is the large majority of police designers ready for such an approach? Are police organizations open to considering multiple values in their technologically mediated practices? Indeed, this is a choice that many police organisations will need to make in terms of time and

resources. I have only given in this this short section a reduced set of examples that show the feasibility of the approach. But until police organizations and technology developers decide to take up VSD on a broader scale, technologies risk encapsulating dangerous sediments within the layers of their software stack.

7.4.4 Towards a sedimentology of infrastructures

Although the attempts to build values in design are important and – indeed – responsible innovations (Von Schomberg 2011), we have seen throughout this book that it was not always sufficient to uphold a value in design to have it protected. When translated in a set of norms to guide the implementation the situation got more complicated. Upholding a value in design is a necessary but not a sufficient condition for its protection when we are dealing with an increasingly technologically mediated policing. Equally important are the ways in which it is translated in code and embedded in infrastructures.

For instance, in the analysis of social media monitoring technology (see Chapter 5), we have seen how the police construction of 'cases' shaped the data gathering process. Cases can be quite flexibly defined and police officers are able to gather large amounts of data as part of a case at hand. While 'privacy by design' may offer guidance with respect to information management, it remains abstract or silent in terms of what a user/police officer is able to define as a 'case'. This aspect is not regulated by design but by users and procedures. Even when police designers explicitly built conceptions of privacy into their designs, in daily practice police officers have a significant set of affordances to define new cases and expand existing, loosely defined ones.

Therefore, even when police designers are highly aware of the importance of a value this does not automatically translate in its adequate protection. Implementation issues became crucial factors in the process of building a value in the design of policing technologies. Software design choices, data mining algorithms, system classifications can incorporate identity related attributes that can open up new values dimensions and foster discriminatory actions when taken up in police practices.

A VSD approach doesn't solve all problems in policing. However responsible a technological design may be, it can only partially influence the way a technological system features in practice. This is particularly relevant in the management of sensor networks, as these technologies can be easily reconfigured in the use context (Dechesne, Warnier, and Van den Hoven 2013). Profiles, for instance, need to adapt on a regular basis to changes in criminal behaviour. When they connect to new sensors in the use context, they introduce new choices with potentially new discriminatory criteria. Therefore, awareness of values needs to be involved in the design as well as in the use and management of policing technologies. Despite the consideration of values in design, we need to promote more studies that explore the "data assemblages and power/knowledge" in indicators, dashboards and other (city) governance technologies (Kitchin, Lauriault, and McArdle 2015, 25). Technologies still need to be analysed in the broader socio-technical ensembles in which they feature.

In this sense I propose to borrow a metaphor from geology to analyse the breadth and depth of socio-technological infrastructures. Sedimentology studies the structure of sedimentary rock and the processes that result in their formation (Nichols 1999). As I will show in this section, applying the insights of this discipline can help us to understand how sedimentary deposits form

and change through time and space while a *lithology of technological environments* could describe their types and characteristics. A geological way of understanding infrastructures maintains the approach of 'digging up' strata that potentially encapsulate relevant deposits – for instance of prejudice – while simultaneously resisting a bias for anthropocentric explanations.

Unlike archaeology, which studies human activities in the past, *a sedimentology of infrastructures* might prove here an adequate metaphor to study the role of both humans and non-human actants. Of course, human activity played a role in design processes but the phenomena we can encounter may or may not be traceable to an initial human activity. At the same time, archaeology – as one of the first academic disciplines to seriously analyse technological change and the social role of artefacts – has a major contribution to this day in the spread of technological determinist views (Wyatt 2008). Wyatt, drawing on Mumford, shows how our contemporary tendency to give reductionist accounts for the social role of technology often stems from an archaeological vocabulary that associates societies, civilizations or whole ages to a single material artefact that happened to be the remaining record (e.g. 'Stone age', 'Bronze age', 'Iron age', 'Computer age' or the 'Beaker Men', the 'Double Axe Men', or the 'Glazed Pottery Men'). As Mumford argues, "the absence of documents and the paucity of specimens resulted in a grotesque overemphasis of the material object, as a link in a self-propelling, self-sustaining technological advance, which required no further illumination from the culture as a whole even when the historic record finally became available" (Mumford 1961, 231 as cited in Wyatt 2008, 168).

In turn, the technologically determinist habit in vocabulary pervaded a whole range of contemporary institutions such as "museums, schoolbooks, and newspapers and on television and radio" (Wyatt 2008, 168). The list of institutions often includes the police as well. We can recall here multiple authors in policing literature illustrating technological determinist accounts (see section 3.2). A shift towards a geological vocabulary would therefore be a step towards correcting this unfortunately-old linguistic habit. Derived from archaeology, this habit tends to explain complex socio-technical phenomena by identifying the man-made artefacts as the primary driving factor.

Finally, bringing in notions from geology to understand technological infrastructures becomes even more relevant in a context in which many organizations engage in practices of data 'mining' – yet another metaphor closely related to the enterprise of understanding and exploring sediments. The vocabulary of many contemporary policing departments is pervaded with 'data mining' practices in which police analysts seek to 'extract' patterns of suspicious behaviour that may be 'hidden' within large 'piles' of data. Haggerty and Ericson also speak of the trails of information about a person's habits, preferences, and lifestyle as 'the *detritus* of contemporary life' (Haggerty and Ericson 2000, 611).

Bringing together these geological metaphors shows even more the relevance of engaging in a sedimentology of technological infrastructures to identify potential 'pockets of prejudice' that may have formed within its 'layers' of software code, algorithmic steps or architectural features. At the same time, a geological metaphor to understand infrastructures may not only conjure up an image of solidified entities and hardened layers but also an image of *flows* of debris, volcanic *explosions* and other dynamic processes. As we have seen throughout this section, how the location of sediments of prejudice can range from 'close to the surface' – as in the case of recently finished algorithms or accessible program parameters – to the 'buried' architectural decisions that get forgotten and persist over the years.

As typical for sediments, there is a correlation (albeit not absolute) between the depth of the sediment and how hard it got to be. That is, the more difficult it is to access and change a particular feature or an algorithmic step and the more time passed without it being changed, the more it tends to be taken for granted. On the one hand, being taken for granted is often manifest in programmers' habits of copy-pasting existing code to new versions ('Why change an old piece of code that has proven to work'). On the other hand, when such 'sediments of prejudice' come to the fore they tend to induce a perception of objectivity towards the enacted group or community, affecting their presumption of innocence, privacy, and other values with moral import.

7.4.5 Conclusion

In their introductory essay to the *Handbook of Knowledge-based Policing*, Bordeur and Dupont acknowledge that too much reliance on automated technological solutions to reveal suspects increases the chances that there will be problematic outcomes. As an important cause for these outcomes they identify "the fact that these tools are designed by engineers and computer programmers instead of experienced investigators" (Brodeur and Dupont 2008, 25). Brodeur and Dupont question "how many names on those endless lists of suspects" provide valuable leads and "how many people with unconventional consumption patterns were flagged as potential jihadists" (Brodeur and Dupont 2008, 25).

On the one hand, this section argues for the need and opportunity for a larger uptake of Value Sensitive Design processes in technologically mediated policing. The previous chapters have shown that many problematic outcomes could have been prevented or minimised, given ethical reflection and consideration of multiple values in the design of policing technologies. On the other hand, technologies work within organizational, legal and use contexts. However responsible a technological design may be and however experienced the investigators that participated in its design, it can only partially influence the way a technological system is engaged in practice. Socio-technical arrangements in policing still need to be continuously scrutinized with an approach that pays attention to the character of sediments that may have accumulated in infrastructures.

7.5 Limitations and future work

This book discussed a diverse but limited set of situations in police organizations throughout European Union countries: The Netherlands, England and Romania. The analyses in this book do not claim to represent all the practices, officers and the specific organizations, let alone the police systems of those countries as a whole. As specific for qualitative research methods, the analyses in this book aim to illustrate, highlight and contrast (new) phenomena and provide in-depth explorations of technologically-mediated policing practices. In this sense, they act as entry points for providing thick descriptions of the practices, affordances and ethically relevant aspects of both wide-spread and state-of-the-art policing arrangements. They argue for and point towards further research in technologically mediated policing with the proposed theoretical approach. In other words, *we've just scratched the surface*.

Much more work needs to be done when we contemplate the significant investments that are made in the development and roll out of 'Internet of Things' (International Telecommunications Union 2005, European Commission 2009b, Gubbi et al. 2013) or 'Smart Cities' (Kitchin 2014). On the one hand, 'smart cities' and other similar terms refer to visions about knowledge based economies, innovation, creativity and entrepreneurship, all made possible by smart people. On the other hand, a smart city refers to "pervasive and ubiquitous computing and digitally instrumented devices built into the very fabric of urban environments […] that are used to monitor, manage and regulate city flows and processes, often in real-time […]" (Kitchin 2014, 2). A common feature of these visions is an emphasis on data gathering and processing to enable dynamic and efficient decision-making and fine-grained, real-time control.

In these visions, "data are seen as providing objective, neutral measures that are free of political ideology as to what is occurring in a city, with the weight of data speaking an inherent truth about social and economic relations and thus providing robust empirical evidence for policy and practice" (Mayer-Schonberger and Cukier 2013 as cited in Kitchin 2014, 3). However, what we have seen in this book is that data is not always providing an adequate representation of reality. Technologies can embody the peculiar world views of their designers or configurators and, in the area of policing, can enact particular views about what is suspect, risky or weird.

Against the background of these developments it may not be enough that a few pilot projects in policing engage in explicitly considering 'privacy by design'. There needs to be a broad movement in policing – to accompany the explosive growth in data and the shift towards proactive styles – that engages a Value Sensitive Design approach and seriously considers a wider range of values. However, this presupposes a shift in thinking about technology in policing from determinist and instrumentalist views on technology towards more constructivist and performative accounts.

A strength of the approach developed in this book is that it offers a vocabulary to trace how various human and non-human actants perform suspects, problematic groups, suspicious behaviour, suspect situations, vehicles, and other entities of police interest. Rather than understanding technologies as tools, useful but obedient in the hands of policing practitioners, a more adequate approach is to analyse technologies as entities that act. Without falling into a technological determinist stance, we need a vocabulary that acknowledges the active role of information technologies. Besides constables, agents and officers, information technologies, too, have agency. They do stuff. Their active role is not just the realm of science fiction or highly sophisticated military projects but it is increasingly characteristic for mundane artefacts in our day-to-day lives. The technologies that the police engage with significantly mediate where, when and whom they put under surveillance.

To promote an efficient policing that protects us from crime as well as from discriminatory interventions and unjustified surveillance we need to continuously engage in studies that probe our technological infrastructures. On the one hand, this means analysing technologies within the socio-technical ensembles in which they feature, along organisational structures, legal frameworks or architectural arrangements. On the other hand, it means performing a lithology of software layers and then beginning to excavate in loci such as the criteria, algorithms, categories and values that shape their design and architecture. Without fetishizing the importance of code, failing to engage in a sedimentological approach allows for the formation of potentially explosive 'pockets' in the software layers of our infrastructures.

Summary

Introduction

Policing matters. The obvious reading of this book title suggests that policing services are likely to gain an increasingly important role in contemporary (European) societies. Of course, policing has been one of the key institutions of sovereign states, entrusted with the use of force in a large array of situations and activities. Policing matters in controlling crime, in protecting property, in securing order and in many other situations with potential for conflict, disturbance and deviance. Moreover, policing receives new challenges and importance against the background of heightened levels of global terrorism and of an increasingly mobile and migratory citizenry, in which massive amounts of people, goods and information are able to move across areas, often in different cities and jurisdictions.

At the same time, these broader socio-technical trends are fostering processes that are not leaving policing matters unchanged. On the one hand, a movement in policing promotes a shift from reactive, investigative approaches towards more proactive and preventive styles. While reactive policing aims to solve committed crimes, proactive approaches aim to strengthen the preventive character of policing. This involves risk assessments rather than only post-factum identification of suspects and perpetrators, assessing suspicious behaviour before an actual crime is committed or performing profiling and early signalling.

On the other hand, a constant of this trend has been the increasing engagement of digital surveillance for exercising decision-making and resource allocation. Digital technologies have become pervasive in our environments and are increasingly relied upon in many policing practices. From intelligent video surveillance and other sensors distributed throughout our smart cities to profiling algorithms and geographical information systems – processing location data and connecting to other databases to enable spatial-temporal analyses – information technologies are steadily becoming constitutive of contemporary policing. Police bodies may vary widely in terms of their organization, functions, themes, priorities or jurisdictions, but they share styles, models and technologies for doing policing.

Chapter 2 gives an overview of contemporary policing models and their association to information technologies: Community policing and its ‘low-tech’ practices, Compstat and geographic information systems, intelligence-led policing and surveillance technologies, and knowledge-based policing and automated profiling. This review of policing literature includes a brief historical account of the ways in which these influential policing models came about in the past decades. At the end of the chapter, the reader should be familiarized with the panoply of contemporary policing models and associated information technologies.

Questions and approach

While information technologies promise to improve the speed and efficiency of police decisions in protecting us from criminal manifestations, they may also bring about problematic outcomes: erroneous interventions that are difficult to prevent, as databases often contain hidden partiality,

ambiguity and error; violations of personal privacy, as they facilitate easy access to the personal data of large numbers of people; discriminatory measures towards persons, groups, areas or communities, as algorithms often contain explicit or implicit, intended or unintended problematic classifications – often based on behaviour but also on socio-economic status and identity attributes (e.g. race or ethnicity); erosions of the presumption of innocence, as they automatically generate indicators of suspicious behaviour before/without crimes being committed; and redefinitions of deviancy and suspicion that call for critical reflection.

These kind of practices and outcomes can have profound social influences: they can lead to unjustified arrests, provoke debates, influence laws, trigger protests and in general shape our society. Of course, issues such as false positives, privacy violations or discriminatory practices are not new in police studies. The gap that may need extra attention though concerns the detailed role of information technologies in these practices. If we want to promote a fast and efficient police while avoiding problematic outcomes we need to investigate the role that technologies play in influencing the decision-making process in policing. If fundamental human rights and values should be persistently upheld, if we want them to play an important role in shaping our future societies, it matters how policing is done. If we want a police that is transparent and accountable in a dynamic, technologically-pervaded environment, this gap needs to be bridged.

From one direction of this 'bridge', the present book aims to contribute with an analysis of the ways in which digital technologies are implicated in transformations of policing practice. This implies a study of their role in changing policing routines, shaping practitioners' perceptions and influencing police action. Therefore, one set of sub-questions derived from this goal looks at the ways in which technologies influence police decision; what roles do they play in processes of inferring suspicion; how do they influence practitioners' behaviour? In sum, what are the police doing with technologies and what are the technologies doing to them?

If the problematic outcomes of certain contemporary policing practices partially stem from the normative charge of technologies, we should also reflect on the ways in which norms get built in technology design. From the other direction of the 'bridge', this book aims to contribute with an analysis of the ways in which the design of policing technologies is being shaped within socio-technical arrangements. This implies asking what values are implicitly built in policing technologies; how do designs get their moral charge; how do values and norms get to play a role in the design of classifications, profiles or suspicion categories in police systems; how do the developers of technologies explicitly build values and norms in design; what are the ethical implications of the practice of translating norms and values into computer code?

Engaging in an analysis of the policing matter – i.e. the material dimension of policing – with potentially profound implications for social values and fundamental human rights, requires a sufficiently broad understanding of the relations between technology and society. In this respect, the book draws on the body of knowledge developed in the fields of police studies, social studies of science and technology, philosophy of technology and surveillance studies.

Chapter 3 offers an analysis of the ways in which technology has often been rendered in the policing studies literature. Drawing from insights from philosophy of technology, the chapter illustrates the influence, implications and limitations of several discourses on technology. It points out how some authors render technology as a tool for efficient police work or as being instrumental for implementing organizational innovations in policing, while others give it an almost autonomous agency, whether with a positive or a negative character. In-between these views the chapter lays out the analytical stance of the book. It explains and shows the relevance

of insights from science and technology studies (STS), surveillance studies and philosophy of technology in providing a more nuanced analysis of policing practices.

The study analyses the mediating role of technologies in contemporary policing. It does this by studying socio-technical arrangements in a variety of organizational settings. Instead of focusing considerations on one policing context, the chapters analyse the mediating role of technologies within multiple sites and policing situations. These span a diverse range of European police organizations – from local to national – concerned with multiple issues and crime phenomena – from youth delinquency to road policing – and adopting a broad range of policing styles – from community policing to intelligence-led policing and knowledge-based policing. The technologies include well known and widespread technologies such as geographic information systems as well as more recent projects where police organizations experiment with sensor networks, social media monitoring and other technologies and institutional innovations. The following three chapters of the book explore the ways in which various technologies mediate practices such as geospatial analysis of crime phenomena, mapping and monitoring risky or problematic persons, groups or areas and profiling suspicious behaviour.

Empirical data

Analysing a diverse set of practices within socio-technical systems helps to chart the networks of relations between police officers, technologies, organizational innovations and the legal frameworks in which they operate. In this way I was able to investigate not only the legal frameworks and procedures that specify how things should be done but also the ways in which police officers and agents work with technologies in their daily routines. Following officers, agents, constables and analysts and analysing the mediating role of technologies in these practices paints a richer picture of how practitioners perceive crime phenomena, how they act with and react to the output of technologies, and how decisions are taken in technologically mediated policing.

Chapter 4 draws on research at a local police station in Romania. It offers an analysis of practices associated to geographic information systems (GIS) as a widespread and well established technology in policing. The chapter demonstrates that rather than playing a mere instrumental role, technologies actively participate in mediating police perception of suspects. It does this by starting from a detailed analysis of an observation about the geo-positioning of a report about a suspect. The suspect report proved to be about a young Roma boy. The chapter shows how the report was insufficiently justified but still mediated the perception of practitioners about the boy. In these ways together, the classification ‘suspect’ accumulated in a set of implications for his presumption of innocence. As the practitioner’s attitudes tended to rely on the information system, suspects were rendered potentially vulnerable during encounters with the police. At the same time, the chapter shows how the system design was influenced by a combination of organizational reforms and software design choices. This detailed analysis of a basic routine renders suspicion as a complex socio-technical construct, even in the seemingly simplest and widespread technologically mediated practices.

Building on the insights of the previous insights, chapter 5 shows how technologies mediate police action. The chapter looks not only at the classification and geographic mapping of youth but also at more recent policing practices: proactive social media monitoring of youth groups. It draws on data in the Netherlands, where ‘problematic youth groups’ are under systematic

police surveillance as part of comprehensive proactive approaches. The chapter shows that larger data gathering from social media is entailed by the ways in which youth groups are enacted as 'cases' and performed as 'problematic' in government discourses and police statistics on the matter.

Chapter 6 makes a transition from asking questions about the role of technologies in influencing the practitioners' behaviour towards questions about the design of policing technologies. It asks how do technologies get their value charge and in-built norms? In particular, it investigates how 'the idea of privacy by design' was translated in configurations of sensor networks and employed in policing practices. The chapter draws from data in both The Netherlands and England, where automatic number plate recognition (ANPR) technology is widely employed in road policing practices.

The chapter contrasts phenomena related to the design choice of storing all traffic data (police in England) and of programming real-time profiles, informed by knowledge rules and combined with cryptographic techniques (Dutch police). This latter engagement with sensor networks (among which ANPR is seen in the police as one type of sensor) is regarded by the Dutch police as promising for both identifying suspect behaviour in big flows (of vehicles, ships, transactions, etc.) while being 'protective of privacy by design' for most of the other traffic participants.

From the empirical findings of the chapter we learn that, in practice, profiles need to adapt frequently to changes in criminal behaviour and consequently have a high number of false positives and false negatives. They become effective only after the police know what suspect behaviour they are looking for. Throughout participant observation sessions it became apparent that this way of working can deliver on its promises only when support is given to knowledge sharing between branches of the police (such that the police can select suspicious behaviour and protect the privacy of those that do not match the criteria of the profile). In the end, the chapter highlights that the profile design – with their criteria and knowledge production processes – becomes an important locus of ethical reflection concerning the engagement of sensor networks in police surveillance.

The analyses in these three chapters show various ways in which technologies mediate the police practitioners' perception, decisions and actions concerning criminal phenomena. Rather than forming only in their minds, 'a suspicious group', 'a dubious activity', 'a fishy behaviour' is also what the screens enact as such. Entities that play important roles in influencing police decision, behaviour and action are software-enabled artefacts such as profiles, classifications and algorithms. Their design mediates intensified surveillance and influences privacy revocation, discriminatory practices and other values and principles with ethical implications. Much more than a mere set of tools, the material dimension of policing works has a significant influence regarding who is seen as suspicious and how, when and where the police puts under surveillance.

Of course, distinguishing between innocents and criminals, normal and deviant, order and disorder are some of the main tasks of policing practitioners, with which we invest them to enable crime control and keeping our societies safe. Still, being invested with a monopoly on the use of power requires that practitioners and police organizations perform these entities – 'suspicious', 'abnormal', 'criminal' – in such a way that they protect the members of society from both crime and their own potentially erroneous, prejudiced and disproportionate interventions.

On the one hand, new information technologies often improve existing policing practices. Connected databases, digitized routines and pervasive screens bring about a more efficient decision making process as well as a more informed practitioner. On the other hand, we have seen that software-enabled representations, algorithmic profiles or system classifications can incorporate identity attributes and prejudiced views towards particular categories. When prejudice is embedded in code, logged in classifications and displayed on screens it matters less how well intended are the individual police agents. Solidifying in infrastructures, these software enabled artefacts become invisible and implicitly guide the policing of groups, categories, areas, persons or communities.

Synthesis

This thesis makes the argument that technologies in policing matter. The last chapter summarizes the findings and discusses a set of themes that cut across the empirical material. First, it discusses the role of technologies in processes of inferring suspicion. Drawing from the material of the previous chapters it shows a paradoxical *solidifying effect* induced by technologies in mediating suspicion and legitimizing surveillance. Despite the flexibility offered by code, software enabled entities related to 'suspicious behaviour' or 'problematic groups' contribute to solidify the practitioners' perception. Once a suspect in a proactive policy is 'in the system' it becomes much more prone to have this status maintained and strengthened. Even if police officers consciously know that they should not take the 'suspect' category as proof of crime, in practice many officers often tend to rely on what they see on the screens as adequate representations of reality. Relying on the corrections that can occur along the criminal justice chain, many policing practitioners, especially field agents, tend to take technologically mediated suspicion as incentives for alertness or surveillance. Understanding surveillance as a non-harmful action, relaxes the need for further justifications. In these conditions, the slightest suspicion becomes a sufficient condition for engaging in surveillance.

Of course, surveillance is one of the typical police actions. It often turns out to be justified as the entity placed under surveillance proves to be the actual culprit. Still, the chapters of this book show that suspicion remains prone to partiality and inadequacy, also when it is mediated by technologies. Rather than being adequate representations of reality – justifying surveillance or supporting prosecution in the criminal justice chain – technologically mediated suspicion appeared here quite questionable, partial and vague. Through their 'solidifying' effect, technologies can further foster unjustified surveillance and erroneous interventions. Entering *a cycle of suspicion-surveillance* increases incentives for intervention and makes it difficult for the enacted entities to invalidate the reasons for which they raised police interest. Whereas in reactive policing surveillance can work to invalidate the suspicion-surveillance cycle, in proactive approaches it tends to foster it.

Second, the chapter discusses how this 'solidification' effect impacted police relations with communities, groups and categories of citizens. It shows how the design of policing infrastructures can accumulate 'depositions of prejudice' in a sedimentary process. These 'sediments' that trickle down in technological infrastructures tend to harden and become simultaneously potent and invisible. In these ways together they contribute to eroding the trust between communities and the police when they carry hidden discriminatory potential.

In this sense, I propose to understand this phenomenon with an analogy from geology. Borrowing a notion from this discipline, we might call this a 'sedimentation' process that takes place in the context of design. In geology, the term sedimentation is used to describe the gradual deposition from a solution (e.g. water), which results in settling and accumulation into sedimentary rock (e.g. on the river bed). Particles that form a sedimentary rock by accumulation are called sediment. In the context of policing I want to suggest that technological infrastructures can entail a gradual disappearance from attention and scrutiny of classifications, categories, algorithmic steps, architectural decisions or identity attributes. Getting 'trapped' into infrastructures, prejudice can accumulate, harden and acquire a character of objectivity. At times, it rises to the surface, becoming potent and effective in mediating police action towards the enacted entities.

We have seen this phenomenon for instance in Chapter 4, in the situation of the community policing in Romania. In the local police system the representation of 'begging' was coded with black dots. The views of the police officer who happened to configure the system got built into the technological infrastructure and trickled down further in the practices of the other officers who worked with the system. Her views concerning the begging practices of Roma ethnics generalised in the technological infrastructure through the GIS representations. From then on, they accumulated and acquired new strength and spread. Not only was the GIS displaying one black dot on the screen but these automatically multiplied in every weekly map with 'the beggar distribution' throughout the city. As the other interviewed officer confirmed, the software-enabled maps evoked a cumulative effect. All begging was done by Roma ethnics. Irrespective of the statistics on the matter, the technological infrastructure induced a uniform perception of the phenomenon. At the same time, without the interview question, the interviewed officer was not aware of the origins and action of the software-enabled artefacts of the colour codes. In this way, 'the past' sediments in infrastructures and carries on prejudice into 'the future'.

Third, and finally, the chapter discusses more generally the relation between technology design and values with moral importance. Drawing from the findings of the previous three chapters, it highlights the multiple ways in which particular conceptions of values such as non-discrimination and privacy were implicitly and explicitly built in and influenced by technology designs. This part of the chapter argues that values in policing should not only be the realm of discourse and policy making but also of technology design. It argues for the need and opportunity for a larger uptake of Value Sensitive Design in developing but also managing technologies in policing. Engaging in a Value Sensitive Design approach in daily policing could nurture an environment that increases the chance for more transparent and ethically informed ways of developing profiles, classifications, algorithms or material arrangements. After all, policing in democratic societies needs to protect citizens from both criminal manifestations as well as unjustified surveillance and discriminatory actions. We need both privacy and integrity, safety and security, justice and non-discrimination.

Still, the chapter ends by qualifying this suggestion. Building of values in design is a promising undertaking but far from a silver-bullet solution to avoid all problems in policing. Technologies work in complex networks of organizations, laws, policies and criminal phenomena in constant change. If we want to promote an efficient and transparent police as well as to avoid problematic outcomes, we need to continuously analyse technologically-mediated policing practices in the socio-technical ensembles in which they feature.

Conclusion

A final reading of the book title proposes an investigative effort in the material dimension of policing. In this sense, we need to develop and engage in *a sedimentology of infrastructures* of which this book offers the first steps. Identifying, investigating and defusing potentially explosive 'pockets of prejudice' that may have formed in our infrastructures, opening up the criteria of suspicion algorithms or creating a more transparent surveillance are all measures towards increasing trust in policing among minority groups, communities and society at large.

Applying the insights of this discipline might help us to understand how sedimentary deposits form and change through time and space while a *lithology of technological environments* could describe their types and characteristics. A geological way of understanding infrastructures maintains the approach of 'digging up' strata that potentially encapsulate relevant deposits while simultaneously resisting a priori anthropocentric explanations. Unlike archaeology, which studies human activities in the past, *a sedimentology of infrastructures* might prove here an adequate metaphor to study a whole set of processes that may or may not be traceable to an initial human activity. Of course, design choices imply designers but the phenomena we have seen in this book require an understanding of infrastructures that allows for sedimentary processes and accumulations.

Bringing in notions from geology to understand technological infrastructures becomes even more relevant in a context in which many organizations engage in practices of data 'mining' – yet another metaphor closely related to the enterprise of understanding and exploring sediments. The vocabulary of many contemporary policing departments is pervaded with 'data mining' practices in which police analysts seek to 'extract' patterns of behaviour that may be 'hidden' within large 'piles' of data.

A geological metaphor to understand infrastructures may not only conjure up an image of solidified entities but also an image of *flows* of debris, processes of *erosion*, volcanic *explosions* and other dynamic processes. Haggerty and Ericson (2000, 611) also speak of the trails of information about a person's habits, preferences, and lifestyle as 'the *detritus* of contemporary life'. Unifying all these metaphors, shows even more the relevance of engaging in a sedimentology of technological infrastructures to identify potentially relevant sediments that may have formed within algorithmic steps, software layers or architectural features.

As documented in this book, the location of sediments of prejudice can range from 'close to the surface' – as in the case of recently finished algorithms or accessible program parameters – to the deep architectural decisions that tend to be forgotten, persist over the years and get taken for granted. On the one hand, being taken for granted is often manifest in programmers' habits of copy-pasting existing code to new versions that maintain algorithmic choices in its 'layers' of software code. On the other hand, when such 'sediments of prejudice' come to the fore they tend to induce a perception of objectivity towards the enacted group or community, often affecting their presumption of innocence, privacy, and other values with moral import.

Social relevance

This thesis makes the argument that technologies in policing matter. That is, more than mere tools, the material dimension of policing has a significant influence on who is regarded as suspicious and where, when and how the police engage in surveillance practices. Technologically-mediated environments, both in policing organizations as well as in our increasingly smarter cities, play an active role in informing, guiding, and defining policing strategies, tactics and practices. What is 'a suspicious group', 'a dubious activity', 'a fishy behaviour' is partly also what the screens enact as such.

The empirical findings of this research suggest an ambivalent result. On the one hand, new information technologies often improve existing policing practices. Connected databases, digitized routines and pervasive screens bring about a speedier decision-making process as well as a more informed practitioner. On the other hand, we have seen that algorithmic profiles or system classifications can incorporate identity attributes and prejudiced views towards particular groups or categories. When prejudice is embedded in code, logged in classifications and displayed on screens it matters less how well-intended are the individual police agents. Solidifying in infrastructures, these software enabled artefacts become invisible and implicitly guide the policing of groups, categories, areas, persons or communities.

Therefore, this book argues that values in policing should not only be the realm of discourse and policy making but also of technology design. Engaging in a Value Sensitive Design approach in policing nurtures an environment that increases the chance for more transparent and ethically informed ways of developing profiles, classifications, algorithms or material arrangements. After all, policing in democratic societies needs to protect citizens from criminal manifestations as well as from unjustified surveillance and discriminatory actions. Defusing potentially explosive 'pockets of prejudice' that may have formed in our infrastructures, opening up the criteria of suspicion algorithms or creating a more transparent surveillance are all steps towards decreasing unjustified harm to various categories of people and increasing trust in policing among minority groups, communities and society at large.

Target groups

A first major group that may benefit from these results are policing organizations. This may include the public, uniformed police, organized at local and state level but also transnational bodies working at European level. They are the primary beneficiaries of new information technologies and they are the ones who need to incorporate innovations in their procedures, routines and practices. Policing practitioners would benefit by becoming aware of the ways in which the technologies that they engage with are mediating their perceptions, decisions and actions, shaping their practices at operational, tactical and strategic levels.

A second group are educational institutions such as police academies, at both national and European levels. Understanding what technologies do besides their instrumental role could

create more awareness among the future policing practitioners. This awareness concerns the mediating role of technologies, minimizing the risk for voluntary and involuntary discriminatory actions and creating better conditions for a privacy protective attitude. Of course, the police education curriculum does already incorporate awareness-raising items concerning inadequate databases, privacy protection and non-discrimination. Still, the pervasiveness of contemporary information infrastructures and new phenomena such as big data, smart cities or the Internet of Things invite a comprehensive approach to understanding technology in police education.

A third group are the technology designers. These may include third party developers who deliver technology to police organizations and in-house police programmers who develop day-to-day profiles, suspicion indicators or algorithmic alerts. Becoming aware of the ways in which technology designs may incorporate pockets of prejudice or problematic classifications, could decrease the risk for the accumulation of informational harm and defuse potentially explosive situations. Moreover, engaging in a Value Sensitive Design approach would create the conditions for less arbitrary ethical reflection in a domain fraught with sensitive decisions.

A fourth group are privacy professionals. Whether privacy officers within police organizations or privacy advocates, the insights produced by this empirical research provide avenues for further investigation and a vocabulary to probe the layers of technological infrastructures. Besides being concerned with data protection or data privacy issues, this book argues that we need to constantly engage in a sedimentology of infrastructures where pockets of sediment might have encapsulated relevant deposits. Upon performing a lithology of software layers this group of professionals can reveal various problematic architectural features or design choices.

A fifth group are policy makers. We have seen that technologies do what they do within socio-technical assemblages where multiple (f)actors play an important but underdetermining role. Problematic outcomes cannot be always traced to design features, organizational structures, legal loopholes or practitioner's behaviour alone. Policy makers can benefit from a lithology of arrangements to enable precise policy changes at organizational, design or legal levels and their interrelation.

Activities/Products

A first item that results from this book is a new process. Target groups (as identified in the previous section) can borrow and expand the approach and vocabulary proposed in this book to continuously scrutinize the underlying lithology of socio-technical infrastructures and gather data and evidence on the nature and depositional conditions for sediments. A sedimentology of infrastructures can span both depth and spread to derive information on the types of sediments, their distribution and dynamics. This may mean periodically welcoming external code reviews, probing the output of suspicion profiles against dynamic changes in the environment and expanding the scope of probes when algorithms aggregate multiple smart sensors and databases. In these ways, target groups are in a better position to identify and defuse potentially problematic situations such as the ones we've seen in this book.

A second item is a process change in the context of design. Instead of allowing the formation of dangerous pockets of sediments in our infrastructures a Value Sensitive Design approach (as proposed in this book) enables a proactive approach that can foster a more transparent and

ethically informed process of design. A pragmatic take of the VSD methodology proposes values as heuristics while requiring a minimum set of values from the VSD researcher/designer. Pluralism and inclusivity are necessary to involve direct as well as indirect stakeholders and transparency would allow the possibility for critical analysis of design choices. Considering other values informs the design process, creating awareness of ethical implications and opening for reflection particular design choices that would otherwise remain implicit. At the same time, the VSD literature offers a growing body of examples that show how conflicting values can be reconciled in a positive sum, rather than a zero-sum approach. We have seen, for instance, in this book how Dutch police designers made efforts and took steps to reconcile privacy and security in their socio-technical arrangements without sacrificing one for the other.

A third item that results from this book is a product. This refers to a course that is being given by the author of this book (currently to students at Erasmus University Rotterdam). With small adaptations the course can be also given in policing educational contexts. As argued in this book, avoiding some of the problematic outcomes in technologically mediated policing requires a shift in thinking about technology in policing from determinist and instrumentalist views towards more constructivist and performative accounts. In the course, students study and critically reflect on policing practices and associated technologies which have become increasingly important in understanding both policing and our contemporary technological culture. The course begins with a module in *Surveillance studies*. It explores various metaphors and theories that shape our understanding of surveillance, ranging from well-known novels and films to concepts developed in contemporary surveillance studies. Students critically reflect on the adequacy of concepts and models for understanding various policing practices that involve information and communication technologies. Second, students examine several conceptualizations of their relations to information and communication technologies in a module on *Philosophy of Technology*. In this part of the course students explore and discuss themes such as technological determinism and individual agency, the inevitability thesis and constructivist approaches to technology, instrumentalism and technological mediation. Through examples and practical activities students apply these concepts and learn to identify the active mediation of various technologies. In a third module on *Values in Design*, students discuss the ways in which values such as privacy, non-discrimination, trust or autonomy can be both eroded and protected through technologically-mediated practices. The course ends by allowing students to present their own views, through a written paper, and come to grips with these processes in ways that reconcile multiple values with efficient policing.

Innovation

A first way in which the results of this book can be called innovative refers to the proposed understanding and assessing of technological infrastructures. The book argues that a geological vocabulary for understanding infrastructures is better prepared to account for a set of newly identified phenomena. Contrasting an archaeological vocabulary that tends to focus on human activity in the past and to equate social processes with (the remaining) human artefacts (e.g. Iron Age), a geological approach resists a priori anthropocentric explanations. While maintaining an approach that is predicated on investigations of layers and strata, it opens the understanding of infrastructures to a whole set of processes that may or may not be traceable to an initial human activity. Of course, design choices imply designers but the phenomena we have seen in this book require an understanding of infrastructures that allows for sedimentary processes, accumulations, erosions, digital debris and volcanic explosions.

A second way in which the argument of this book can be called innovative refers to the proposed application of a Value Sensitive Design approach to the design of policing technologies. On the one hand, VSD has not been traditionally employed in the area of policing, although there are a few projects that looked into taking a VSD approach to the design of military technologies (Cummings 2006). On the other hand, VSD can expand existing approaches that look into privacy by design. Rather than concentrating on privacy, a VSD approach can foster reflection on a broader set of values. For instance, we have seen how problematic discrimination on a range of identity criteria requires separate consideration in particular socio-technical arrangements and not merely be related to privacy issues.

A third way in which the results of this book can be called innovative refers to the combination of modules in the course mentioned in the Activities/Products section. First, the module on *Surveillance studies* offers students a conceptual background that moves their understanding of surveillance beyond the concepts developed in the police studies literature. It projects police surveillance against the background of a technological culture in which surveillance is practiced by a wide variety of public and private bodies, institutional and individual actors. Second, the module on *Philosophy of Technology* takes the theme of technology seriously. Rather than relegating information technologies to useful tools or technical instruments – as present in a significant body of the police studies literature – it proposes a study of their active role in shaping policing practices and policing models. Bringing in the latest insights from the philosophy of technology, the module invites students to think about the mediating role of ubiquitous information infrastructures and how does this relate to policing models such as community policing or intelligence-led policing. Third, the module on *Values in Design* invites students to think about the design of policing technologies as an ethical process. In a working environment in which police decision-making is partly influenced by the output of risk profiles and algorithms, it is increasingly necessary to reflect on the ways in which these design choices are informed by the explicit and implicit values of their designers.

Schedule & Implementation

Regarding a potential course given to police academy students, the risks involved seem to be rather low. The author of this book is already experienced in teaching a similar course with good evaluations from students. The opportunity to give it in a policing context requires an adaption of focus but the main concepts, approaches and modules derived from this book remain valid. In terms of a schedule, such a course can begin immediately provided openness from educational institutions in policing.

Regarding a VSD approach in policing, the risks seem to be higher. They pertain to the openness of policing organizations to account for values in design and to open the criteria of risk profiles and suspicion algorithms to a more transparent process of design. The empirical research presented in this book demonstrates that such openness is possible but more transparency needs to come from policing organizations themselves. On top of this, implementing such a design process requires a basic but more spread familiarity in policing with the insights of philosophy of technology and science and technology studies. These, of course, can be given through the above mentioned course, either in an educational context or in police organizations themselves. Still, the planning for the valorisation of these results suggests here a sequential process.

About the author

Vlad Niculescu-Dincă (1978) is currently a lecturer at the Erasmus University Rotterdam, The Netherlands. Before this he has been working in Maastricht for his PhD research, culminating in the book you are currently reading. Vlad holds a master degree in Philosophy of Science, Technology and Society (2009) from the University of Twente. During that period he investigated the structure of ethical debates around new and emerging technologies for improving human performance. Besides qualitative approaches to surveillance and suspicion, Vlad's research interests surround social and ethical aspects of the design and use of new information technologies. He draws from the intellectual background of Science and Technology Studies and Philosophy of Technology that he constantly relates to his technical background. He holds degrees in Software Engineering from the Technical Universities of Eindhoven (PDeng.) and Bucharest (B.Sc.). Vlad lives in Eindhoven together with his wife, Mateia and their three girls.

List of figures

References

Aarts, Emile, and Stefano Marzano. 2003. *The New Everyday: Visions of Ambient Intelligence*: 010 Publishers.

Akrich, Madeleine. 1992. "The de-scription of technical objects." In *Shaping Technology/ Building society: Studies in Sociotechnical Change*, edited by Wiebe Bijker and John Law, 205-224. Cambridge, MA: MIT Press.

Akrich, Madeleine, and Bruno Latour. 1992. "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies." In *Shaping Technology/ Building society: Studies in Sociotechnical Change*, edited by Wiebe Bijker and John Law, 259-264. Cambridge, MA: MIT Press.

Albrecht, Jan Philipp. 2012. Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) edited by Justice and Home Affairs Committee on Civil Liberties: European Parliament.

Alderson, John. 1977. *Communal Policing*. Exeter: Devon and Cornwall Constabulary.

Amnesty International. 2014. Amnesty International report 2014/15. The state of the world's human rights. Peter Benenson House, London, United Kingdom: Amnesty International.

Andrejevic, Mark. 2004. *Reality TV: The Work of Watching, Critical Media Studies: Institutions, Politics, and Culture*. Lanham MD: Rowman & Littlefield Publishers.

Azenkot, Shiri, Sanjana Prasain, Alan Borning, Emily Fortuna, Richard E. Ladner, and Jacob Wobbrock. 2011. "Enhancing independence and safety for blind and deaf-blind public transit riders." In *Proceedings of CHI 2011*, 3247-3256. New York: ACM Press.

Bakker, Hette. 2006. "Politie in Stromenland: Over nodes en netwerken." *Het tijdschrift voor de politie* no. 10:19-23.

Barr, Robert, and Ken Pease. 1990. "Crime Placement, Displacement, and Deflection." In *Crime and Justice: A Review of Research*, edited by Michael Tonry and Norval Morri, 277. Chicago: University of Chicago Press.

Bigo, Didier. 2006. "Security, exception, ban and surveillance." In *Theorizing surveillance: The panopticon and beyond*, edited by David Lyon, 46-68. Cullompton: Willan Publishing.

Bijker, Wiebe. 1992. "The Social Construction of Fluorescent Lighting, or How an Artifact was Invented in its Diffusion Stage." In *Shaping Technology / Building Society:*

Studies in Sociotechnical Change, edited by Wiebe Bijker and John Law, 75-104. Cambridge, MA: MIT Press.

Bijker, Wiebe. 1995. *Bikes, Bakelite, and Bulbs: Steps Toward a Theory of Socio-Technical Change*. Cambridge: MIT Press.

Bijker, Wiebe. 2010. "How is technology made?—That is the question!" *Cambridge Journal of Economics* no. 34:63-76.

Bogard, William. 1996. *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge: Cambridge University Press.

Borning, Alan, Batya Friedman, and Peter Kahn. 2004. Designing for human values in an urban simulation system: Value sensitive design and participatory design. In *Short Papers, Eighth Biennial Participatory Design Conference*. Palo Alto, CA: Computer Professionals for Social Responsibility.

Borning, Alan, and Michael Muller. 2012. "Next steps for Value Sensitive Design." *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems. ACM*:1125-1134.

Borst, Wim L. 2013. "Privacy by design on the crossroads of chains, Lessons from the chain of criminal justice in the Netherlands." *Journal of Chain-computerisation, Information Exchange for Chain Co-operation* no. 4 (5):1-10.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out Classification and Its Consequences*. Cambridge, MA: MIT Press

Boyne, Roy. 2000. "Post-Panopticism." *Economy and Society* no. 29 (2):285–307.

Brey, Philip. 1998. "Artifacts as Social Agents." In *Inside the Politics of Technology. Agency and Normativity in the CoProduction of Technology and Society*, edited by Hans Harbers, 61-84. Amsterdam: Amsterdam University Press.

Brodeur, Jean-Paul, and Benoit Dupont. 2006. "Knowledge workers or "knowledge" workers?" *Policing and Society* no. 16 (1):7-26.

Brodeur, Jean-Paul, and Benoit Dupont. 2008. "Introductory Essay: The Role of Knowledge and Networks in Policing." In *The Handbook of Knowledge-based policing. Current Conceptions and Future Directions*, edited by Tom Williamson, 9-33. West Sussex, England: John Wiley & Sons.

Bruggeman, Willy. 2011. "The boundaries and the future of technological control: technological control has its limits on ethical grounds, but also from a social control point of view." In *Technology-led policing*, edited by Evelien De Pauw, Paul Ponsaers, K. Van der Vijver, Willy Bruggeman and Piet Deelman, 127-164. Antwerpen | Apeldoorn | Portland: Cahiers Politiestudies.

Bureau Beke. 2009. *Shortlist methodology in seven steps*. Arnhem: Bureau Beke.

Bureau Beke. 2010. Approach to problematic youth groups, guidlines for municipalities. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Bureau Beke. 2013. Problematic youth groups in Netherlands, extent and nature in autumn 2012. Arnhem: Ministry of Security and Justice.

Bureau Beke. 2014. Problematic youth groups in Netherlands, extent and nature in autumn 2014. Arnhem: Ministry of Security and Justice.

Button, Mark. 2002. *Private policing*. Cullompton: Willan Publishing.

Byrne, James, and Gary T. Marx. 2011. "Technological innovations in crime prevention and policing. A review of the research on implementation and impact." In *Technology-led policing*, edited by Evelien De Pauw, Paul Ponsaers, K. Van der Vijver, Willy Bruggeman and Piet Deelman, 17-40. Antwerpen | Apeldoorn | Portland: Maklu.

Callon, Michel. 1986. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay." In *Power, Action and Belief*, edited by John Law, 196–233. London: Routledge & Kegan Paul.

Callon, Michel. 1987. "Society in the making: The study of technology as a tool for sociological analysis." In *The social construction of technological systems*, edited by W. E. Bijker, T. P. Hughes and T. J. Pinch, 83-103. Cambridge, MA: MIT Press.

Callon, Michel. 1991. "Techno-economic networks and irreversibility." In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 132-164. London: Routledge.

Cambridge News. *Switching off Royston's 'Ring of Steel' of ANPR cameras has had 'no impact' on crime figures* July 31st 2014. Available from http://www.cambridge-news.co.uk/Switching-RoystonsRing-Steel-ANPR-cameras-hadno-impact-crime-figures/story-22369244-detail/story.html.

Castells, Manuel. 1996. *The rise of the network society: volume i: the information age: economy, society, and culture*. Oxford UK: Wiley-Blackwell.

Cavoukian, Ann. 2009. Privacy by Design - The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.

Chainey, Spencer, and Jerry H. Ratcliffe. 2005. *GIS and crime mapping*. Edited by Chainey and Ratcliffe. Chichester: John Wiley & sons ltd.

Chan, Janet B. L. 1997. *Changing police culture: Policing in a multicultural society*. Cambridge, UK: Cambridge University Press.

Chan, Janet B.L. 2001. "The technology game: how information technology is transforming police practice." *Journal of criminal justice* no. 1 (2):139-159.

Chatwin, Caroline. 2003. "Drug policy developments within the European Union: the destabilizing effects of Dutch and Swedish drug policies." *British journal of Criminology* no. 43 (3):567-582.

Chu, Jim. 2001. *Law Enforcement Information Technoogy: a managerial, operational and practical guide*. Boca Raton | London | New York | Washington D.C.: CRC Press.

Clarke, Ronald V., and David Weisburd. 1994. "Diffusion of Crime Control Benefits: Observations on the Reverse of Displacement." *Crime Prevention Studies* no. 3 (2):165-183.

Cohen, Irwin M., Darryl Plecas, and Amanda V. McCormick. 2012. A Report on the Utility of the Automated Licence Plate Recognition System in British Columbia. School of criminology and criminal justice University College of the Fraser Valley.

Cole, Simon. 2001. *Suspect identities. A history of fingerprinting and criminal identification*. Cambridge, Massachusetts, London, England: Harvard University Press.

Collingridge, David. 1980. *The social control of technology*. New York: St. Martin's Press.

Cope, Nina. 2008. "'Interpretation for action?': definitions and potential of crime analysis for policing." In *Handbook of policing*, edited by Tim Newburn, 404-429. Cullompton: Willan Publishing.

Council of Europe. 1950. European Convention of Human Rights as amended by Protocols No. 11 and 14 supplemented by Protocols No. 1, 4, 6, 7, 12 and 13. edited by European Court of Human Rights. Council of Europe. F-67075 Strasbourg cedex.

CSAT, Supreme Council for National Defence. 2007. National Security Strategy of Romania. Bucharest: Supreme Council for National Defence.

CSAT, Supreme Council for National Defence. 2010. National Security Strategy of Romania. Bucharest: Supreme Council for National Defence.

Cummings, Mary L. 2006. "Integrating ethics in design through the value sensitive design approach." *Science and Engineering Ethics* no. 12 (4):701-715.

Davis, Janet, and Lisa Nathan. 2015. "Value Sensitive Design: Applications, Adaptations, and Critiques." In *Handbook of Ethics, Values, and Technological Design*, edited by Jeroen van den Hoven, Pieter E. Vermaas and Ibo van de Poel, 11-40. Springer Netherlands.

Dechesne, Francien, Martijn Warnier, and Jeroen Van den Hoven. 2013. "Ethical requirements for reconfigurable sensor technology: a challenge for value sensitive design." *Ethics Information Technology* no. 15 (3):173–181.

Deleuze, Gilles. 1992. "Postscript on the Societies of Control." *October* no. 59 (Winter):3-7.

Den Boer, Monica. 2011. "Technology-led policing in the European Union: An asessment." In *Technology-led policing*, edited by Evelien De Pauw, Paul Ponsaers, K. Van der

Vijver, Willy Bruggeman and Piet Deelman, 39-57. Antwerpen | Apeldoorn | Portland: Cahiers Politiestudies.

Dubbeld, Lynsey. 2004. *The regulation of the observing gaze: privacy implications of camera surveillance*. Enschede: PrintPartners IpsKamp.

Eck, John, and Edward Maguire. 2000. "Have changes in policing reduced violent crime? An asessment of the evidence." In *The crime drop in America*, edited by A. Blumstein and J. Wallman, 207-265. Cambridge: Cambridge University Press.

Eck, John, and David Weisburd. 1995. *Crime and place*. Edited by Ronald V. Clarke. Vol. 4, *Crime Prevention Studies*. Monsey, NY: Willow Tree Press.

Ellul, Jacques. 1964. *The technological society*. Translated by John Wilkinson. New York: Vintage books.

Emsley, Clive. 2008. "The birth and development of the police." In *Handbook of Policing*, edited by Tim Newburn, 72-89. Cullompton, Devon: Willan Publishing.

Ericson, Richard, and Kevin D. Haggerty. 1997. *Policing the Risk Society* University of Toronto Press.

European Commission. 2009a. C(2009) 3200 - Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Official Journal of the European Union. Brussels.

European Commission. 2009b. COM(2009) 278 - Internet of Things — An action plan for Europe. Brussels.

European Commission. 2010a. COM 609 - A comprehensive approach on personal data protection in the European Union. Brussels.

European Commission. 2010b. COM 673 - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels.

Feenberg, Andrew. 2002. *Transforming technology: a Critical theory revised*. Oxford | New York: Oxford University Press.

Feinberg, Joel. 1984. *The Moral Limits of the Criminal Law Volume 1: Harm to Others*. New York: Oxford University Press.

Flaherty, David. 1997. "Controlling Surveillance: Can Privacy Protection Be Made Effective?" In *Technology and Privacy: The New Landscape*, edited by Philip E. Agre and Marc Rotenberg, 167-192. Cambridge, MA: MIT Press.

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

Foucault, Michel. 1977. *Discipline and Punish: The birth of the prison*. New York: Vintage Books.

Friedman, Batya, and Nathan G. Freier. 2005. "Value Sensitive Design." In *Theories of information behavior: A researcher's guide*, edited by Karen E. Fisher, Sanda Erdelez and Lynne E. F. McKechnie, 368-372. Medford, NJ: Information Today.

Friedman, Batya, Peter H. Kahn, and Alan Borning. 2002. Value Sensitive Design: Theory and Methods. In *Technical Report 02-12-01*: Dept. Of Computer Science & Engineering. University of Washington.

Friedman, Batya, Peter H. Kahn, and Alan Borning. 2006. "Value Sensitive Design and information systems." In *Human-computer interaction in management information systems: Foundations*, edited by P. Zhang and D. Galletta, 348-372. New York: M.E. Sharpe.

Friedman, Batya, Peter H. Kahn, Jennifer Hagman, Rachel Severson, and Brian Gill. 2006. "The watcher and the watched: Social judgments about privacy in a public place." *Human-Computer Interaction* no. 21:235-272.

Friedman, Batya, Ian Smith, Peter H. Kahn, Sunny Consolvo, and Jaina Selawski. 2006. Development of a privacy addendum for open source licenses: Value Sensitive Design in industry. Paper read at Ubicomp 2006, at Berlin, Heidelberg, New York.

Fulda, Joseph S. 2000. "Data Mining and Privacy." *Albany Law Journal of Science and Technology* no. 11:105-113.

Galindo, David, and Jaap-Henk Hoepman. 2011. "Non-interactive Distributed Encryption: A New Primitive for Revocable Privacy." In *Workshop on Privacy in the Electronic Society (WPES)*, 81-92. Chicago, IL, USA.

Gerson, Elihu, and Susan Leigh Star. 1986. "Analyzing due process in the workplace." *ACM Transactions on Information Systems (TOIS)* no. 4 (3, Special issue: selected papers from the conference on office information systems).

Gordon, D. 1990. "The Electronic Panopticon." In *The Justice Juggernaut: Fighting Street Crime, Controlling Citizens* 438–51. New Brunswick, NJ: Rutgers University Press.

Graeff, Christine, and Michael C. Loui. 2008. "Ethical Implications of Technical Limitations in Geographic Information Systems." *IEEE Technology and Society Magazine* no. 27 (4):27-36. doi: 10.1109/MTS.2008.930566.

Green, Stephen. 1999. "A plague on the panopticon, Surveillanc and power in the global informationeconomy." *Information, Communication & Society* no. 2 (1):26-44.

Grint, Keith, and Steve Woolgar. 1997. *The machine at work: Technology, Work and Organization*. Cambridge: Polity Press.

Gromme, Francisca. 2012. "Surveillance in the supermarket: Technology and the pluralization of crime control." In *Crime, Security and Surveillance. Effects for the surveillant and the surveilled*, edited by Vande Walle Gudrun, Van den Herrewegen Evelien and Nils Zurawski, 33-53. The Hague: Eleven international publishing.

Gromme, Francisca. 2016. "Data mining 'Problem Youth': Looking closer but not seeing better." In *Digitizing Identities. Doing Identity in a Networked World*, edited by Van der Ploeg Irma and Jason Pridmore, 163- 183. New York: Routledge.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future Generation Computer Systems* no. 29 (7):1645-1660.

Gürses, Seda, Carmela Troncoso, and Claudia Diaz. 2011. Engineering Privacy by Design. In *Computers, Privacy & Data Protection (CPDP)*. Brussels.

Gutwirth, Serge. 2002. *Privacy and the Information Age*. Boston: Rowman& Littlefield.

Haberfeld, Maria, Piotr Walancik, and Aaron Uydess. 2002. "Teamwork - not making the dream work. Community policing in Poland." *Policing: An international journal of police strategies and management* no. 25 (1):147-168.

Haggerty, Kevin D. 2006. "Tear down the walls: on demolishing the panopticon." In *Theorizing Surveillance*, edited by David Lyon, 23-45. Cullompton, Devon: Willan Publishing.

Haggerty, Kevin D., and Richard Ericson. 2000. "The surveillant assemblage." *British Journal of Sociology* no. 51 (4):17.

Hakim, Simon, and George Rengert. 1981. *Crime Spillover*. Beverly Hills: Sage.

Harris, Christopher J. 2007. "Police and soft technology: how information technology contributes to police decision making." In *The new technology of crime, law and social control*, edited by J. Byrne and D. Rebovich, 153-183. Monsey, NY: Criminal Justice Press.

Hellemons, Ad, Peter van de Beek, Jan Malenstein, André aan ‘t Goor, Cor Kuijten, and Willem Schewe. 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, Kären M., and Christine Hess Orthmann. 2010. *Criminal Investigation*. 9th ed. Canada: Delmar Cenage Learning.

Hildebrandt, Mireille. 2011. "Legal protection by design: objections and refutations." *Legisprudence* no. 2 (5):223-248.

Hildebrandt, Mireille, and Serge Gurtwith. 2008. *Profiling the European Citizen*. Berlin: Springer.

Hildebrandt, Mireille, and Bert-Jaap Koops. 2010. "The Challenges of Ambient Law and Legal Protection in the Profiling Era." *Modern Law Review* no. 73:428-460.

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

Ihde, Don. 1990. *Technology and the lifeworld*. Bloomington: Indiana University Press.

Innes, Martin, and Colin Roberts. 2008. "Reassurance policing, community intelligence and the co-production of neighbourhood order." In *Handbook of Knowledge Based Policing*, edited by Tom Williamson, 241-262. West Sussex, England: John Wiley & Sons.

International Telecommunications Union. 2005. The Internet of Things. In *ITU Internet Reports*. Geneva: International Telecommunications Union.

IPCC. 2013. Report on Metropolitan Police Service handling of complaints alleging race discrimination. Independent police complaints comission.

Jenkins, David, and Lisa A. McCauley. 2006. "GIS, SINKS, FILL, and disappearing wetlands: unintended consequences in algorithm development and use." In *Proceedings of the Twenty-First Annual ACM Symposium on Applied Computing*, 277–282. New York: Association for Computing Machinery.

Joerges, Bernward. 1999. "Do Politics Have Artefacts?" *Social Studies of Science* no. 29 (3):411-431.

Johnson, Deborah G., and Jameson M. Wetmore. 2008. "STS and Ethics: Implications for engineering ethics." In *The Handbook of Science and Technology Studies*, edited by Edward J. Hackett, Olga Amsterdamska, Michael Lynch and Judy Wajcman, 567-582. Cambridge, London: The MIT Press.

Jones, Matthew, and Michael Rowe. 2015. "Sixteen Years On: Examining the Role of Diversity Within Contemporary Policing." *Policing* no. 9 (1):2-4.

Jones, Trevor, and Tim Newburn. 2002. "The transformation of policing." *British journal of Criminology* no. 42 (1):129-146.

Jones, Trevor, and Tim Newburn. 2006. *Plural policing, a comparative perspective*. London and New york: Routledge.

Kahn, Peter H., Batya Friedman, Brian Gill, Jennifer Hagman, Rachel L. Severson, Nathan G. Freier, Erika N. Feldman, Sybil Carrere, and Anna Stolyar. 2008. "A plasma display window?—The shifting baseline problem in a technologically mediated natural world." *Journal of Environmental Psychology 28 (2008)* no. 28:192–199.

Kamiran, F., A. Karim, S. Verwer, and H. Goudriaan. 2012. Classifying Socially Sensitive Data Without Discrimination: An Analysis of a Crime Suspect Dataset. Paper read at Data Mining Workshops (ICDMW), IEEE 12th International Conference, 10-10 Dec. 2012, at Brussels.

Kammerer, Dietmar. 2012. "Surveillance in literature, film and television." In *The Routledge International Handbook of surveillance studies*, edited by David Lyon, Kirstie Ball and Kevin D. Haggerty, 99-106. London, New York: Routledge.

Kitchin, Rob. 2014. "The real-time city? Big data and smart urbanism." *GeoJournal* no. 79 (1):1-14.

Kitchin, Rob, Tracey P. Lauriault, and Gavin McArdle. 2015. "Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards." *Regional Studies, Regional Science* no. 2 (1):6-28.

Koops, Bert-Jaap, Jaap-Henk Hoepman, and Ronald Leenes. 2013. "Open-source intelligence and privacy by design." *Computer law & security review* no. 29:676 - 688.

Koops, Bert-Jaap, and Ronald Leenes. 2005. "'Code' and The Slow Erosion of Privacy." *Michigan Telecommunications & Technology Law Review* no. 12 (12):115-188.

Koops, Bert-Jaap, and Ronald Leenes. 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* no. 28 (2):159-171.

Koskela, Hille. 2003. "''Cam Era" – The Contemporary Urban Panopticon'." *Surveillance and Society* no. 1 (2):292–313.

Kroener, Inga, and David Wright. 2014. "A Strategy for Operationalizing Privacy by Design." *The Information Society: An International Journal* no. 30 (5):355-365.

Latour, Bruno. 1987. *Science in Action*. Cambridge: Harvard University Press.

Latour, Bruno. 1988. "Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer." *Social Problems* no. 35 (3 Special Issue: The Sociology of Science and Technology):298-310.

Latour, Bruno. 1991. "Technology is Society made Durable." In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 103-131. London: Routledge.

Latour, Bruno. 1994. "On technological mediation: Philosophy, Sociology, Genealogy." *Common knowledge.*

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

Latour, Bruno, and Emilie Hermant. *Paris: Invisible City* 2006. Available from http://www.bruno-latour.fr/livres/viii_paris-city-gb.pdf.

Law, John. 1987. "Technology and Heterogeneous Engineering: The Case of Portuguese Expansion." In *The Social Construction of Technological Systems*, edited by Wiebe E. Bijker, Thomas P. Hughes and Trevor Pinch, 111–134. Cambridge MA: MIT Press.

Law, John. 2008. "Actor-network theory and material semiotics." In *The New Blackwell Companion to Social Theory, 3rd Edition*, edited by Bryan S. Turner, 141–158. Oxford: Blackwell.

Law, John. 2009. "Seing like a survey." *Cultural Sociology* no. 3 (2):239-256.

Law, John, and Annemarie Mol. 2001. "Situating technoscience: an inquiry into spatialities." *Environment and Planning D: Society and Space* no. 19 (5):609-621.

Leipnik, Mark R., and Donald P. Albert. 2003. *GIS and law enforcement: Implementation issues and case studies*. London: Taylor & Francis.

Leman-Langlois, Stéphane. 2012. *Technocrime, Policing, and Surveillance*. Vol. 3: Routledge.

Lemieux, Frederic, and Brian Bales. 2013. "Investigating transnational cybercrime: current challenges and emerging initiatives." In *Technocrime, policing and surveillance*, edited by Stephane Leman-Langlois, 65-78. Oxon: Routledge.

Los, Maria. 2006. "Looking into the future: surveillance, globalization and the totalitarian potential." In *Theorizing surveillance: The panopticon and beyond*, edited by David Lyon, 69-94. Cullompton: Willan Publishing.

Lyon, David. 2003. *Surveillance as Social Sorting, Privacy, risk and digital discrimination*. NY: Routledge.

Lyon, David. 2006a. "The search for surveillance theories." In *Theorizing surveillance: The panopticon and beyond*, edited by David Lyon, 3-20. Cullompton: Willan Publishing.

Lyon, David. 2006b. *Theorizing Surveillance*. Cullompton, Devon: Willan Publishing.

Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique." *Big Data & Society* no. 1 (1):1–13.

MacKenzie, Donald, and Judy Wajcman. 1985. *The Social Shaping of Technology: How the Refrigerator got its hum*. Milton Keynes, Philadelphia: Open University Press.

Maguire, Mike. 2000. "Policing by risks and targets: Some dimensions and implications of intelligence-led crime control." *Policing and Society* no. 9 (4):315-336.

Mancuhan, Koray, and Chris Clifton. 2014. "Combating discrimination using Bayesian networks." *Artificial Intelligence and Law* no. 22 (2):211-238. doi: 10.1007/s10506-014-9156-4.

Manders-Huits, Noëmi. 2011. "Regulating Invisible Harms." In *Innovating Government*, edited by S van der Hof and M. M. Groothuis, 57-73. Information Technology and Law Series.

Mannermaa, Mika. 2007. "Living in the European Ubiquitous Society." *Journal of Future Studies* no. 11 (4):105-120.

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

Martin, Aaron, Rosamunde Van Brakel, and Daniel Bernhard. 2009. "Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework." *Surveillance & Society* no. 6 (3):213-232.

Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.

Marx, Gary T. 2009. "A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-neutralization Dynamics." *Surveillance and Society* no. 6 (3):294-306.

Marx, Gary T., and N. Reichman. 1984. "Routinizing the discovery of secrets: computers as informants." *American Behavioral Scientist* no. 27 (4):423-452.

Mawby, Rob. 1999. "The changing face of policing in central and eastern Europe." *International journal of police science and management* no. 2 (3):199-216.

Mawby, Rob I. 2008. "Models of policing." In *The Handbook of policing*, edited by Tim Newburn, 17-46. Cullompton: Willan Publishing.

McLennan, David, and Adam Whitworth. 2008. Displacement of Crime or Diffusion of Benefit: Evidence from the New Deal for Communities Programme. London: Report by the Social Disadvantage Research Centre, University of Oxford.

Mol, Annemarie. 2010. "Actor-Netwrok Theory: Sensitive terms and enduring tensions." *Kölner Zeitschrift für Soziologie und Sozialpsychologie* no. 50 (1):253-269.

Moore, Mark H. 2003. "Sizing up Compstat: an important administrative innovation in policing." *Criminology and public policy* no. 2 (3):469-494.

Moraes, Claude. 2013. Draft report on the US-NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. edited by European Parliament's Committee on Civil Liberties Justice and Home Affairs: European Parliament.

Newburn, Tim. 2001. "The commodification of policing: security networks in the late modern city." *Urban studies* no. 38 (5-6):829-848.

Newburn, Tim. 2008a. *The Handbook of policing*. Cullompton, UK: Willan Publishing.

Newburn, Tim. 2008b. "Policing since 1945." In *Handbook of policing*, edited by Tim Newburn, 90-114. Cullompton, Devon: Willan publishing.

Nichols, Gary. 1999. *Sedimentology & Stratigraphy*. Malden, MA: Wiley-Blackwell.

Niculescu-Dinca, Vlad, Irma Van der Ploeg, and Tsjalling Swierstra. 2016. "Sorting (out) youth. Transformations in police practices of classification and social media monitoring." In *Digitizing Identities. Doing Identity in a Networked World*, edited by Irma Van der Ploeg and Jason Pridmore, 184-205. Abingdon, UK: Routledge.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*: Stanford University Press.

Norris, Clive, and Gary Armstrong. 1999. *The Maximum Surveillance Society*: Oxford, Berg Publishers.

Norris, Clive, Xavier L'Hoiry, Antonella Galetta, Paul De Hert, Ivan Szekely, and Charles Raab. 2015. Policy brief. Recommendations to the Council of the EU and the European Parliament on access rights, in the context of the European data protection reform. Brussels: IRISS project.

Orlikowski, Wanda. 2002. "Knowing in practice: enacting a collective capability in distributed organizing." *Organization science* no. 13 (3):249-273.

Orwell, George. 1949. *Nineteen Eighty-Four*. New York: Penguin.

Oudshoorn, Nelly, and Trevor Pinch. 2003. *How Users Matter, The Co-construction of Users and Technology*. Massachusetts: MIT Press.

Pakes, Francis. 2010. *Comparative criminal justice*. Cullompton, Devon: Willan Publishing.

Papanicolaou, Georgios. 2011. *Transnational policing and sex trafficking in southeastern Europe*. Hampshire: Palgrave Macmillan.

Parker J.R., and Pavol Federl. 1996. "An Approach To Licence Plate Recognition." *Computer Science Technical reports, University of Calgary, Alberta Canada* no. 591 (11).

Pinch, Trevor, and Wiebe Bijker. 1987. *The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other*. Edited by Wiebe Bijker, Trevor Pinch and Thomas P. Hughes: MIT Press.

Podesta, John, Penny Pritzker, and Ernest J. Moniz. 2014. Big data: Seizing opportunities, preserving values. edited by Executive Office of the President. Washington: The White house.

Police.uk. *Crime and policing in England, Wales and Northern Ireland*. Home office 2014 [cited April 12, 2014. Available from https://www.police.uk/information-and-advice/automatic-number-plate-recognition/.

Punch, Maurice, Bob Hoogenboom, and Kees Van der Vijver. 2008. "Community policing in the Netherlands: Four generations of redefinition." In *The Handbook of knowledge-based policing*, edited by Tom Williamson, 59-78. Chichester: John Wiley& Sons, Ltd.

Radder, Hans. 2009. "Why technologies are inherently normative." In *Philosophy of Technology and Engineering Sciences*, edited by A.W.M. Meijers, 887-921. Amsterdam: Elsevier.

Ratcliffe, Jerry H. 2008. *Intelligence-Led Policing*. Cullompton: Willan Publishing.

Rawlings, Philip. 1995. "The idea of policing: a history." *Policing and Society* no. 5 (2):129-149.

Reiner, Robert. 1994. "Policing and the Police." In *The Oxford Handbook of Criminology*, edited by Mike Maguire, Rod Morgan and Robert Reiner, 705-72. Oxford: Clarendon Press.

Rosenberger, Robert, and Peter-Paul Verbeek. 2015. *Postphenomenological Investigations: Essays on Human–Technology Relations, Postphenomenology and the Philosophy of Technology*: Lexington Books.

Sanders, Carrie. 2006. "Have you been identified? Hidden boundary work in emergency services classifications." *Information, Communication & Society* no. 9 (6):714-736.

Scarman, Lord. 1982. *The Scarman report: The Brixton disorders, 10-12 April 1981*. Harmondsworth: Penguin Books.

Schakel, Jan-Kees, Rutger Rienks, and Reinier Ruissen. 2013. "Knowledge-Based Policing: Augmenting Reality with Respect for Privacy Discrimination and Privacy in the Information Society." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky, 171-189. Heidelberg, New York, Dordrecht, London: Springer

Sclove, Richard. 1995. *Democracy and Technology*. New York: Guilford Press.

Șerb, Stancu. 2006. *Manual de tactică polițienească (Police tactics manual)*: Editura MAI (The Publishing house of the Romanian Ministry of Administration and Internal affairs).

Shaw, Clifford R., and Henry D. McKay. 1931. Social factors in juvenile delinquency. In *Report on the causes of crime, national commission of law enforcement and observance*. Washington, DC: Government Printing Office.

Shearing, Clifford D. 1996. "Public and private policing." In *Themes in contemporary policing*, edited by William Saulsbury, Joy Mott and Tim Newburn. London, UK: Police Foundation with Policy Studies Institute, London, UK.

Shearing, Clifford D. 2005. "Nodal security." *Police quarterly* no. 8 (1):57-63.

Sheptycki, James. 2005. "Transnational policing." *Canadian review of policing research* no. 1:1-7.

Sherman, Lawrence W. 1995. "Hotspots of crime and criminal careers of places." In *Crime and place. Crime prevention studies*, edited by John E. Eck and David Weisburd, 35-52. Monsey, NY: Criminal Justice Press.

Simon, Bart. 2005. "The Return of Panopticism: Supervision, Subjection and the New Surveillance." *Surveillance & Society* no. 3 (1):1-20.

Skogan, Wesley. 2008. "An overview of Community Policing: origins, concepts and implementation." In *Handbook of Knowledge based policing*, edited by Tom Williamson, 43-57. West Sussex, England: Johh Wiley & so.

Skogan, Wesley, and Susan Hartnett. 1997. *Community policing. Chicago style*. New York Oxford: Oxford University Press.

Solove, Daniel, Marc Rotenberg, and Paul M. Schwartz. 2005. *Privacy, Information and Technology*. New York: Aspen Publishers

Star, Susan Leigh. 1991. "Power, Technologies and the Phenomenology of Conventions: On Being Allergic to Onions." In *A Sociology of Monsters. Essays on Power, Technology and Domination*, edited by John Law, 26-56. London: Routledge.

Steeves, Valerie. 2012. "Hide and Seek: Surveillance of Young People on the Internet." In *The International Handbook of Surveillance Studies*, edited by David Lyon, Kevin Haggerty and Kirstie Ball, 352-359. London, New York: Routledge.

Swierstra, Tsjalling, and Jaap Jelsma. 2006. "Responsibility without Moralism in Technoscientific Design Practice." *Science, Technology & Human Values* no. 31 (3):309-332.

Tilley, Nick. 2008. "Modern approaches to policing: community, problem-oriented and intelligence-led." In *Handbook of Policing*, edited by Tim Newburn, 373-403. Cullompton: Willan Publishing.

Tilley, Nick. 2009. *Crime Prevention*. Cullompton, Devon: Willan Publishing.

Timan, Tjerk. 2013. *Changing landscapes of surveillance. Emerging Technologies and participatory surveillance in Dutch nightscapes*, Department of Science, Technology and Policy Studies, University of Twente, Enschede.

Tromp, Nynke, Paul Hekkert, and Peter-Paul Verbeek. 2011. "Design for socially responsible behavior: A classification of influence based on intended user experience." *Design Issues* no. 27 (3):3–19.

United Nations General Assembly. 1948. Universal Declaration of Human Rights. Palais de Chaillot, Paris: United Nations.

Van Brakel, Rosamunde, and Paul De Hert. 2011. "Policing, surveillance and law in a pre-crime society, understanding the consequences of technology based strategies." In *Technology-led policing*, edited by E. De Pauw, Ponsaers, P., Vijver, K. V. der, & Deelman Piet., 163–192. Cahiers Politiestudies.

Van Burik, A. E., C. Hoogeveen, B.J. de Jong, B. Vogelvang, A. Addink, and M. van der Steege. 2013. Evaluation of the approach to criminal youth groups. edited by Van Montfoort / Bureau Alpha/ Nederlands Jeugdinstituut: Ministerie van Veiligheid en Justitie.

Van den Hoven, Jeroen. 1999. "The Internet and the Varieties of Moral Wrongdoing." In *Internet and Ethics*, edited by D. Langford, 127-157. London: McMillan Press.

Van den Hoven, Jeroen. 2007. "ICT and Value Sensitive Design." In *IFIP International Federation for Information, The Information Society: Innovations, Legitimacy, Ethics and Democracy Processing*, 67-72. New York: Springer

Van der Ploeg, Irma. 2003. "Biometrics and Privacy A note on the politics of theorizing technology." *Information, Communication & Society* no. 6 (1):85-104.

Van der Ploeg, Irma. 2005. *The Machine-Readable Body. Essays on Biometrics and the Informatization of the Body*. Maastricht: Shaker.

Van der Ploeg, Irma. 2008. Social and Ethical Aspects of Digital Identities. Towards a Value Sensitive Identity Management. In *European Research Council research proposals*. Maastricht: Zuyd University.

Van der Ploeg, Irma, and Jason Pridmore. 2016. *Digitizing Identities. Doing Identity in a Networked World*. Abngton, UK: Routledge.

Van Gemert, Frank. 2012. "Five decades of defining gangs in the Netherlands: The Eurogang paradox in practice." In *Youth Gangs in International Perspective: Results from the Eurogang Program of Research*, edited by Finn-Aage Esbensen and Cheryl Lee Maxson, 69-83. New York Dordrecht Heidelberg London: Springer.

Van Sluis, Arie, Peter Marks, and Victor Bekkers. 2011. "Nodal Policing in the Netherlands: Strategic and Normative Considerations on an Evolving Practice." *Policing and Society* no. 5 (4):365-371.

Vedder, Anton. 2001. "KDD, Privacy, Individuality, and Fairness." In *Readings in CyberEthics*, edited by R.A. Spinello and H.T. Tavani, 404-412. Boston, Toronto, London, Singapore: Jones and Bartlett Publishers.

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

Verbeek, Peter-Paul. 2006. "Materializing Morality. Design Ethics and Technological Mediation." *Science, Technology, & Human Values* no. 31 (3):361-380.

Verbeek, Peter-Paul. 2008. "Obstetric Ultrasound and the Technological Mediation of Morality: A Postphenomenological Analysis." *Human Studies* no. 31:11–26.

Verbeek, Peter-Paul. 2011. *Moralizing Technology: Understanding and Designing the Morality of Things*: University of Chicago Press.

Verbeek, Peter-Paul. 2015. "COVER STORY Beyond interaction: a short introduction to mediation theory." *interactions* no. 22 (3):26-31.

Vermaas, Pieter, Peter Kroes, Ibo van de Poel, Maarten Franssen, and Wybo Houkes. 2011. *Philosophy of Technology. FromTechnical Artefacts to Sociotechnical Systems*. Edited by Caroline Baillie, *Lectures on Engineers,Technology, and Society*: Morgan & Claypool publishers.

Von Schomberg, Rene. 2011. Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Directorate General for Research and Innovation of the European Commission.

Waelbers, Katinka. 2011. *Doing Good with Technologies. Taking Responsibility for the social role of emerging technologies, Philosophy of Engineering and Technology*. Netherlands: Springer

Wajcman, Judy. 2010. "Feminist theories of technology." *Cambridge Journal of Economics* no. 34 (1):143–152.

Weisburd, David, Wim Bernasco, and Gerben J.N. Bruinsma. 2009. *Putting crime in its place: units of analysis in criminology*: Springer.

Werret, Simon. 1999. "Potemkin and the Panopticon: Samuel Bentham and the Architecture of Absolutism in Eighteenth Century Russia." *Journal of Bentham Studies* no. 2.

Williams, Vicky S., and Barry O. Williams. 2008. "Technology applications: Tools for law enforcement." In *Handbook of police administration*, edited by Jim Ruiz and Don Hummer, 165-173. Boca Raton, London, New York: CRC Press, Taylor& Francis Group.

Williamson, Tom. 2008. *The Handbook of Knowledge-Based Policing. Current Conceptions and Future Directions.* West Sussex, England: John Wiley& Sons.

Winner, Langdon. 1980. "Do Artifacts have Politics?" *Daedalus. Modern Technology: Problem or Opportunity?* no. 109 (1):121-136.

Wisler, Dominique, and Ihekwoaba Onwudiwe. 2009. "Rethinking police and society: community policing in comparison." In *Community Policing. International patterns and comparative perspectives,* edited by Dominique Wisler and Ihekwoaba Onwudiwe, 1-17. NY: CRC Press. Taylor and Francis Group.

Wood, David Murakami. 2006. A report on the surveillance society. edited by Information Commissioner: Surveillance Studies Network.

Woolgar, Steve, and Geoff Cooper. 1999. "Do Artefacts Have Ambivalence? Moses' Bridges, Winner's Bridges and Other Urban Legends in S&TS." *Social Studies of Science* no. 29:433-449.

Wyatt, Sally. 2003. "Non-users also matter: The construction of users and non-users of the Internet." In *How users matter*, edited by Nelly Oudshorn and Trevor Pinch, 67-79. Cambridge: MIT Press.

Wyatt, Sally. 2008. "Technological Determinism Is Dead; Long Live Technological Determinism." In *The Handbook of Science and Technology Studies*, edited by Edward J. Hackett, Olga Amsterdamska, Michael Lynch and Judy Wajcman, 165-180. Cambridge: MIT Press.

Zureik, Elia, and Mark B. Salter. 2005. *Global surveillance and policing: Borders, security, identity*. Cullompton: Willan Publishing.