Electronic Fortune-Tellers

Predictive policing as a sociotechnical phenomenon

By Ailo K. Ravna

Master thesis at the Centre for Technology, Innovation, and Culture (TIK)
Faculty of Social Sciences
Spring 2015

UNIVERSITY OF OSLO

25.05.2015

Word count: 38882

Electronic Fortune-Tellers

- Predictive policing as a sociotechnical phenomenon

Anderton said: "You've probably grasped the basic legalistic drawback to precrime methodology. We're taking in individuals who have broken no law."

"But they surely will," Witwer affirmed with conviction.

"Happily they don't – because we get them first, before they can commit an act of violence. So the commission of the crime itself is absolute metaphysics. We claim they're culpable. They, on the other hand, eternally claim they're innocent. And, in a sense, they are innocent. (…) In our society we have no major crimes, but we do have a detention camp full of would-be criminals."

Philip K. Dick, The Minority Report (1956)

The predictive-policing era promises measureable results, including crime reduction; more efficient police agencies; and modern, innovative policing. Predictive policing already has been shown to enable doing more with less, while significantly improving policing outcomes through information-based tactics, strategy, and policy.

Charlie Beck and Colleen McCue, Police Chief Magazine (2009)

2015

Electronic Fortune-Tellers – Predictive policing as a sociotechnical phenomenon

Ailo K. Ravna

http://www.duo.uio.no/

Printing: Reprosentralen, Universitetet i Oslo

Abstract

Big Data technologies are becoming increasingly prevalent across many aspects of society. By using advanced algorithmic models and vast databases, programmers have developed tools that can accurately calculate the probabilities of future events occurring. Predictive policing is one such tool, promising to forecast criminal activities down to a particular time of day and a 150x150 meter area. By analyzing criminological data and other contextual information, patrolling officers receive continually updated predictions through smart-pads outfitted in their cars. This signifies a change in policing, from taking a reactive approach to crime, towards being proactive and preventing the crime from happening in the first place. Although some law enforcement officials have been quick to embrace this new technology, proclaiming a new era of policing, others are less enthusiastic. Citing potential issues such as the erosion of civil rights and unconstitutional racial profiling, critics of predictive policing are actively emphasizing certain aspects of the technology as a means to highlight controversial issues.

In this thesis, I explore how a technological artefact such as predictive policing is inseparably tied up in a number of socio-political issues. When analyzing technology, it is important to consider not only the hard technical factors, but also assess the social context. I draw upon theories from Science and Technology Studies (STS) as a basis for analyzing the debate surrounding predictive policing. This entails identifying the relevant actors of the debate, but also includes opening the "black box" of Big Data by examining its inner workings. Using concepts from the Social Construction of Technology (SCOT), as well as Actor-Network Theory (ANT), I outline how social groups are formed and maintained as they attempt to negotiate technological and social change. Thus, the social context of the technology is presented as part of a seamless web, where technical, social, and political matters are inseparably entwined. Finally, I use concepts from John Dewey's theory of the public to demonstrate how political issues are embedded in and around technologies. The aim of my thesis is to show how complex technological systems such as predictive policing are embedded in a sociotechnical world, and to demonstrate how concepts from STS can be used to better understand the social underpinnings of the technology. This implies that in order to properly evaluate such technologies, one must take care to consider the interests of actors who become implicated in the technology through being affected by its consequences.

Acknowledgments

In the course of the months spent writing this thesis, I have received invaluable assistance and advice from a number of people. Without these individuals, I would undoubtedly have felt lost at sea at several junctions. It's been an interesting journey, filled with excellent high-points and some frustrating lows, and I am grateful for all the support. As all things must end, it is time to cut myself off from further edits and rewrites, and finally send the thesis to the printers.

Big thanks are due to my supervisor Sissel Myklebust, for invaluable guidance and many interesting discussions about Big Data and its wider implications. The encouragement has been helpful, but the constructive criticism and suggestions for further theoretical pursuits have been even better. Additional thanks to my family, particularly my parents who have both provided the inspirational spark to pursue a master's degree, and provided constant reassurance and in-depth proofreading whenever it's been needed. Further gratitude goes out to my wonderful girlfriend Amanda, for her unwavering patience, backing, and for keeping me sane. Finally, appreciation is in order to the people at the TIK-centre at UiO, and to Teknologirådet, for their friendliness and for helping me steer my project onto the right track. If not for all of you, this final product would undoubtedly be worse off. Cheers!

Ailo Ravna

May 2015

Table of contents

1 Introduction

1.1 Predicting crime using Big Data

With the dawn of the Information Age, the growth and spread of new digital technologies is on a steady upward trajectory. Clever programmers, innovators, and Silicon Valley entrepreneurs are developing new ideas on a massive scale, with promising start-ups appearing on an almost monthly basis. Everything from birth records to cemetery memorials1 have taken the step into the digital world, and the growth of storage capacity and processing efficiency has yet to start seeing diminishing returns. Although in some ways still an abstract concept, “Big Data” has become an increasingly popular buzzword in the last few years. From cutting edge business and entertainment services, to health care and biological research, Big Data promises increased efficiency and accuracy to an unprecedented degree. Improvements in digital technologies allow for cheap and plentiful storage, and the ability to analyze and manipulate enormous databases with literally just a few clicks. Advanced algorithms can be used to find and extract patterns in one or more sets of data, from which novel inferences can be drawn.

As the technology spreads through different areas of society, the promise of Big Data is also appearing in various public institutions. Tools are being co-developed by law enforcement officials, universities, and independent research firms, with the central goal of more efficiently assisting the police in their daily tasks. As an institution with vast archives of information at their disposal, the technologically limited ability of searching and extracting relevant data has long been a bottleneck for police research. With the introduction of Big Data, this appears to be changing. A series of innovative technologies, collectively known as “predictive policing”, have already been rolled out in several police districts in the United States and in the United Kingdom. By analyzing crime statistics and other contextual data on the spot, continually updated information about vulnerable areas can be quickly dispatched to patrolling officers, allowing the officers to arrive at probable crime scenes to prevent

[1] http://www.findagrave.com/

transgressions from occurring. As the technology is diffused throughout law enforcement agencies, it may change the ways that officers work on the streets, eventually transforming traditional policing. Alternately, predictive policing could become just another tool in the police arsenal, comparable to the Taser gun or the police radio. Both of these predictions may be equally valid, and I will show how a range of both similar and occasionally contradictory views pervade in the discussion surrounding the technology. By presenting a number of these perspectives, I want to uncover the underlying social aspects of predictive policing, and demonstrate that it might be impossible, or irresponsible, to properly assess the technology without paying heed to its many facets. By extension, I also aim to address how technologies such as predictive policing are entangled with broader social aspects, and may even be inseparable from political issues.

1.2 Theoretical basis

In this thesis, I will explore the concepts of Big Data, and particularly the algorithmic tools that constitute predictive policing, by drawing on literature covering different aspects of this continually expanding and developing field. My aim is to analyze predictive policing as a socially embedded technological artefact, by using theoretical concepts from Science and Technology Studies (STS). In a significant portion of STS literature, technological artefacts are approached and analyzed as socially constructed phenomena. This is usually done by identifying and following involved actors or stakeholders, and seeing how these relate to each other and to the artefact. Technologies are assessed not as closed-off entities, but rather as products of social negotiations and as enduring processes. By refusing to separate technology from domains such as the social, the political, or the economic, a social constructivist theory of technological change thus operates by unpacking not only the physical inner workings of the artefact, but also aims to reveal the context, or worlds, that are negotiated and maintained within and around the technology. Through the lens supplied by STS, I want to examine how technologies and society are co-constitutive, and consequently that technologies must be evaluated in context of relevant social and political factors.

Based on insights from STS, my goal is not limited to understanding how crime can be predicted by the use of algorithmic functions. Of course, an understanding of the technical functions is important in any analysis of a specific technology, and will therefore make up a considerable part of this thesis. I also want to go further, however, by showing how various actors and social groups have different understandings of, and assign their own meanings to, technological artefacts. For this purpose, one of my theoretical backbones will come from the STS theory Social Construction of Technology, or SCOT. By looking at technological artefacts as a continuously negotiated product of a social process, the SCOT approach emphasizes that there is nothing inherently natural or determined about how an artefact is developed, shaped, or used. What may seem like a tool for hammering nails to one person may be a means of defense to another, or even a symbol of the proletariat to a third party. An artefact may be construed as several different artefacts at once, depending on who is contemplating it, or on the context of its use. It is therefore not a given fact that a particular artefact represents the ideal outcome of a process of elimination; perhaps history had been different if different groups had their version of a technology come out on top. In other words, there is a streak of methodological relativism running through the SCOT theory, where everything is up for discussion and very little is taken for granted. In addition to using methods from SCOT, I will be supplementing my analysis by using Actor-Network Theory (ANT). ANT is focused on the relationship between actors and technologies, and the ways in which they interact and shape themselves. ANT deals with both the shaping and maintenance of social networks, and the ways that material objects are part of these networks. I will therefore make use of ANT to emphasize the process in which technology is shaped, as a way to "fill in the gaps" in areas where SCOT focuses more on the structure of the social groups.

1.3 Research questions

By bringing concepts and methods from STS to the case of predictive policing, I hope to provide a better understanding of how technologies can be multifaceted. Where other sociological theories have a tendency to focus only on the social factors and leave the technologies themselves unexplored, the SCOT approach transcends the boundaries between the purely technological and the social, treating these boundaries as artificial constructs. Predictive policing as a case study has the advantage of being a novel piece of technology, where negotiations about its meaning are still taking place. As I will demonstrate, different actors and groups are in disagreement about not only whether predictive policing is an effective measure for crime-prevention, but also about if it is an acceptable technology within a democratic society. Predictive policing, then, is not simply an elegant technical solution for patrolling officers, nor is it a cynical political tool for holding certain minorities down. It can be construed as both of these, and more, but at the heart of the matter it is a conceptual framework where different actors meet and negotiate their own principles and meanings, inscribing themselves onto the technology. By acknowledging this, it appears that the questions surrounding predictive policing are also inseparably tied to concepts of broader society and to the political.

This leads me to my research questions, which are based upon central concepts from the SCOT and ANT theories.

1) Who or what are the relevant actors and social groups, and how do they define the meaning and acceptability of predictive policing?

2) How are these groups mobilizing, and which closure mechanisms are they employing when attempting to shape predictive policing in their own image?

3) How does the technology reflect the interests of, or otherwise affect different social groups, and how are certain political issues embedded in the technology?

In other words, my analysis will cover three main conceptual levels, which are inseparably entwined in the technology. These aspects are the technology in itself, actors and social groups, and political issues. By giving a thorough description of both the technical functions, meaning how predictive policing actually works, and of the differently perceived possible problems and solutions that follow, I want to make a contribution to understanding how Big Data technologies are more than simply material objects. One of my overarching goals, then, is to demonstrate how complex technological systems such as Big Data should not be evaluated on a strictly technological basis. By mapping the variety of actors, social groups, and issues raised around the technology, it should become clear that predictive policing needs to be assessed as a sociotechnical phenomenon. On a bigger scale, I want to emphasize and show how society and technology are dynamic and interactional concepts, and that they should be treated as co-productive phenomena. As they develop and change, they impact each other in significant ways, and this must be considered when assessing the technology and its wider application.

1.4 Thesis structure

One of the main advantages of doing a SCOT analysis is that it does not ignore or gloss over the inner workings of the technology itself. Chapter 2 will therefore be mostly descriptive, in an attempt to give some clarity to what the concept of "Big Data" actually entails. The technology, and particularly the algorithms working behind the scenes, is becoming increasingly advanced and, consequently, difficult to understand. The descriptive account of chapter 2 will therefore be further elaborated upon in chapter 3, where I give a more specific overview of the particularities of predictive policing. Drawing inspiration from earlier SCOT case studies,[2] I will present a narrative of how predictive policing was developed, and go on to briefly look at how it has been taken into practical use. This lays the groundwork for understanding the process of how the technology is formed. Because of the complexity of the algorithmic process, I will dedicate chapter 4 to explain the inner workings, or "opening the black box" of Big Data. With the mostly descriptive account out of the way, in chapter 5 I will explain my theoretical framework, presenting key concepts from the SCOT and ANT theories. These theoretical concepts are put more directly into practice in chapter 6, in which my chosen methods and empirical material are laid out. The analysis, which will take up the entirety of chapter 7, will give an account of the process in which social groups are shaped, as they simultaneously ascribe meaning to the technology. These often-conflicting views play a key part in how the groups define themselves, but also form the front lines on which closure mechanisms are developed and applied. Additionally, I will explore the ways in which political and social issues are embedded in the technology. I will conclude by summing up and reflecting on my main points and discoveries in chapter 8, and point towards possible areas for further research.

[2] Amongst others, the studies presented in the chapters by Bijker, John Law, and Donald MacKenzie in Bijker, Hughes, and Pinch (1987)

2 Big Data

2.1 Introducing Big Data

In our increasingly digitalized world, almost everything that can be quantified is recorded and stored on central databases or servers. From social networks and smartphones, to health registers and parking meters, technological gadgets and applications are constantly collecting a continuously flowing stream of information. These enormous amounts of data have a lot of potential to make our lives, and the lives of legislators and government officials, easier, streamlined, and more comfortable. For an example of how these technologies might influence your daily life, one needs only look to the recommendation algorithms of online marketplaces such as Amazon and eBay. Every time you place an order, a number of algorithms work behind the scenes to show you other products you may like, based on your previous purchases and the history of other customers. Every transaction feeds into the algorithm, which adjusts itself accordingly to ensure even better recommendations in the future.[3] A similar innovation is behind Facebook's presentation of advertisements that are suited to each member's personal interests. If you click many links about sports and fitness, it is likely that you will see advertisements about gym memberships, fitness clothing and so on. Besides the obvious commercial advantages this provides, it is easy to see how this process helps you and other customers have an optimal personalized experience, to which all users contribute without having to go through the effort of customer surveys or other more intrusive feedback mechanisms. The process of collecting, analyzing, and using these vast amounts of information is part of the technology collectively known as "Big Data". In this chapter, I will give an account of the phenomenon that is Big Data, setting the stage for more specialized artefacts such as predictive policing. The "hardest" descriptive account, concerning the complex inner workings of the process, will be held off until chapter 4.

Microsoft researchers Danah Boyd and Kate Crawford draw a distinction between the traditional concept of "big data" and the novel technological concept "Big Data", capitalizing

[3] See Linden, Smith, and York (2003), for an overview of Amazon.com and their use of recommendation algorithms.

the latter to particularize the modern use of the term (Boyd and Crawford 2012, 663). This distinction is necessary because large datasets have been a common feature of quantitative research and statistics for a long time, and is therefore not an inherently novel phenomenon. Even the computerization of such data is not a new concept, but whereas scientists 50 years ago relied on supercomputers to analyze their comprehensive databases, technologies such as cloud computing, increased processing power, and advancement in digital storage have progressed to the point where a mid-range desktop computer is able to do the job. Therefore, Boyd and Crawford emphasize that the novelty of Big Data is not primarily about the data itself, but rather applies to the unprecedented capacity to search, aggregate, and cross-reference/compare these enormous sets of data. Big Data, then, is a matter of developing newer and more effective tools for analysis. Throughout this thesis, I will be leaning on Boyd and Crawford's definition of Big Data, denoted by the capitalization. However, there are aspects of Big Data that go beyond the physical tools that enable it.

The modern concept of Big Data can be summarized as a cultural, technological, and scholarly/scientific phenomenon that is built upon the interplay of technology, analysis, and mythology. The technological aspect, as noted, consists of maximization of computational power and algorithmic accuracy, including storage space, processing power, and digital networking. By improving these factors, the Big Data process can become more effective at gathering data, as well as analyzing, linking, and comparing the data sets. On the analytical level, a Big Data process is able to identify patterns in the raw data, and through further analysis, it can infer claims about social, legal, economic, natural, or technical issues, amongst others. The final aspect of Big Data that Boyd and Crawford identify is the rather abstract concept of "mythology". By mythology, they refer to a widespread belief that by analyzing sufficiently large sets of data, one may be able to generate insights or truths that would be unreachable without these new technological tools. This involves having faith in, that with enough data, you may gain access to a form of higher objectivity, undiluted by human interference or bias (Boyd and Crawford 2012, 663). Together, these three factors make Big Data something more than simply the large sets of data in itself. This implies that the technology represented by the term "Big Data" is not simply a black box that digests data and spits out truth, it is also inseparably embedded in a sociotechnical world.

2.2 The Big Data process

Although somewhat simplified, one can say that the process usually involved in Big Data consists of three basic stages. These stages can be divided into the collection of data, the storage and aggregation of data, and the process of data analysis, with the possible addition of a fourth step, consisting of putting the results of analysis into practical use. The analytical process is quite complex, and therefore a more in-depth account of the process will be given its own chapter. The actual collection of data may seem fairly straightforward, although the complexity of the task will vary depending on what is being analyzed. In the case of earthquake-prevention, this can include geological findings, historical data about previous conditions, and contextual information. In the case of social media, ways of collecting data can range from voluntarily supplied personal information, such as your name and date of birth on Facebook, to hidden trackers that analyze which links you are clicking and how much time you are spending on each website. In the case of predictive policing, we will see that the data gathering can consist of compiling existing databases on criminal statistics, but other sources such as weather conditions, community planning data, and social factors can also be potentially fruitful. Data-collection may also entail searching legal and other official documents, and most other digitally available sources of information are potentially viable sources of useful data.

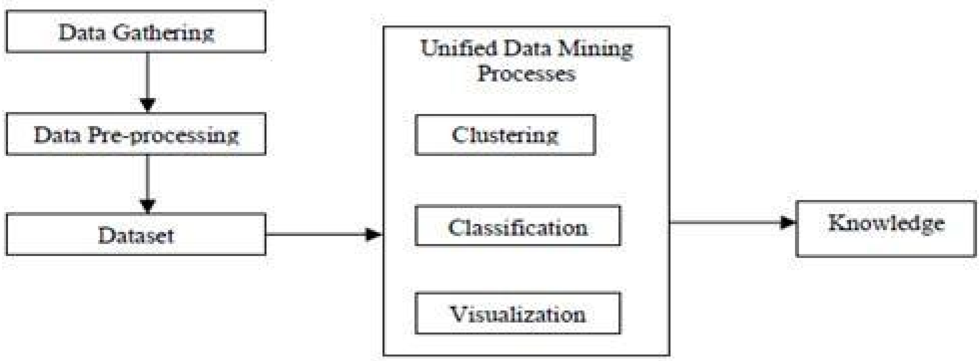

Figure 1: A simple illustration of what a data mining process might look like. Source: Khan, Mohamudally, and Babajee (2012)[4]

[4] http://www.intechopen.com/books/advances-in-data-mining-knowledge-discovery-and-applications/towards-the-formulation-of-a-unified-data-mining-theory-implemented-by-means-of-multiagent-systems-m [accessed 26.02.2015]

The next step of a Big Data analysis consists of storing, processing, and aggregating all the collected data. Servers, hard drives, networked storage (such as cloud computing), and other digital storage mediums are growing in size at reduced costs, and can contain unprecedented amounts of data, transferrable almost instantly. It is common to apply several methods of post-processing after the data has been collected. In cases where personal or sensitive data is used, for example, it is common to anonymize the data at the point of storage. This is possible by omitting information that could lead to identification or re-identification of individuals, or through the process of aggregation. Aggregation involves joining individual data into larger sets, and for example rounding off numbers and omitting anomalies in order to avoid that any potentially harmful or identifiable information stands out from the set. All of this may take considerable computing power, especially with larger sets of data. This represents a significant break from earlier processes of analysis, which were limited by technological confines. It is important that the system can deal with both structured and unstructured data, indexing the data, and making it searchable (Datatilsynet 2013, 14). As hardware improves and costs are reduced, the threshold for working with Big Data analytics thus becomes lower. With access to the right databases and sufficient knowledge of the process, anyone with the proper analytical tools and a decent computer should in practice be able to work with Big Data. The third step of the Big Data process entails the actual analytical process. For now it is suffice to say that there are a large number of different methods of analysis. The methods will vary depending on the sort of data one is working with, the sought after results, and technological limitations. A more in-depth account of some of these methods will follow in chapter 4.

2.3 What makes Big Data different?

As with many new technologies, stakeholders and other supporters are often eager to proclaim the revolutionary nature of Big Data, while other groups are more apprehensive. As noted, there is nothing inherently groundbreaking about collecting and analyzing datasets, and statisticians have been doing probabilistic calculations for a long time without the aid of Big Data systems. To get a firm grasp on what Big Data means, it is therefore necessary to clearly identify what sets it apart from its predecessors. Building upon earlier empirical approaches, Big Data analytics are able to estimate the probability that certain facts are true, or that they will become true in the future. This is already a part of the traditional methods in statistics, but when used in an area such as law enforcement, a break from earlier techniques can be clearly distinguished. Previous information systems used by the police draw upon databases with the potential for statistical analysis, but are mainly used to locate particular data points, such as outstanding warrants, identifying legal precedents, and so on (Moses and Chan 2014, 663).

With the use of Big Data analytics, the focus is removed from the particular data points, acknowledging their possible inaccuracies, and instead looking at the bigger picture. As more data is included, the potential to find correlations and patterns increases, which can be used to make new inferences. Although the theoretical potential for this method already existed, the sheer efficiency of the Big Data process makes it a significantly more feasible method for practical use. When looking at smaller data sets, which less advanced approaches are often limited to, one will often face the problem of lacking statistical significance. By aggregating enormous numbers of data points through the use of Big Data tools, inferences can be accurately generalized to large populations, thereby also strengthening the predictive value in practical contexts such as policing. However, this approach may also have consequences for the interpretability and transparency of the produced results. The automated analytical and inferential tools could draw conclusions that are statistically justified, but problematic in other aspects. It is therefore important not to be blinded by the mythological factor of Big Data as a phenomenon. More advanced technologies do not necessarily mean that higher truths are accessed, and one should remain vigilant so that faulty reasoning or similar problems are not obscured by complicated technological mechanisms. As Moses and Chan note, *"As data size increases, so does the potential for mistakes."*(Moses and Chan 2014, 666).

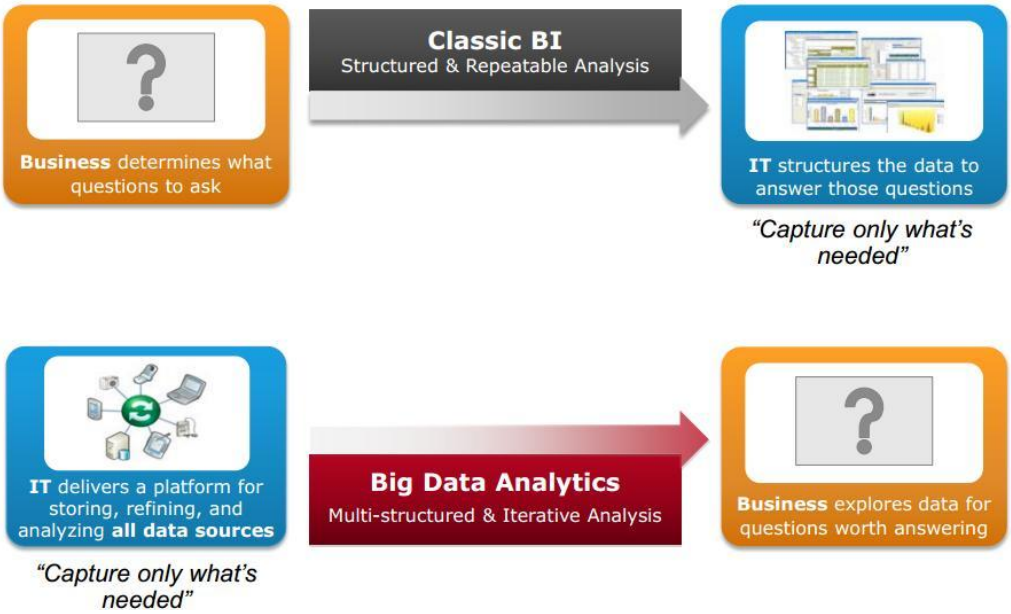

Figure 2: An example of Big Data turning the search for solutions on its head. Source: Rose Business Technologies (2013)[5]

2.4 Summing up

In this chapter I have shown how Big Data tools are changing the convenience of personalized and public services, but may also transform certain methods of gathering knowledge. The increased ability to gather, store, and analyze enormous sets of data is making data analysis into a very complex, yet highly efficient method of extracting new knowledge and uncovering correlations. There are, however, aspects of Big Data that stretch beyond the purely mathematical and statistical. In addition to identifying patterns that would be impossible to discover using traditional methods, Big Data also carries a certain mystique, or mythological factor. There is a tendency amongst some proponents of Big Data to believe that, with enough data, one might gain access to objective truths. When analyzing Big Data from a sociotechnical perspective, this concept of mythologization is important in order to understand how different social groups assign their own meanings to the technology. As new technologies are developed and diffused, what some groups *believe* the technology to be, could be as important as its actual functions.

[5] See http://www.rosebt.com/blog/category/database%20management%20systems/2 [Accessed 26.02.2015]

3 Predictive policing

3.1 What is predictive policing?

Predictive policing is a set of new technologies that use Big Data processes in order to effect real world changes. It is a tool developed by mathematicians, physicists, and statisticians, applying Big Data-based algorithmic principles to the very human phenomenon of crime. By calculating the probabilities of certain crimes taking place in a particular area, at a specific time, predictive policing can be used to direct patrolling officers towards crime scenes before they happen. One broad definition of predictive policing reads as following;

> Predictive policing refers to <u>any</u> policing strategy or tactic that <u>develops</u> and <u>uses</u> information and <u>advanced analysis</u> to inform <u>forward-thinking</u> crime <u>prevention</u>. (Morgan, in Uchida 2009, 1, emphasis in original).

Reformulated, this includes using Big Data analytics to calculate the probability of future criminal occurrences, integrating criminological data archives into the process, and allowing officers to act proactively in order to prevent these events. In this chapter, I will describe the case of how one such technology was developed, a piece of software named PredPol. I will chronicle its early development by university researchers and programmers, and the initial results from its practical use by law enforcement institutions. Using the right kind of data and algorithms, predictive policing technologies could also be used for identifying individual threats such as potential terrorists, likely victims of targeted attacks, and so on. Although these applications undoubtedly raise a lot of questions concerning privacy, I will focus on the models used to target geographical locations rather than individuals, as this most closely matches the models currently in use by law enforcement.[6]

---

[6] The RAND Corporation have published an extensive report on different facets of predictive policing. I will be drawing on some of its content, but as noted this will be focused on the design of the PredPol-case. The possibility of singling out or targeting individuals raises critical questions of privacy, which I will avoid for the purpose of my thesis. For the 189-page report, see Perry (2013)

3.2 The technology emerges

Technologically minded seismologists, the scientific study of earthquakes, were early adopters of using Big Data analytics for scientific purposes. By using geological information, historical records, and other context-sensitive data, innovative programmers were able to construct algorithms that can predict aftershocks with a high degree of accuracy (Reich 2002). The following is a story about a meeting of minds, and of how earthquakes and crime could have more in common than you might think. Sometime around 2007 in Los Angeles, an anthropologist named Jeffrey Brantingham met up with fellow UCLA-researchers, mathematicians Andrea Bertozzi and Lincoln Chayes. Their ambition was to devise a method for understanding criminal behavior with the help of advanced mathematical models. A research program was founded, and the researchers began experimenting with models based on existing criminological methods, including what is known as "hot spotting". The basic idea of hot spotting is that crime multiplies and clusters, leading to certain areas becoming "hot spots" for unlawful activity. Identifying such hot spots has been a routine part of police work for some time, as an efficient way to assign patrols and dedicate resources to vulnerable areas. What the researchers were after, however, was an algorithmically based model to improve and to some degree automatize the process. The group created computer simulations to map the hypothetical movement and clustering of crime, with varying degrees of success. Hot spots were shown to emerge, but the model was still purely theoretical and lacked the real-world data that would make it practical for actual police use.[7]

The tools the scientists needed surfaced when the mathematician George Mohler joined the team. He brought a method known as "stochastic declustering", an analytical tool used by seismologists when they model earthquakes and its aftershocks. As seismologists are well aware of, the risk of earthquakes are persistently higher in certain geographical regions. California, situated on the tectonic boundary between the Pacific and the North American tectonic plates, is particularly earthquake-prone. In addition to these relatively constant geological data, there is also a geographical and time-dependent risk of aftershocks. Although, even within earthquake-prone zones, the actual quakes mostly occur seemingly at random, the aftershocks follow certain spatial and temporal patterns. With stochastic

[7] Detailed in Mackenzie (2012), at http://www.siam.org/news/news.php?id=1953 [last accessed 02.03.2015]

declustering, traditional statistical methods are combined with Big Data analytics, in order to calculate the relationship between the patterns of aftershocks and the constant geological factors. The information derived through this method can then be used to predict how future earthquakes will lead to potential aftereffects (Mackenzie 2012).

3.2.1 From aftershocks to criminal activity

Imagine the city and surroundings of Los Angeles through the eye of a criminologist. Some neighborhoods are hot spots, or in layman terms, simply "bad neighborhoods". These may be areas of poverty, drug-abuse, low police presence, and so on. In criminology, there is a general theory stating that crimes begets more crime, so for example when a house is robbed, the risk of burglary in the adjacent area rises. This is called a "near-repeat effect", and mainly applies to geographically dependent crimes like burglaries and gang-related turf-wars.[8] The parallels to earthquake-behavior becomes clear when applying similar terms. A robbery, although seemingly occurring at random, might trigger aftershocks consisting of similar crimes in the surrounding area. This can happen, for example, by a burglarized house signaling that security in an area is lax, or roaming groups of criminals could be operating in particular neighborhoods. By using existing data about past crimes and related incidents, much in the same way that seismologists use geological and seismological data, the UCLA anthropologists and mathematicians wanted to predict how crime is likely to spread. Adapting models from seismology and mathematics, the researchers were primarily interested in the physical act of crime and its patterns. Other motivating or sociological causes of crime, like poverty, inequality, and alienation, were put aside as external factors, outside the scope of the simulation. In other words; the focus of the research treated criminal behavior as a purely physical act of opportunity.

At the core of the project was the idea that human behavior is inherently predictable, and that with enough information it might be possible to forecast human action with a high degree of accuracy. While that idea in itself may seem counterintuitive, or even an indictment of freedom of will, the idea is not new to social sciences. Models that range from urban planning

[8] Demonstrated in Townsley, Homel, and Chaseling (2003)

to economic simulations are dependent on the phenomenon that given large enough numbers, people will behave and act in certain ways.[9] As Brantingham explained in an interview with the LA Times, “In a sense, crime is just a physical process, and if you can explain how offenders move and how they mix with their victims, you can understand an incredible amount.” (Rubin 2010). In other words, since human behavior is not random, it can be calculated and translated into mathematical terms. This opens the doors for algorithmic analysis of behavioral patterns.

Another member of the research team, the physicist Martin Short, worked on a somewhat different method for understanding crime. By adapting statistical and economic theories to criminal behavior, he wanted to understand when, where, and why transgressions occur. Like his colleagues, Short also left social factors out of his analysis, rather opting for a sort of rational choice-theory approach. In this model, would-be criminals are treated as habitual and opportunistic actors who act purely based on rationale and opportunity. In simple terms, this means that the criminal in most cases would choose to commit crimes with a high payoff and minimal risk. Following this theory, a gated community is less likely to be victim of crimes because there are few opportunities for criminal activity, while unprotected houses are easy targets and are therefore honeypots for burglars. With this decision-based theory as his foundation, Short designed a simulation to understand how crime clusters (Rubin 2010). As with Brantingham and Mohler’s models, the simulation started as highly theoretical and abstract. In order to make real-world predictions, Short would need access to real world data, for example information on the housing and security-information in actual neighborhoods, which is not immediately accessible to physicists and mathematicians.

3.3 A police department in search of new methods

In an article published in the Police Chief Magazine in late 2009, the Chief of Detectives for the Los Angeles Police Department (LAPD), Charlie Beck, writes enthusiastically about the promise that Big Data holds for law enforcement. He explains that due to severe budgetary restraints, resulting in understaffing and overstretching of police resources, police departments across the US are in dire need of adapting to doing more work with fewer assets.

[9] For an example, see Pentland and Liu (1999)

Placing the situation in a historical context, an image of a police force that is struggling with being thinly stretched emerges. Beck specifically evokes the terrorist attacks of 9/11 to explain how even small town police are now responsible for doing their part in the war on terror, transforming the duty of homeland security into hometown security. According to Beck, the attacks and their aftermath has had a profound effect on not just the police as an institution, but the very nature of practicing law enforcement (Beck 2009).

Proclaiming predictive policing to herald a new era of law enforcement, Beck briefly summarizes previous paradigmatic police methods. Supplanting the traditional model of community-policing, in which the police would focus not only on stopping crimes, but also address the underlying conditions that foster criminal activity, the post-9/11 era would be characterized by intelligence-led policing (ILP). The main innovation of ILP was a focus on research and analysis through the help of communications technology, including an increased emphasis on efficient sharing of information. This also encompassed a shift from earlier evidence-based methods, moving towards intelligence- or prediction-based action.[10] With an improved flow of information, additional focus on accountability also became important. ILP did not appear directly as a result of 9/11, however, having its roots in the mid 1990's CompStat model.

The CompStat model, or "comprehensive computer statistics", has been used across the US in a variety of forms, and includes monthly meetings of police chiefs, where each district is held directly accountable for their measurable results. With modern technology and programs designed to streamline access to information, the process of identifying criminal hot spots and improving police response were implemented. Because each district could be held directly accountable, identifying the effectiveness of different methods was made easier, and the process could be continually evaluated.[11] With an abundance of access to a plethora of data about crime, social mapping, and other factors, CompStat was not limited by access to information. A bottleneck appeared in the form of analyzing this information; the process of

[10] This does not mean that evidence-based policing was sidelined, but rather that it was assisted by the methods of ILP (Uchida 2009, 2).
[11] *What is CompStat?*, http://www.compstat.umd.edu/what_is_cs.php [accessed 02.03.2015]

extracting data relevant to pending investigations was complicated by the huge amount of material at hand. Police officials had all the necessary data, but lacked the proper tools to exploit it. Meanwhile, the UCLA researchers were developing powerful analytical tools, but needed more data. Thus, when representatives for the LAPD contacted the UCLA research team, a productive collaboration was born.

3.4 Predicting crime with PredPol

The product of the collaborative work between the LAPD and the researchers at the UCLA was a piece of software named PredPol. PredPol uses algorithmic models to analyze existing criminological databases. Through discovering patterns in the existing data, for example related to the place and time of day a car theft is statistically likely to occur, the algorithms are able to project a probability of similar outcomes in the near future. This means that patrolling officers, outfitted with smart pads in their cars, can be supplied with computer-generated tips about where to go, narrowed down to areas the size of 500x500 feet, or about 150x150 meters (Friend 2013). The software also specifies the type of crime, meaning that the officers can be on the lookout for particular types of behavior that fit their existing profiles of gang members, burglars, and so on. Historical data from the last 3-5 years is combined with continuously updated new information, in order to ensure that the probabilities dispatched to the officers are as up to date and accurate as possible. Thus, the police can focus their presence on areas that are high-risk hot spots, or "high crime areas", with a mathematical precision resulting from rapidly sifting through stores of data. Whereas the traditional method of hot spotting is largely dependent on heuristic methods such as the individual officer's familiarity with certain neighborhoods, PredPol allows the officers to supplement their experience with hard statistical probability.

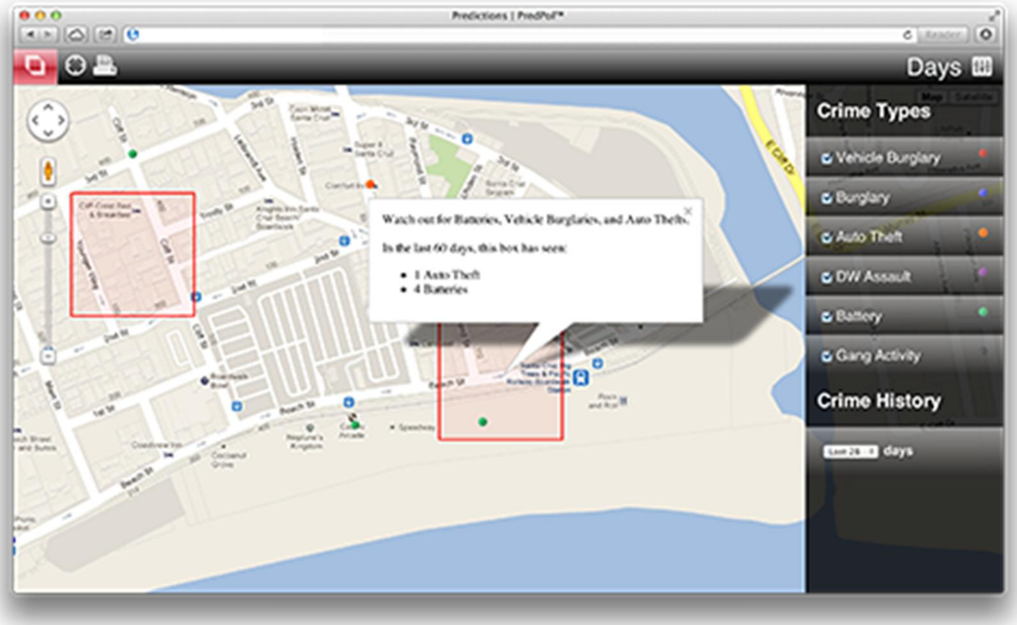

Figure 3: A screenshot from the PredPol software Source: FBI (Friend 2013)[12]

In addition to the obvious strategic advantages that predictive policing provides, the ability to arrive in an area before it has become a crime scene marks a shift in how the police work. The general idea is that by being present at an identified vulnerable spot, the focus can shift from making arrests to preventing the crime from occurring in the first place.

> "This is sort of a paradigm shift in how officers have done policing," says Seattle Police Department Lt. Bryan Grenon. "Before, it was random patrol, go find something. So you're successful if you write that ticket, if you make an arrest. But, in this, if you're out there and your presence alone dissuades a criminal from committing a crime, you're successful." (Kile 2013)

When adding factors such as shrinking police budgets, and the fact that preventing a crime from occurring at all is more economically viable than making arrests, it is not hard to imagine why a number of police departments and their chiefs are lauding predictive policing as a major paradigmatic shift. For now, it should be kept in mind that whereas the researchers approached predictive policing as a way of understanding crime as a physical and predictable

[12] http://leb.fbi.gov/2013/april/predictive-policing-using-technology-to-reduce-crime [accessed 03.03.2015]

phenomenon, law enforcement officials were focused on the problems of funding and resource allocation.

3.4.1 Initial results

On the official PredPol website, the creators claim that after 6 months of randomized trials, experienced crime analysts using predictive technologies operated at twice the efficiency of comparably skilled colleagues with only traditional tools at their disposal. Los Angeles' Foothill Division, which took part in the early pilot project, experienced a 13% drop in arrests compared to non-participating districts. In addition to the significant improvement in statistics, the website asserts that predictive technologies has been a helpful tool for training new officers, as well as improving the knowledge of experienced patrolmen.[13] In Santa Cruz, another PredPol pilot-district, two dozen arrests were made inside the predicted hot spots during the first six months of the trial. As noted, however, the overarching goal of using PredPol is not to increase the number of arrests, but rather to prevent the criminal activity from occurring in the first place. Over the same six months, the Santa Cruz police department also experienced a 19% decline in burglaries (Friend 2013). After another six months had passed, the results were still looking solid.

> In its first year using the software, the Santa Cruz Police Department saw assaults drop by 9 percent, burglaries down 11 percent, and robberies down 27 percent. Meanwhile, auto theft recoveries rose by 22 percent and arrests were up 56 percent. (Kile 2013)

These results come from departments with staffing and budgetary problems, and to which no additional resources (apart from the software) had been granted during the trial period. There are, of course, reservations to be made about such results. Placebo-like effects, in which the patrolling officers are more likely to behave differently because of the new technology, is one factor that might skew the statistics. Patrolling officers and other police officials, excited to prove the efficiency of the innovative system, may add another subjective element. Despite such possibilities, however, it was concluded that the initial results were looking very promising. The pilot program has since been rolled out in several other US cities, as well as in certain districts in the United Kingdom. Initial results after a four month trial showed a 6%

[13] See PredPol (n/d), http://www.predpol.com/results/ [accessed 24.09.2014]

reduction in street violence in the UK district of Kent,[14] while in the Atlanta-area a trial project reported reductions in burglaries and robberies of between 15-30% (Frampton 2013).

3.5 Summing up

We have seen how Big Data analytics already in use in fields such as seismology, mathematics, and statistics, were adapted to analyze and predict deviant human behavior for law enforcement purposes. The initial research project at the UCLA focused on the non-random aspects of criminal activity, and the researchers were able to construct sophisticated models, but were lacking access to real-world data. Around the same time, police departments in the Los Angeles area were struggling with cutbacks, resorting to seeking new methods and tools to improve their efficiency. The combined outcome of these two ventures was a new piece of Big Data software called PredPol. By consulting a continually updated map on a smart pad, patrolling officers are given algorithmically derived predictions about when and where specific crimes are likely to occur. When the story is told like this, it seems easy to fall for the so-called mythological aspects of Big Data; the PredPol software appears almost as a magical black box, which feeds on information and produces accurate predictions and tangible results. In the following chapter I will dispel this notion, by opening the technological black box and detailing the algorithmic workings within. What might appear to a casual observer as computer magic, is actually far more complex than some digital crystal ball.

[14] See BBC (2013) http://www.bbc.co.uk/news/uk-england-kent-23689715 [last accessed 12.05.2015]

4 Opening the black box – The inner workings Big Data

4.1 Data mining

Recalling the Big Data process outlined in chapter 2, the third and arguably most important step of extracting novel information from Big Data is the analytical process. To acquire new information and make inferences from the existing data, it is often necessary to combine different sets of data and cross-reference them in the search for patterns. For example, if an online retailer such as Amazon want to find out what fans of the *Twilight*-series are likely to be interested in buying, they can use data sets including age groups and geographical data, combined with data about individual purchase histories, and create a profile best suited to different demographics. Customers who fit the demographic will then receive recommendations based on the bracketed profile in which the algorithm has placed them. In the following I will go into detail about how such processes actually work, by describing a number of methods and algorithmic tools that are commonly used in predictive policing.

There are several different ways to analyze the massive amount of information that has been collected and stored. The best-known term used when referring to Big Data analytical methods is known as data mining. According to the Merriam-Webster Online Dictionary, data mining is "the practice of searching through large amounts of computerized data to find useful patterns or trends".[15] Data mining, then, is a process through which big sets of data are analyzed in order to produce patterns that were previously hidden. The inclusion of the word "computerized" is important, as it implies that the volumes of mineable data exceeds the capability of human cognition. For my purposes, I will be using "data mining" as a sort of blanket term for doing Big Data analytics by searching through data pools. Data mining can be done in a variety of ways, often depending on the sort of data one wants to analyze, the desired information to extract, and on the kind of algorithms used. Therefore, before starting the analytical process, it is important to recognize what kind of data one is dealing with. This

[15] http://www.merriam-webster.com/dictionary/data%20mining [accessed 03.03.2015]

will affect the choice of methods, and consequently the entire analytical process (Perry 2013, 69). In informatics, for example, it is becoming increasingly common to employ a technique known as *machine learning*. This is a form of artificial intelligence, which enables computers to learn certain behavior based on empirical data. Within this system, algorithms are used to accurately recognize and predict patterns within data streams, resulting in the computer learning how to deal with and solve irregularities as they appear by adjusting its behavior. This is used in systems such as the Netflix recommendation engine. The more movies you watch, the better the artificial intelligence will be able to predict what other movies you might enjoy, and decisions about proper recommendations are possible without much, if any, human interference.[16] Another frequently used model of data mining is *prediction analysis*, which revolves around predicting future behavior, likelihoods, and trends. In such a model, several so-called "predictors" work in tandem by weaving together data to assert a certain degree of possibility or probability. Prediction analysis is applicable to different units of analysis, from large-scale natural systems (e.g. a weather forecast) and down to an individual personalized level (Datatilsynet 2013, 15-16).

4.1.1 Turning inference on its head

One essential feature of a process such as machine learning, is the way that it changes conventional statistical inference. In traditional statistical inference, hypotheses are devised based on existing research. When working with machine learning tools, statisticians provide so-called "training data", which are examples of data sets. Through analysis of these training data, the algorithm identifies hypotheses by finding patterns in the data sets. In other words, rather than analyzing data from the basis of a hypothesis, the machine learning tool takes a bottom-up approach, creating the hypothesis from raw data.[17] After working with sufficient training sets, the algorithms are able to discern potentially predictive relationships within the data (Moses and Chan 2014, 648). The process is not, however, completely automated or autonomous. Human manipulation is a key factor in machine learning, as it takes a researcher

[16] Netflix detail their algorithmic approach in their tech blog, see for example Alvino (2015), at http://techblog.netflix.com/2015/04/learning-personalized-homepage.html [accessed 15.05.2015]

[17] The idea of Big Data allowing researchers to derive hypotheses from raw data is controversial. An often cited, although somewhat extreme example, is Anderson (2008). Anderson, Wired Magazine's editor in chief, claims that what he calls the "data deluge" signals that the scientific method has become obsolete. For a rebuttal of Anderson's argument, see for example Timmer (2008).

to select input, set device parameters, and otherwise make sure that the predictive relationships are accurate by cross-referencing them. There is always a selection process involved when data is analyzed, and there is bound to be a certain degree of inductive bias involved in deciding which elements should be treated as relevant. This human element of the process is an important part of most data mining processes, although it is often ignored when approaching Big Data as a mythological concept or buzzword.

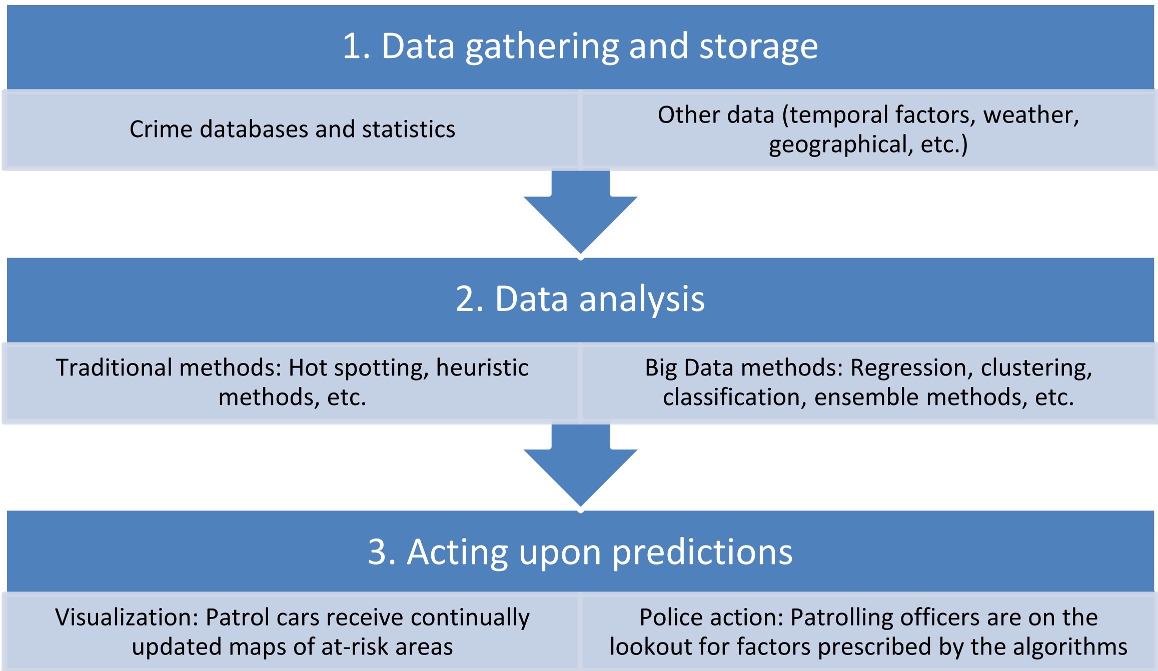

Figure 4: A simple representation of the process of data mining and its tangible results in a predictive policing context. Throughout the process, human interference may occur at all three stages.

4.1.2 Methods of data mining

In an investigative paper on the usefulness and applicability of governmental data mining, professor of law Tal Zarsky investigates the concept of data mining as a technical term. He defines data mining as a "(…) nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data." (Zarsky 2011, 291). This designation mirrors the dictionary definition, changing "computerized" into "nontrivial". He goes on to distinguish two different forms of data mining. What Zarsky calls "subject based" searches are database-searches directed at specific individuals, events, or predetermined patterns. This form of data mining could for example be used to identify a potential terrorist. Certain parameters are set up, and an individual's data are thoroughly explored and cross-referenced with matching profiles, indicating potential threats. The more widely used method of data mining consists of "pattern based", or "event based" searches. When engaging in pattern based data mining, the analysts do not predetermine any specific factors that the analytical process is going to use. They only define general parameters regarding the patterns and results they are looking for, thus defining what is acceptable when it comes to factors such as margins of error.

The process of data mining can be used to perform either descriptive or predictive tasks. When using data mining for descriptive purposes, it can help analysts better understand the information that is being analyzed. Trends and patterns that were previously hidden may be uncovered, and thus the algorithms can extract new information. In law enforcement, this method can for example be an effective way to discover certain patterns of behavior in ongoing cases, for assisting the police in understanding criminal behavior, and similar purposes. When data mining for predictive purposes, the analysts can generate new rules based on existing data, applying these rules to newer partial datasets. The data mining application uses a feedback loop, a variation of machine learning, to continuously learn new patterns, and can use these increasingly advanced patterns to recognize signs of repetition. Ideally, the algorithms will be able to project preexisting patterns onto incomplete or current datasets, thereby predicting (or more accurately, calculating the probability of) future behavior (Zarsky 2011, 292). In law enforcement, as demonstrated by PredPol, these algorithms can assist the police to act upon events before they happen, or for example to calculate the risks of probationer recidivism.[18] In the predictive model of data mining, the methods of prediction analysis and machine learning are working together to improve and further refine the algorithms and the predictive process.

[18] In Philadelphia an algorithmic tool is used to classify prisoners according to their projected risk of recidivism. See Ritter (2013).

4.2 The algorithms behind predictive policing

Let us now enter the black box of predictive policing, by examining a number of relevant algorithmic methods that are commonly used either individually or in combination. This will build upon the concepts introduced above, narrowing the methods down to those explicitly contained within the artefact that is predictive policing. For this purpose I will mostly be drawing on the RAND Corporation's report on predictive policing,[19] since it explains these complex methods in a structured and comprehensible manner. All of these methods have their roots in procedures used before the dawn of Big Data, but the increased processing power and reliance on large data sets have significantly changed their efficiency and practical usability to a degree where they can be considered novel approaches. In the process of identifying high-risk areas, several levels of analysis are being done.

Table S.1
Law Enforcement Use of Predictive Technologies: Predicting Crimes

Problem	Conventional Crime Analysis (low to moderate data demand and complexity)	Predictive Analytics (large data demand and high complexity)
Identify areas at increased risk		
Using historical crime data	Crime mapping (hot spot identification)	Advanced hot spot identification models; risk terrain analysis
Using a range of additional data (e.g., 911 call records, economics)	Basic regression models created in a spreadsheet program	Regression, classification, and clustering models
Accounting for increased risk from a recent crime	Assumption of increased risk in areas immediately surrounding a recent crime	Near-repeat modeling
Determine when areas will be most at risk of crime	Graphing/mapping the frequency of crimes in a given area by time/date (or specific events)	Spatiotemporal analysis methods
Identify geographic features that increase the risk of crime	Finding locations with the greatest frequency of crime incidents and drawing inferences	Risk terrain analysis

Table 1: An overview of predictive policing methods. Source: Perry (2013, xv)

[19] Cited as Perry (2013).

As the above table shows, hot spotting and near-repeat modeling are only two of the ways in which predictions are made. The main difference between conventional crime analysis and predictive analytics, is the sheer amount of data being analyzed. In this particular table, Perry (2013) uses the designators “low to moderate” to signify complexities that an analyst can comprehend and recall, while methods with “large” demands and complexity requires the assistance of computer programs and advanced algorithms in order to be processed. In other words, the tasks described below will in most cases be too complex to be performed without the technological tools that Big Data provides. As emphasized in the RAND Corporation’s report, it is important to recognize that none of these methods are meant to literally predict where and when the next crime will occur.[20] Instead, “(…) they predict the relative level of risk that a crime will be associated with a particular time and place.” (Perry 2013, 55). When reviewing these methods, it is important to remember that they do not give unfiltered access to the truth. They are artefacts that have to be adjusted based on the context of their use, either by a human analyst or by machine learning tools, and are thus subject to some degree of human manipulation.

4.2.1 Regression

The method of regression has been common in police work for some time, and involves finding mathematical relationships between the variables that one wants to predict, and with various explanatory variables (Perry 2013, 30). For example, a burglary may be related to previous crimes of a similar nature, but also to variables such as population density in the area, number of former convicts living nearby, and so on. In law enforcement, regression is used to calculate the statistical likelihood of crimes occurring, down to explicit numerical ranges. The method can be relatively simple, with only a few variables, or very advanced with a large selection of variables. A lack of sufficient variables may create inaccurate results, as may the use of incomplete data sets. However, as a general rule, it is assumed that as the sets of data included in a regression analysis grow larger, the predictions will be more accurate.[21] Selecting which input variables to use can be a challenge when working with the regression method. Simply including every possible variable may result in the output being dominated

[20] In the literal sense of the word “predict”. Perhaps “forecasting policing” would be a more accurate term.
[21] Note that this conflicts with Moses and Chan’s assertion that more data means more potential for error.

by random noise and coincidences rather than actual correlations. Selecting relevant variables can be done through manual adjustments and experimentation (human interference), or by employing further algorithms to strip away any variables that are deemed statistically insignificant. An additional important concept for regression models is called a leading indicator. Leading indicators, similarly to the aforementioned predictors, are signs with predictive value, which can be used to indicate for example in which direction crime is likely to move in the near future. A leading indicator can be a change in geographical factors (e.g. a new mall being constructed), a change of weather (fall is approaching), or even current economic climates (a recession is looming). By using these factors as variables, it allows law enforcement to be proactive rather than reactive. As traditionally used by the police, the method of regression is fairly simple and can be managed and maintained with analyst supervision.

4.2.2 Clustering and classification

The method of clustering is a form of data mining that uses algorithms to sort data into clusters, based on shared or similar attributes (Perry 2013, 38). When the data has been grouped into clusters, the algorithms work by identifying properties shared by members of a particular cluster, and finds mutual features that are significantly more common within a certain cluster than outside of it. By using large data sets, the algorithms can thus identify common features about crimes that might seem unrelated for a human analyst. These shared traits can then be turned into patterns, and applied to predictive models by projecting them onto future possible crimes. Clustering can thus be effective in identifying criminal hot spots, by for example uncovering variables in the environment that is shared with previously identified hot spots. The advantages that Big Data technologies provide are obvious when it comes to clustering methods. By sorting through enormous amounts of data in a relatively short time, computer-powered algorithms are able to uncover patterns at a rate and efficiency that no human analyst could hope to compete with.

Algorithms using the classification method work by creating rules that assign labels or classes to events (Perry 2013, 39). By using training sets of data, the algorithms learn (through machine learning methods) that certain patterns constitute a specific category of events, which can then be used to map possible or probable patterns of future events. A variation of the classification method is used by Philadelphia's Adult Probation and Parole Department (APPD) in order to predict the future behavior of parolees. By using a specifically tailored tool called "random forest modelling", the APPD use classification algorithms to categorize probationers as either "high", "medium", or "low-risk" (Ritter 2013). The categories are informed by data on the behavior of previous parolees, in addition to a variety of other variables. Similarly, classification methods can be used to categorize geographical areas as being at different risk levels. The learning mechanisms built into more advanced algorithmic models allow the models to adjust themselves based on both human input and on changing trends over time. By combining the classification method with clustering and regression methods, the random forest model is what can be described as an "ensemble" method. The increased computing power available in Big Data systems, allows for complicated ensemble methods to be used in tasks such as predictive policing, combining the modes of data mining outlined above in order to produce more accurate predictions. Sufficiently advanced combinations of methods become very difficult to fully comprehend or penetrate, and are consequently known as *black box methods* (Perry 2013, 36).[22]

4.3 Summing up

We now know the basic process of a Big Data analysis, with special focus on the process of data mining. Loosely defined, data mining is the procedure of searching through large sets of computerized data in order to uncover patterns and other correlations. In predictive models such as predictive policing, several methods of data mining are commonly employed, and with enough processing power, they can be combined to produce accurate predictions. By using regression methods, algorithms scan for patterns in order to find statistically significant correlations between criminal acts and other variables. The method of clustering involves

[22] Note the use of the concept "black box", which mirrors the concept of "black boxing" often used in STS literature. As detailed in chapter 5, the STS-concept of a black box means that a technology is being taken as a fact, and is thus withheld from scrutiny. Black box methods may similarly avoid criticism because they are too complex for potential critics to fully comprehend. The main difference between the uses of the term seems to be that in STS, "black boxing" often implies that information is deliberately obscured for political or other purposes. The way that Perry (2013) uses the term does not seem to involve any deliberate effort to hide information, but is rather a "natural" consequence of the complexity of certain technologies.

uncovering hidden shared features of different data, such as discovering that certain crimes that may seem unrelated actually share mutual key elements. Classification algorithms are used to categorize events based on rules discovered from analyzing data sets. Once rules have been established from scanning past cases or events, they can be employed in order to classify areas, individuals, or other entities according to the likelihood of certain events happening. By combining these techniques with visual mapping technologies such as Geographic Information System (GIS) technologies, predictive policing technologies have the ability to produce prescriptive courses of action based on existing criminological and other data. In other words, the process behind the technology can be very complex and contain a wide range of variables. The more complex the process becomes, the more difficult it might be to understand. As we will see, this has implications that go beyond the technological functions of predictive policing.

5 Theoretical basis

5.1 Science and Technology Studies

So far I have outlined the technological artefacts and processes behind Big Data and predictive policing, including the story of how the latter was developed and exploring its inner workings. Throughout this chapter, I will introduce and explain a number of theoretical concepts that will be central to the rest of my analysis. Drawing upon the field of Science and Technology Studies (STS), my aim is to present an alternative account of the process behind the technology. I will show how predictive policing contains aspects that are often obscured by focusing solely on the technology itself. Technologies such as predictive policing have a tendency to become impenetrable because of their complexity. If the artefact is not understandable for groups other than its inventors, they run the risk of becoming exempt for public scrutiny. However, policing technologies often affect larger segments of the population, and should therefore be assessed with its possible social implications in mind. In order to uncover these aspects, a STS approach will provide the backbone for a deeper analysis of the broader social context surrounding and embedded in the technology.

The field of STS contains a wide variety of theories, but my analysis will mainly be drawing on Actor-Network Theory (ANT) and the Social Construction of Technology (SCOT). Although the two approaches diverge in a number of ways, they share the general idea that social context is important when analyzing technologies, and that treating technological artefacts as independent from their sociotechnical context only provides a limited understanding. I will be focusing on the social constructivist aspects of SCOT, supplemented by the more process-based approach of ANT, especially when examining the formation and mobilization of social groups. In addition to emphasizing the interdependence of the technology, social groups, and actor-networks, I will demonstrate how technologies can embody certain political themes, taking inspiration from Dewey's theory of the public and issue-articulation. I will begin by introducing some key concepts from STS, before giving an overview of the theoretical literature on SCOT and ANT that I will be using. In the final part of the chapter, I will highlight some relevant discussions and criticism surrounding the theories.

5.1.1 Key concepts

Before delving further into the theory and methodologies of STS, it will be useful to define a number of key concepts that will guide the remainder of this thesis. Even presumably clear-cut and common notions such as “technology” and “social groups” are loaded concepts, and must therefore be seen in light of the theoretical literature. I will begin by presenting the perhaps most loaded term of my analysis, namely that of “technology”. In order to do this, I will draw upon the definitions put forth by the technology scholar Wiebe Bijker, who is often credited as one of the creators of the SCOT field. In SCOT, it is common to distinguish three different layers of meaning that are usually ascribed to technologies (Bijker 2006, 3). In everyday discourse, technology is used to denote physical objects, or artefacts, which have been created through human effort. When referring to a specific object, such as a smart-pad supplied with PredPol-software, this is the meaning of technology one evokes. Although this definition is the most commonly used when referring to technology in everyday speech, the concept is somewhat limited as it ignores most social aspects. The second layer of meaning of technology also includes human activities, including the act of creating, manipulating, and using technological artefacts. A patrolling officer receiving a tip about a possible crime hot spot from his PredPol-software is thus a part of the technology in this second sense of the concept. The same can be said of the programmer who is designing the software, as well as the technician adjusting its parameters, the chief of police working to implement it, and so on. In short, this perceptual level is concerned with the process involved in the creation and use of technology (Bijker, Hughes, and Pinch 1987, 4).

Finally, the third layer of meaning ascribed to technology also includes knowledge of the artefact and its processes. In this definition of the concept, understanding the algorithms behind predictive policing can thus be considered a part of the technology itself. Knowing what the machine or artefact does is only one basic level of understanding, however, and knowledge stretches far beyond being able to observe the machine’s input and output. In order to have a clear understanding of the technology that is predictive policing, one might have to understand the algorithmic functions, the categories of information that are being processed, how the resulting data is used, and more. Additionally, the concept of knowledge itself can be divided into different categories such as expertise, tacit knowledge, commonsensical knowledge, and a number of others.[23] As a side note, this means that it may be practically impossible for a single person to have a complete understanding of a sufficiently complex technological artefact. By acknowledging that technology encompasses both material artefacts, a process of development and use, and a broader set of knowledge, we may be better suited to undertake an analysis of predictive policing. By broadening the meaning of technology beyond the material object, it becomes clear that technology is embedded into a broader sociotechnical world.

5.1.2 Two ways of understanding technological change

Since I will be taking a social constructivist approach to my analysis, it is necessary to explain how this approach differs from a more traditional understanding of technological change. Bijker identifies two main conceptions of technological transformation, referred to respectively as "the standard image of science and technology", and "the constructivist image of science and technology" (Bijker 2006, 4-8). The "standard", or traditional view of science and technology was common in the study of technology before the 1980s, and is still a widely held belief amongst lay people, politicians, and even engineers. In this view, science is regarded as having special access to objective truths, and is therefore exempt from subjective judgments based on factors such as personal values and agendas. Consequently, technology is often seen as an extension of scientific knowledge, or applied science. Thus technological artefacts are primarily regarded as neutral tools, exempt from human bias. The artefacts are acted upon by users, who may have their own values and perceptions of the world, but these factors only exist separately from the technology itself. The artefacts in themselves, then, are regarded as following an independent path, and in the case of malpractice, one should blame the user rather than the artefact. When predictive policing is presented as being just another tool in the police arsenal, the standard image of technology is at play. This view of technology often leads to an acceptance of what Bijker calls technological determinism.[24]

[23] See Collins (1987) for a comprehensive overview of forms of knowledge
[24] For an overview of technological determinism, and the rise of STS as an alternative position, see for example Williams and Edge (1996)

Bijker sums up technological determinism as consisting of

> (…) two elements: it maintains that (1) technology develops autonomously, following an internal logic which is independent of external influences; and that (2) technology shapes society by having economic and social impacts. (Bijker 2006, 6)

This implies an understanding of technologies developing and evolving in relatively unproblematic ways, improving in efficiency for each new iteration. It follows that technological artefacts are on a rail-like trajectory, where it is useless or even foolish to attempt to interfere. In short, technological artefacts are seen as standing outside society, impacting the way we live while following its own path. Consequently, artefacts are put in a position where it is either too soon to foresee the consequences and implications of adopting them, or it is too late to intervene because the technology has been too entrenched in society to change it (Bijker 1993, 129).

In academic fields such as sociology and economics, the (often tacit) acceptance of technological determinism has resulted in technology being bracketed, or "black boxed". In other words, although technology is often acknowledged as having an impact on outside factors, the artefacts themselves are assumed to be opaque and therefore do not warrant further inquiry (Bijker, Hughes, and Pinch 1987, 21). This black boxing remains common and often unquestioned outside of academia, for example in politics, and also in everyday discourse. Rather than asking about the inner workings of particular technologies and how they can be adapted to societal needs, politicians may instead focus on how society may adapt to technologies. As we have seen, complex technological artefacts such as Big Data have a tendency to become black boxed. When the technology becomes impenetrable to non-experts, the temptation to just take the inner workings for granted and instead focus on the more familiar social aspects becomes greater. In this way, public discussion may be led away from the technology, and rather than asking "how does Big Data work?" or "how do we want Big Data to work?" the questions tend to veer towards "what is the best way to implement Big Data?". In this scenario, Big Data is an unstoppable train, and society is placed in a position where one either has to get aboard or be left behind (or worse, be run over!). Deliberately black boxing an artefact, thus silencing debate around it, can be an effective rhetorical technique for people who want to gain acceptance for their technology of choice.

5.2 SCOT: The Social Construction of Technology

A significant common factor of many STS theories involves the rejection of technological determinism. One of SCOT's central ideas can be briefly summarized as "technology does not follow its own momentum, nor a rational goal-directed problem-solving path, but is instead shaped by social factors." (Bijker 2006, 6). The social constructivist position holds that social context forms the ways that technology is created, and the ways in which it evolves. When analyzing technology from a SCOT perspective, emphasis is put on the idea that outside factors are constantly shaping how technological artefacts advance, and this means that one cannot easily point to any natural end point or superior solution for the technology. When technologies fail (meaning that they are discarded, abandoned, or discontinued), it is not necessarily because they are inferior to the "winning" alternatives, but rather because outside social factors "decided" on one alternative out of many, after a process of negotiation. In fact, even the idea of "success" is, as we will see, far from clear-cut in a constructivist view. The idea that technology can evolve along many different lines at the same time before a winning design is stabilized, is called a multi-directional view. With the multi-directional view of technological development in mind, I will outline some relevant aspects of a SCOT-analysis, using short examples from the case of predictive policing, which will be elaborated upon in the main analysis. A SCOT analysis consists of a three-step process:

> (i) sociological deconstruction of an artefact to demonstrate its interpretative flexibility; (ii) description of the artefact's social construction; and (iii) explanation of this construction process in terms of the technological frames of relevant social groups (Bijker 2010, 69).

5.2.1 Relevant social groups and interpretative flexibility

Since the SCOT theory poses that technology evolves concurrently with social forces, the first step of a proper analysis consists of deconstructing the technology, which is done by identifying relevant social groups. The concept of what constitutes a "relevant social group" can in itself be problematic, since different groups can be affected by a specific technological artefact in wildly different ways, individual actors may not know that they are implicated in a group,[25] and they are not limited to any single group. For the purpose of my analysis, however, more generalized groups directly affected by predictive policing, such as "the police", "minority citizens", and "civil rights advocates" seems adequate. I will be using concepts from ANT, detailed below, in order to explain the dynamic nature of these groups. The main reason for identifying relevant social groups is that different groups will have potentially quite different interpretations of what a certain technological artefact is, or what it is supposed to be. For the patrolling officer, predictive policing could be "just another tool" in her arsenal, a way to make her job easier, or a potential threat to her policing expertise. To a young black man living in Los Angeles, on the other hand, predictive policing could be one more source of agitation, resulting in unwarranted searches by the police, or it could be a way to reduce crime and thus make him feel safer.

This multiplicity of meanings given to the same artefact is what Bijker calls interpretative flexibility (Bijker 2006, 6). Interpretative flexibility, in short, means that the identity and meaning of an artefact, as well as what represents its apparent success or failure, is subject to its social context. This implies that an object that seems more or less unambiguous on the surface can be better understood as several different artefacts at once. These different artefacts are "hidden" within the one perceived "thing", but can be uncovered by looking at the relevant social groups and the meanings that they ascribe to the "thing" (Bijker 1993, 118). In other words, a concept such as "predictive policing" is not in itself much more than an empty shell or a designator. The emergent meaning and trajectory of the technology is largely dependent on outside social variables, and what may seem like "X" to one group could easily be construed as "Y" to another. A key for doing a successful STS-analysis, then, is to focus on the *process* of the social shaping, rather than fixating on the end product.

[25] Dewey writes that actors are implicated in a technology because they are either directly or indirectly affected by harmful consequences. With sufficiently complex technologies, however, it is not always possible to know that one is being affected. "(…) the machine age has so enormously expanded, multiplied, intensified and complicated the scope of the indirect consequences, (…) that the resultant public cannot identify and distinguish itself." (Dewey 1927, 126). Thus, it is possible to be a relevant stakeholder without actively pursuing such a role.

5.2.2 Stabilization and closure

Despite the flexible state of technology "in the making", usually at some point a common meaning or interpretation of a particular artefact is reached. The second step of a SCOT analysis involves exploring how the interpretative flexibility of a particular technology is gradually reduced, as the meanings ascribed to the artefact converge, and some artefacts and interpretations gain dominance over others (Bijker 2006, 6). In SCOT, this process of meanings converging, or being agreed upon, is known as stabilization. During the course of this process, involved actors and groups will negotiate and attempt to establish the technology in their own image. Stabilization does not happen overnight; it may take years of similar artefacts competing, or the meaning of one artefact being disagreed upon, before meanings converge. It's important to recognize that stabilization is a gradual process, and a matter of degrees. Thus the freedom of choice concerning different alternatives and meanings of artefacts will gradually narrow. Once a winner has emerged, the technology has achieved closure. When an artefact is closed, a sort of point of no return has been reached.[26] The history of the technology is often retroactively written to fit a linear or deterministic model, resulting in a misleading notion that the current version of the artefact is the best possible version (Bijker 1993, 122). In regards to predictive policing, there are still potentially competing technologies under development, although the main concept seems to be stabilizing. The controversy now appears to revolve around the implementation of the technology, and whether it should be implemented at all. To summarize, stabilization is a gradual process in which relevant social groups negotiate or struggle to shape the artefact in their own image. As the process continues, some meanings will usually gain ground (by for example enrolling other actors to their cause, mobilizing resources, etc.). Thus the interpretative flexibility of the technology is gradually reduced, until a winner emerges and the artefact reaches closure.

5.2.3 Closure mechanisms

There are several ways in which technologies can achieve closure, and the main common factor is that this does not happen on purely technical merits, or as the end result of some

[26] As will be shown, closure is not an irreversible process. If new social groups or meanings form or gain power, artefacts that were "closed" may be reopened for further negotiations.

predetermined path. In their 1984 paper *The social construction of facts and artefacts*, Pinch and Bijker identify two main ways that closure may occur. The first one of these, rhetorical closure, involves the artefact being accepted as a sufficient solution to some perceived problem. Predictive policing, for example, is regarded by many of its proponents as a solution to problems such as officers often not being at the right place at the right time, allocation of limited police resources, and similar issues. As Pinch and Bijker point out, however, when it comes to technological closure, what counts as an actual "solution" of a problem is never clear cut. The most important factor is that some of the relevant social groups *perceive* the problem as being solved (Pinch and Bijker 1984, 427). Advertising is one important way one can achieve such rhetorical closure, by for example coming up with a solution to a problem that might not have existed in the first place. A technological controversy can thus reach closure by enough groups being convinced that accepting the artefact in question is in their best interest, poses no threat to their way of life, etc. However, as we will see, in many cases social groups do not even agree on the kind of problems an artefact is meant to solve.

Pinch and Bijker's second closure mechanism, called closure by redefining the problem, entails a group or actor putting forth a new problem that should be solved, rather than directly addressing the originally presented problem. One way that this can happen is by "moving the goalposts", so to speak, meaning that the groups/organizations/actors with vested interest in a certain technology being a success, shifts the focus of the discussion away from criticism raised by their opponents. In this way, a debate about "could predictive policing be a civil rights issue?" can transform into "how can predictive policing be made more accurate?". The former issue then achieves a kind of quiet closure by going ignored, and the latter question might reach closure by using existing technological solutions such as improved algorithmic tools. As we will see, this closure mechanism is often used as a way to silence public debate, redirecting the focus away from potential controversial topics. Conversely, groups may open up less controversial technologies by focusing on potentially harmful consequences.

5.3 The formation and mobilization of social groups

The third step in Bijker's analytical approach entails explaining the social construction of technologies by reference to technological frames. At this point I will diverge from the traditional SCOT approach, as the concept of technological frames is mainly focused on the structural aspect of social groups. SCOT does not go into much detail on the process of how these groups initially form and gain momentum. This group formation will often be a key factor in deciding the outcome of a technological debate; superior numbers lends a certain strength to many arguments. Therefore I have chosen to eschew the concept of technological frames, instead drawing upon ideas from the actor-network theory (ANT) in order to explain the process of group formation. In his 1986 article *Some Elements of a Sociology of Translation*, Michel Callon describes how social groups, or actor-networks, are formed around technological artefacts, through deliberate action from certain system-building actors.

The process where different actors or groups interact around an artefact, is called translation. During this process, identities, knowledge, and the possibilities for action are continuously renegotiated and redefined (Callon 2007, 59). The process of translation can be divided into four steps, or "moments of translation", which may occur either chronologically or to some degree overlap. The first step Callon describes is called problematization. Problematization involves a double-movement, where an actor or group attempts to define a certain problem which must be solved, and at the same time establish themselves as indispensable when it comes to finding a solution. This means that the system-building actors seize the technology, in an attempt to take control of the situation and secure their own role in the process. Similarly to the SCOT-concept of closure by redefining the problem, the system-builders thus attempt to demonstrate that there is a clearly defined problem that needs to be solved, and that they hold the key to the solution. By positioning themselves as keepers of the solution, the system-builders take the role as an obligatory passage point. Obligatory passage points are, as the name implies, a node in the sociotechnical network that all further translation and interaction needs to pass through. In other words, problematization lets the system-building actors anchor themselves as an indispensable part of the process, and other actors in the network have to collaborate with or surrender to the system-builders if they want access to the solution.

The process of problematization invariably involves certain actors submitting themselves to other actors. Because this is can be a problematic process, additional steps must be taken to ensure the stability of the group that is being formed. The second moment of translation, which Callon calls interessement, is concerned with making sure that the alliances that are being forged remain stable (Callon 2007, 62). As we have seen, social groups are heterogeneous entities, and may therefore be vulnerable to internal conflict. In order to impose a common goal or meaning, the leading actors may employ certain devices or mechanisms in order to sever ties to outside factors that could threaten the stability of the group. This means that the process of interessement involves an attempt to close off other venues of debate within a group, tightening the focus towards the narrative represented by the system-builders. One way of achieving this is by separating the actors and the problems of the group from their broader context. The UCLA researchers transformed or reframed the question of crime, from being regarded as a social problem, to a statistical or mathematical problem. This reframing of the problem serves to removing issues such as ethics from the equation. Thus, the problem is translated into a language with its own set of rules and accompanying solutions. Thus, interessement brings the different actors together under the language of the system-builders. The issue at hand, crime-prevention, becomes molded to fit the narrative of the researchers, and the artefact of predictive policing becomes a means of interessement; a way to shape the identities of the involved actors in the emerging social group.

If the interessement is successful, the third moment of translation may proceed. As the social group in favor of predictive policing is stabilized, the broader question of “how can Big Data be used to prevent crime?” is transformed into more specific and definitive statements such as “Predictive policing is an effective way of preventing crime”. Once the social group has become established and stabilized, the next step requires what Callon calls enrollment. This includes negotiating the roles of the actors within the network, further solidifying identities and choosing representatives. Actors can be enrolled in a number of ways, including by persuasion, seduction, and even by force. Law enforcement organizations may be persuaded that predictive policing is the answer to their prayers, while actors such as politicians may be convinced that focusing on new technologies is an advantage during an election year. Some actors may be silenced, by outsourcing their voice to a representative or to the group as a whole. The main point of the moment of enrollment, however, is that even though a group has been formed, the process of negotiating roles and identities continues.

5.3.1 Mobilization

As the social group or actor-network is stabilized around an artefact, the final moment of translation follows. Mobilization is the process in which many heterogeneous actors turn into one articulate actor, through a process of representation. This means that as the actor-network mobilizes, many voices are substituted with a singular clear voice. A piece of software such as PredPol is the product of many theories and individual actors, thus the artefact in a way embodies and represents a large group of actors and ideas. However, rather than speaking of resources, politics, or crime prevention, the artefact only communicates easily transferable numbers; statistics, probabilities, and geographical locations. Through this manner of representation, all of the actors or stakeholders of the group are being mobilized in an easily communicable and unambiguous manner (Callon 2007, 72). The variety of original messages and goals that constituted the "Big Data for crime-prevention"-network have been synthesized into simple statements that are easily packaged with the technology. "Predictive policing has reduced crime by 20%", "Predictive policing will improve police efficiency by 15%", and similar statements now represents the social group favoring the technology. The eager policeman, the statistician, the politician, and the concerned citizen have all been displaced from their physical realities, and reassembled in the form of the technological artefact.

Summing up Callon's point, we can now see how new social groups are formed and stabilized around technological artefacts. Similarly to how interpretative flexibility decreases as social groups converge, the process of translation involves the gradual reduction of many actors into a singular group, represented by a technological artefact. A general question or problem is gradually translated into concrete statements, enrolling and shaping actors as the statements are become more definite. In the process, certain actors (or system-builders) will take control over others as obligatory passage points, and shape the problems and solutions in their own image. Again, one can notice a certain resemblance of the negotiation between groups and artefacts; closure mechanisms are at work both in the process of group-formation, and when a social group attempts to stabilize an artefact. This is indicative of the ways that social groups/networks and artefacts continually shape and constitute each other.

5.3.2 Summing up the theories

Summing up what we have seen so far, the SCOT method involves several distinct analytical steps. On the most basic level, it looks at the artefact itself, by opening the black box and examining the inner workings of the technology. After this is established, the interpretative flexibility of the artefact becomes the main focus of study. In order to understand how one artefact can be construed in different ways, it is important to identify relevant social groups, since these groups will assign their own meanings to the technology. Interpretative flexibility therefore becomes a way of demonstrating how one artefact can actually be understood as a series of different artefacts. Once relevant groups have been identified, the attention turns back towards the artefact, by examining how the technology stabilizes. This can be done by tracing the process of negotiation, uncovering how interpretative flexibility diminishes as different meanings begin to converge. In this process, some artefacts or social groups gain dominance, and by employing closure mechanisms they will attempt to shape the technology in their own image. By establishing themselves as obligatory passage points, some actors use technology in order to enroll other actors and thereby gain momentum. Thus, a technological artefact such as predictive policing is not only a material object; it also becomes an anchoring point where different social groups are drawn together and represented by the artefact itself. By uncovering this process, it is possible to demonstrate how technology develops in one direction rather than another, how the involved actors negotiate the technology and their own roles, and ultimately how the technology embodies certain social relationships and is inseparably embedded in a sociotechnical context.

5.4 Criticisms of SCOT and how to address them

With SCOT and ANT as a theoretical basis, the stage seems clear for a comprehensive sociotechnical analysis of predictive policing. Before embarking on the main analysis, however, I want to highlight a few points that often materialize when discussing STS. I will also suggest using Dewey's philosophy as a way to address one of these problems, and to bring politically charged issues into my analysis. One aspect of social constructivism that warrants further scrutiny, is its supposed relativism. The interpretative flexibility of artefacts seems to imply that one can never make value-judgments about the technology in itself. If one accepts that predictive policing could be interpreted as a means of oppression, yet also as a potential tool of equity, social constructivism appears to lack the proper tools to weigh one interpretation over the other. In a situation where existing power structures mean that one social group's interpretation can be forced through, or opposing voices are silenced, the SCOT-scholar could be sitting idly by and simply documenting the forming of the technology without regard to existing power structures. This relativistic distancing might not be inherently undesirable. As part of an analytical discipline, it is not outrageous for a researcher to avoid "taking sides". In a case where implications are made regarding policy and legislation, however, it seems difficult to avoid any sort of politicizing in the analysis itself.

Langdon Winner has criticized SCOT specifically for what he views as its disregard for the social consequences of technical choices. By focusing on the process of innovation and on how technological advances are made, SCOT runs the risk of missing the broader question of why and how technologies matter (Winner 1993, 368-369). Winner goes on to problematize the concept of relevant social groups, pointing out that the constructivist position lacks the means to distinguish any boundaries for determining which groups should be considered relevant. Technological debates and questions in themselves are not given, and certain groups have the power to define the questions while others are silenced. It is not simply a matter of being affected by the technology in question, but also of possessing the resources to mobilize. Perhaps somewhat harshly, Winner sums it up thusly: "Interpretive flexibility soon becomes moral and political indifference" (Winner 1993, 372). What is missing in social constructivist theories of technology, he suggests, is the ability to take a stand on not only how a technology developed, but also whether it ought to be developed. Similar issues regarding the perceived political relativism of SCOT has also been raised by technology scholar Stewart Russell (1986), who points out that the acceptance of social constructivism may prohibit any form of political normativity.

These criticisms against the SCOT-program bring up some relevant points that I will address before proceeding to the methodological chapter and my analysis. The most straightforward response to the problem of relativity is concisely addressed by Bijker himself, who stresses that any relativism in the social constructivist framework is strictly methodological (Bijker 1993). Despite the SCOT-method not coming "pre-packaged" with an ethical framework, it is not inherently opposed to or incompatible with taking a normative stand (Bijker 2010, 64). There are therefore no contradictions in analyzing technologies as socially constructed, while still recommending a course of action for technology policies or similar political action. Examples of combining SCOT with existing ethical programs exist, for example by choosing a pragmatist approach (Keulartz et al. 2004), classical virtue ethics, or alterity ethics (Steen 2014).

5.5 Dewey, the public, and issue-articulation

The idea that technologies are inseparable from the social and the political, implies that artefacts might provide some insight into the formation of political issues. Borrowing some ideas from John Dewey's *The Public and its Problems*, it can be shown how publics (and consequently democratic processes) form around particular issues. Since issues often arise around new technologies, a closer look at the process involved in negotiating controversial technologies may allow some insight into the democratic process. In her 2007 paper *The Issues Deserve More Credit*, Noortje Marres brings Dewey's theory of the public into a modern setting, applying his theories to a STS context. Dewey himself saw the public as an expression or movement that takes place when enough individuals are impacted by the harmful consequences of technologies.

> (…) the essence of the consequences which call a public into being is the fact that they expand beyond those directly engaged in producing them. Consequently special agencies and measures must be formed if they are to be attended to; or else some existing group must take on new functions. (Dewey 1927, 27)

When such consequences occur, actors who would otherwise stay uninvolved become implicated in the technology. In a modern setting, this could happen for example as a result of profiling on the basis of predictive policing, which might impact certain groups more than others. In order for public involvement to take place, however, an issue first needs to be properly articulated (Marres 2007, 768). Dewey proposed that when issues in modern societies become too complex to be solved by existing institutions, public involvement is required in order to settle them. Whereas “simple” problems are easily understandable and can be handled by public representatives and institutions, more complex technologies give rise to issues that must be solved differently; they require a public (Marres 2005, 7). As controversial issues arise, institutional procedures regularly fail to present a solution that is satisfactory to all parts. As Marres puts it, “the role of the public is to articulate issues that have insufficient institutional support, while also requiring political settlement.” (Marres 2007, 771). In other words, the public might be formed as a means to contest issues, and therefore opening them up. Without the formation of a public, such issues might fly under the radar, without being properly addressed by existing institutions. The formation of a public and the articulation of an issue is therefore a sort of double-movement. This way of opening up the issues for outside involvement, could potentially serve as a pragmatist alternative to a more technocratic method; where the technocrats would “railroad” technologies into use by referring to a concept of the common good, pragmatists such as Dewey sees the public as a means to actually solve complex problems in a democratic way.

The point of bringing Dewey’s theory into this account is that by focusing on the issue, it appears that certain technologies may be articulated either as an “open” democratic issue, or as a “closed” entity where the public is left out. The opening up of an issue means that the irreconcilability of certain views and interests contained within an artefact are highlighted. If it is acknowledged that some associations within or surrounding the technology are mutually exclusive, for example if surveillance technologies represent a clash between liberty and security, a controversy forms, and a public consisting of concerned actors and groups may form. This resembles the SCOT-characterization of relevant social groups, but with one important addition. By focusing on the formation of the issue, Dewey acknowledges that it is also possible to articulate issues to deliberately exclude public involvement, for example through propaganda and advertising. “Whatever obstructs and restricts publicity, limits and distorts thinking of social affairs.” (Dewey 1927, 167). Consequently, if an issue is articulated by leading attention towards aspects of a technology that are uncontroversial, the potential conflicts and harmful consequences of the technology are obscured. In effect, it becomes a non-issue (Marres 2007, 772). The role of the public therefore also involves disputing such de-publicizing of issues, bringing in interests that might otherwise go unspoken or unheard. As I will return to in chapter 7, this way of articulating an issue by highlighting potential conflicts and thus allowing a public to form, leads us back to the broader context of the sociotechnical. By going from the material object, to the social groups, and on to the formation of issues, one can capture the artefact from a material, a social, and a political side, seamlessly moving between these. The articulation of an issue in the context of a technology, reveals the political aspect of technological change.

5.6 Aims of the analysis and contributions to the field

Before moving on to the methodological and analytical chapters, I will give a brief recap of my aims with this thesis. As shown, SCOT provides a theoretical framework in which technology is studied in symbiosis with the society in which it exists. As predictive policing is still very much a technology in the making, it provides an interesting and timely subject to which the SCOT method can be applied. Since it is a technological artefact that can be explicitly tied to a major governmental institution (law enforcement), and which includes direct social consequences as one of its goals (reduced crime), the politically charged dimension of the technology is immediately clear. In light of Dewey's theory of the public, we can see that predictive policing represents a controversial technology that gives rise to questions that stretch beyond arguing whether it is functional or not, and it may therefore represent a public issue. Drawing on Callon's description of the actor-network, I will be using concepts from ANT in order to further illustrate the process of group-formation. This will ensure that I am better equipped to identify how these groups ascribe various meanings to predictive policing. Consequently, I will attempt to uncover the closure mechanisms or techniques the groups in question utilize, in an attempt to establish or close the technology in their own image. By tracing these competing ideas and the formation of social groups back to the concept of issue-formation and the public, I hope to cast light on why artefacts as complex as Big Data have the potential to raise more questions than they answer, and on how such artefacts present issues that might warrant public involvement. Bucking the trend of buzzwords such as "data revolution", I aim to contribute to a more nuanced and socially conscious conception of data mining and its proposed "catch-all" solutions.

6 Methodology and empirical material

6.1 Case study

In this chapter, I will describe and outline the choices I've made regarding my use of methods and source material. Drawing upon the methods outlined in Yin (2009), I will be taking a case study approach to my analysis. The advantages of a case study method are many, especially when studying a contemporary multi-faceted process rather than an isolated or historical phenomenon. When applying STS-theories to a case study, the lines between the phenomenon under inquiry (predictive policing) and its broader context will be blurred, as technology, social groups, and political issues all become entangled in a sociotechnical web. As a result of this heterogeneity, my empirical material is taken from a broad variety of sources. The case study approach allows for drawing these widely differing sources together, in order to present a more complete and nuanced picture of the phenomenon (Yin 2009, 16-19). Bijker (1993) recommends using a descriptive model which takes the technological artefact as its center, and consequently my analysis will revolve around predictive policing itself.

In order to provide a comprehensive STS-analysis, it is important to open the black box of the technology by giving a description of its inner workings. Subsequently, however, it is vital to return to the outside of the box, revealing the co-constitution of the artefact's inner workings and broader social processes. In other words, I want to maintain a balance between the "hard" technological description, and a broader analytical distance, to preserve the value of the case study for cross-case comparisons (Bijker 1993, 119). Chapters 2-4 have covered the main technological description, and I will dedicate the majority of the following chapters to analyzing the sociotechnical aspects of predictive policing. Reviewing the available information and sources related to predictive policing, the formation of certain social groups reveals itself. Recalling Winner's criticism of SCOT, it is important to remember that the published sources do not necessarily show the whole picture, as some voices may not have the resources required to mobilize. Callon's theory of group-formation may explain how some actors are silenced by delegating their voices to representatives, or surrendering to obligatory passage points. By keeping this in mind, a reflexive approach should be possible, although my main focus will be on the "main players", so to speak. Building upon the STS theories presented in chapter 5, the following section will elaborate on my choices of analytical focus points, and provide a short overview of my empirical sources.

6.2 Analytical focus

At the outset of my project, I had originally planned to look at the phenomenon of predictive policing within a predominately Norwegian context. In the wake of the terror attack at Utøya in 2011, the Norwegian police have been under pressure to modernize and improve their methods, particularly regarding communication and technology.[27] By allocating more resources to novel policing technologies, the use of Big Data for policing purposes was put under consideration. After a cursory exploration of existing debates, however, it became increasingly clear that Predictive Policing is not much more than a subject for the water-cooler at Norwegian police institutions. The Norwegian Data Inspectorate (Datatilsynet) have looked at the potential for the technology (Datatilsynet 2013), and representatives from IBM have pitched the idea to the Oslo police department (Inderhaug 2013), but there is little available information suggesting that predictive policing is about to be imported to a Norwegian context. Through personal correspondence with the Norwegian Council of Technology (Teknologirådet), I have been made aware that a Norwegian report on predictive policing was being finalized in 2014, but as of yet it remains unpublished.[28] When the report is published, and if the technology becomes more common beyond the pilot project areas, predictive policing might become a hot topic also in Norway. With little time to wait around for a more pronounced Norwegian debate, however, I turned my focus towards the American police districts where predictive policing is already in use.

As I have already described, predictive policing has been launched as a pilot project in several police departments in the US and in Britain. Since the technology was both developed and is being tested in California, more specifically in Los Angeles and its surroundings, I turned my

[27] For the complete evaluation, see Politidirektoratet (2012)
[28] As of May 2015, there is still no sign of the report. To my knowledge, Teknologirådet are aiming at publishing their report on predictive policing during the summer 2015.

interest there. This shift of geographical focus came with the advantage of letting me move rather seamlessly between the actual development of the technology and its practical application. By using SCOT and ANT as a theoretical basis, I wanted to explore how the discussion around predictive policing has evolved along with the technology itself, and uncover the ways in which social groups are formed and mobilized as they attempt to stabilize or destabilize the artefact. Being situated in Oslo, I chose not to pursue interviews and similar methods of gathering data. With the exception of talking to a representative from the Norwegian Council of Technology,[29] I decided that existing reports and articles would provide me with the information I needed to meet the goals of my thesis. With predictive policing drawing considerable interest from academics and journalists alike, from countries including the US, Australia, and Israel, there was no shortage of information and opinions, especially considering the relatively narrow use of the technology. In the end, I believe that my thesis is better off for focusing on the American setting, as it allows for a broad variation of voices and perspectives that simply would not exist if I had concentrated on Norway.

6.3 Analytical approach

Following Bijker's suggestions, I have devoted considerable time and space to understanding how Big Data technologies works, and especially to the functions of predictive policing. As noted, several levels of meaning may be assigned to any form of technology. Existing at the most basic level is the technology as a pure material artefact. Here one finds the infamous black box; a technological artefact as advanced as Big Data can seem impenetrable at first sight. In the previous chapters, I have attempted to outline the inner workings of the algorithms in an understandable manner. My focus in the following analysis, then, will lean towards the other two conceptual levels of technology, concerning myself with the process of technology in the making and the way in which actors and groups identify and constitute themselves in relation to the artefact. Following the SCOT approach, my analysis begins with identifying relevant social groups and the ways in which they relate to the technology. It is

[29] This correspondence and meeting helped me attain an overview over the situation of predictive policing in a Norwegian context (which is, as noted, sparse), and gave me pointers on fruitful ways to approach the technology. As the correspondence was informal, I have not used it as a direct source for my thesis.

through the perception and meanings assigned by these groups that the different facets, or the interpretative flexibility, of the technology reveals itself.

Bijker recommends taking technologically controversial artefacts as a point of departure, noting that "(…) instability is more revealing about a system's characteristics than stability" (Bijker 1993, 119). Points of disagreement, not only about solutions, but about which problems the artefact is meant to solve, is a fertile venue for exploring the process of the social shaping of technology. Since social groups are shaped in their interactions around the artefact, the mapping of prominent actors who are participating in the discussion is a useful first step. In a departure from the SCOT method, I have chosen to focus on the process in which actors form and mobilize through social groups. Drawing on ANT, specifically the theory of group formation presented by Michel Callon, I will identify key actors who act as system builders, and look at how they mobilize in order to shape the debate (and consequently, the technology itself).

Identifying and exploring the key actors and social groups, meaning those playing important roles in the shaping of predictive policing, will constitute my first research question. For this purpose, I have reviewed papers from criminologists[30], professors of law[31], public policy researchers[32], and communication scholars[33]. This variety of points of view have allowed me to reach a broader understanding of the different facets and perceived problems of predictive policing, and by paying attention to frequently cited articles, some main actors have revealed themselves. I have also examined articles published in police journals[34], press releases and other material from commercial actors[35], news articles, and interest groups such as human rights and civil liberties organizations.[36] By tracing the different arguments and the ways that social groups mobilize around the technology, I aim to answer my second research question, namely identifying which closure mechanisms are being used in attempt to stabilize or

[30] For example Willis and Mastrofski (2011), Byrne and Marx (2011)
[31] Zarsky (2011), Ferguson (2012)
[32] Yiu (2012)
[33] Moses and Chan (2014)
[34] Beck (2009), Inderhaug (2013)
[35] IBM (2012), PredPol (2014)
[36] PrivacySOS (n/d)

destabilize predictive policing. Finally, I will bring the conceptual level up to a broader political context, drawing on Dewey's theory of the public, which constitutes itself when conflicting issues arise in a technological artefact. This constitutes my third research question; in which I explore how political issues are embedded in technologies. By answering these three research questions, I will have covered the technological, the social, and the political aspects of predictive policing, demonstrating how they are all constituted around and embedded in the artefact.

6.3.1 Choosing which actors to follow

When analyzing technology as a sociotechnical phenomenon, where actors, technologies, and groups negotiate and co-produce each other, it is easy to become entangled in a problem of extension. Put bluntly, despite the rather broad and expansive concept of "relevant social groups", an analysis must have a boundary, even if such bounds may be artificial. There will therefore always be some form of reductionism in a sociotechnical analysis, if only because papers must have an end. Although one major aim of studying sociotechnical ensembles is to go beyond the reductive explanations put forward by technological determinism and social reductionism, an analysis with no reductive properties whatsoever will inevitably lapse into indiscriminate empiricism. As Bijker points out, however, reductionism should not be taken as something inherently negative, and when doing an STS analysis, it is not unusual to set aside or bracket some parts of the sociotechnical web, regarding them as fixed entities for the sake of the analysis (Bijker 1993, 127). By leaving these fixed sociotechnical worlds in the background, one can focus on the main objects of interest without getting caught up in an endless descriptive analysis where everything is up for debate. I will therefore regard institutions such as "civil liberties organizations" or "law enforcement" as a more or less coherent organizations with fixed goals, despite this not being a completely accurate reflection of the internal reality of the institution. In other words, when networks have stabilized as successful entities, they in a sense become a black box themselves. The network or group is represented under the shared flag of the institution itself, which translates its variety of voices and goals into one coherent entity (Callon and Law 1997, 174).

6.4 Personal positioning and source-criticism

Before continuing to the analysis, a few words about my personal position in regard to the case study are in order. When immersing oneself in a controversial technology, it can be difficult not to let personal opinions or beliefs color ones perception. Going beyond the purely technical aspects of predictive policing, one inevitably encounters perspectives that may seem disagreeable or even dishonest. In such situations, there are two main challenges which must be met. Most obviously, a healthy dose of source criticism is in order. Technologies that could potentially infringe on civil rights or be construed as surveillance-technologies, often appear to incite arguments based on emotions rather than facts. Although emotional arguments are an integral part of interpretative flexibility, one must draw a line somewhere. During my research, I have encountered potential sources ranging from propaganda pieces to borderline conspiratorial blogs. Filtering the relevant from the dubious was a necessary step from the beginning of the process. After all, a STS approach encourages keeping an open mind, but not so open that the noise outweighs the legitimate content. I have made a conscious choice, however, to include articles that are explicitly part of a marketing strategy as sources.[37] This provides a good example of how agents with vested economic interest may attempt to seize an artefact and close the debate on their own terms.

As for my personal position, I have made an effort as a researcher to distancing myself from any personal bias or beliefs, to the degree that this is possible. By letting the sources speak for themselves, a clearer picture of how social groups are mobilized, changed, or maintained appears. It seems suffice to say that throughout my analysis I will attempt to put each social group on even footing, and that dichotomies such as right/wrong or good/bad will only be present in cases where the actors themselves explicitly employ them as part of their strategies. I have stated that one of my aims is to demonstrate how certain technologies should not be evaluated on a solely technological basis. Although this in itself might reveal a certain partiality towards a social constructivist perspective, I believe that the variety of opinions presented in the following chapter will sufficiently back up my view.

[37] Most notably the official PredPol website, which lists a long range of endorsements for the technology.

7 Analysis

7.1 Introduction

Following up on the ideas introduced in the previous chapters, I will embark on my analysis by applying theories and concepts from STS, to the empirical material outlined in chapters 2 and 3. One of my overarching goals with this thesis is to demonstrate how technological artefacts are not in possession of some determined or “natural” form, but are constructed as part of an ongoing social negotiation. Through looking at artefacts, individual actors, groups, and political issues, I aim to show how technological artefacts are inseparably embedded in a sociotechnical world. If artefacts are socially constructed, it seems to follow that technologies should be considered from multiple points of view before being implemented, particularly when it comes to technologies used by governmental or public institutions. Additionally, perhaps approaching technologies from a sociotechnical perspective may serve to uncover underlying political issues, issues which could even be explicitly articulated in the technology itself. Through deconstructing predictive policing as a seamless web of material, social, and political factors, I will demonstrate how there is no single “correct” way to define a particular technology. In order to demonstrate the interpretive flexibility of predictive policing, I will identify certain important actors who take on the role of system-builders. This means that as the technology develops and is negotiated, actors will attempt to form and mobilize social groups, as a way of gaining support for their interpretation. By positioning themselves as obligatory passage points, these actors secure their roles in the proceedings, while representing and translating other individual actors into one coherent faction.

Returning to my research questions, this means that I will be looking at three different aspects, which are all inseparably embedded in the technology that is predictive policing. These are the artefact itself, the actors and social groups who negotiate and relate to each other around the artefact, and the political issues that are be articulated in and around the technology. By highlighting all of these aspects, I aim to demonstrate that technologies such as predictive policing cannot be evaluated on the basis of one context alone; a mix of perspectives is needed in order to properly understand the technology and its possible consequences.

7.1.1 Structure of the analysis

The structure of my analysis will involve a combination of concepts from SCOT, accompanied by ideas from ANT about how social groups (or actor-networks) are formed and maintained. I will dedicate a section to each of the relevant social groups, describing the process of how they are mobilized and the ways in which they understand and relate to predictive policing. Since the groups differ in many aspects, my approach will also be adapted to better suit the key actors. For example, the law enforcement group is more of a group in the traditional sense, while some of the legality-focused groups are represented by a single actor writing reports on the subject. This means that I will spend more time focusing on the formation of the actor-network in the former case, whereas for the latter I will mainly concentrate on the issue-articulation taking place. Using examples from my empirical material, I will trace how these groups have attempted to shape the debate surrounding the technology according to specific narratives. By defining a number of important actors and social groups, I aim to uncover which closure mechanisms these groups are employing as they try to steer the technology. As there has not been a very pronounced public debate about predictive policing, my main sources will be academic papers, press releases, and newspaper articles. The articles have a tendency to represent only one point of view, and some of the sources directly contradict each other. These points of contention provide a venue for exploring the broader political issues that are being articulated through the technology and the debate surrounding it. By outlining the seemingly insoluble conflicting views, I want to conceptualize the ways that certain issues are articulated and embedded in the technology itself, for example by being explicitly codified in the algorithms.

As a point of departure for my analysis, I will broadly define the relevant social groups as being either in favor of, or against predictive policing. This is, of course, a simplification, and for the sake of accuracy I will further subdivide the groups according to the main focus of their arguments. I will draw inspiration from the divisions made by Moses and Chan (2014).

In their discussion of the pros and cons of using Big Data for law enforcement purposes, Moses and Chan make use of a three-dimensional framework in order to examine the usefulness and acceptability of the technology. They address the functionality (technical), likelihood of take-up/diffusion (social), and the normative dimension of the technology. This framework seems to work well with the STS concepts of interpretative flexibility and the actor-network, and Moses and Chan specifically note that it is necessary to recognize the social context and influences if one wants to comprehensively analyze a technological artefact (Moses and Chan 2014, 652).

7.2 The technological argument

As noted in chapter 5, the concept "technology" can be separated into three different layers of meaning. The everyday use of the term concerns itself with the artefact itself, for example as a machine that performs one or more specific tasks. In this view, the success of a certain technological artefact mainly depends on its efficiency and accuracy when performing the tasks that it was designed for. In this section, I will show how some social groups interpret predictive policing on predominantly technical terms. If predictive policing performs as well as its proponents are claiming, then, according to this view, that in itself should be a sufficient reason to adopt it. On the other hand, if the inner workings of the artefact are concealed or if the tool is unsuited for its job, it might be regarded as a failure and be discarded. In defining predictive policing on solely technological terms, the following groups attempt to shut out other venues for discussion. I will begin by looking at how law enforcement officials are mobilizing in order to define predictive policing based on its technological merits.

7.3 Predictive policing as a tool: The law enforcement perspective

One of the most widely cited articles in the discussion surrounding predictive policing is taken from the magazine *The Police Chief*, which is published in collaboration with the International Association of Chiefs of Police. The article, which is written by Charlie Beck[38]

[38] Chief of Detectives, Los Angeles Police Department

and Colleen McCue[39], was addressed in chapter 3, but is central enough to the debate to warrant another look. As a piece written by and for law enforcement officials, Beck and McCue's presentation of the subject can be seen as an attempt to form and mobilize an actor-network in support of the technology. Recalling Callon's four moments of translation, we can see how Beck and McCue position themselves as representatives for their fellow officers.

As noted, Callon's first moment of translation consists of problematization, meaning that the system-building actors suggest a clearly defined problem as well as a possible solution. Beck and McCue set the stage for predictive policing as a solution by placing it in both a historical and a practical context. Written as an appeal to fellow Police Chiefs, Beck makes his case for why he fully endorses predictive policing as a vital part of "the next era of policing" (Beck 2009). The article opens with a rhetorical appeal to fellow law enforcement officials, citing the post-9/11 climate in the US, as well as the current economic situation, as major catalysts for change in policing. Police districts around the country are put in a situation where they have to be vigilant for potential emergencies, but at the same time, their budgets are being severely restricted by economic cutbacks. The problems that law enforcement agencies are currently facing thus seem fairly straightforward, according to Beck and McCue. With Callon's concept of problematization in mind, the following is a telling example:

> As these new budgetary restraints and limitations are faced, the question to ask with more urgency is "Why just count crime when you can anticipate, prevent, and respond more effectively?" Predictive policing allows command staff and police managers to leverage advanced analytics in support of meaningful, information-based tactics, strategy, and policy decisions in the applied public safety environment. As the law enforcement community increasingly is asked to do more with less, predictive policing represents an opportunity to prevent crime and respond more effectively, while optimizing increasingly scarce or limited resources, including personnel. (Beck 2009).

There is a clear problem that must be dealt with, "doing more with less", and the solution comes in the form of the innovative technology predictive policing. Beck and McCue's solution is unambiguous; increasing the efficiency of police work and optimizing resources is

[39] President and Chief Executive Officer, MC2 Solutions

the answer to (at least some of) their woes, and predictive policing provides the tools to realize this potential. Here the double movement that characterizes problematization is clearly recognizable; Beck and McCue simultaneously define the problem and demonstrate that they have an elegant technological solution. By speaking on behalf of the LA police, as well as the predictive policing technology and its developers, Beck and McCue are positioning themselves as an obligatory passage point. Or, more accurately, they are presenting predictive policing as the obligatory passage point – anyone who wants to solve the problems facing law enforcement, must go through predictive policing in order to gain access to the promised efficiency and resource-saving properties of Big Data.

In addition to appealing to the current problems facing law enforcement, Beck and McCue also place predictive policing in a historical context. They summarize a number of policing innovations, including CompStat and ILP, noting the successes but also the limitations of each of these. Predictive policing, they claim, builds directly upon the successes of these previous innovations, while improving them by removing the obstacles that used to face police analysts. The results are directly measurable, and predictive policing demonstrably leads to improved statistics. When results are easily observable, the technology can be packaged as a marked improvement in terms of public safety, meaning that predictive policing should be rather unproblematic to implement (Willis and Mastrofski 2011, 316). Additionally, Beck and McCue point to examples of other successful uses of predictive Big Data analytics. As they point out, large retailers such as Wal-Mart have successfully used similar analytics to anticipate customer demands, tapping into their databases in order to spot patterns and future trends. If it works for Wal-Mart, then it should work for the LAPD.

7.3.1 Law enforcement – Moments of translation

Returning to Callon's moments of translation, once a problem and a possible solution has been defined, the process of interessement follows. Interessement is a process where the system-builders attempt to stabilize the actor network they have created, by strengthening their narrative, ensuring a common language for its members, and thus closing off other venues for discussion. The focus on clearly observable (quantifiable) results, has the function of separating the technology from other less easily measurable problems,[40] and pinpoints the issue as a question of stopping crime and dealing with shrinking budgets. This is an attempt to recruit fellow law enforcement individuals to their group by making predictive policing a gatekeeper, providing a common language for the actors. The third moment of translation, enrollment, describes the means through which the system-builders attempt to further establish the roles and identities of actors within their group. As representatives for the group of law enforcement, Beck and McCue place predictive policing in a historical context where predictive policing appears to be an almost natural next step in policing technologies. By appealing to a historical account of police technologies, they want to ensure that fellow members of the police subscribe to their techno-optimism. Following a narrative that places predictive policing as a natural evolution of previously successful technologies, actors opposing the technology might as well be luddites or spoilsports. The question of "how can Big Data technologies used by companies such as Wal-Mart be used for law enforcement purposes" has already become "predictive policing is the natural next step for policing".

At this stage, it is no longer a question of whether predictive policing *should* be implemented, instead the impression given by Beck and McCue is that it would be foolish *not* to adopt the technology. This leads us to Callon's fourth and final moment of translation, mobilization. By transforming the more open-ended questions, such as how to deal with certain problems, into concrete statements about the proven efficiency of Big Data, Beck and McCue are attempting to establish and solidify predictive policing as a representative of their actor-network. Rather than being about police-interests such as budgets and working-hours, an artefact such as PredPol is a representative that seamlessly communicates efficiency and accuracy. The post-9/11 reality of policing, the ideas of adapting corporate algorithms to policing, the officer patrolling the street, the history of CompStat and ILP – all of these actors and ideas are displaced from their physical reality and represented by Beck and McCue's idea of predictive policing. This embodies what Callon means when talking about a sociology of translation; many actors have been translated into one actor-network, represented by and therefore embedded in the technological artefact that is predictive policing (Callon 2007, 75).

[40] Such as for example socioeconomic factors or other perceived underlying issues that might lead to criminal activity.

7.3.2 Law enforcement – Closure mechanisms

The attempt at placing predictive policing as the natural continuation of a historical narrative bears some similarity to technological determinism. Not only is predictive policing presented as a natural evolution of decades of innovation, it is also lauded as a seemingly ideal tool for the current social and political climate. Law enforcement is in crisis, and Big Data appears as a saving grace. In this view, there seems to be little room for negotiation at all. The pressing problem is clear – especially to those with experience of working in law enforcement under current conditions – and the solution is readily available, having been proven to work for other big organizations such as Wal-Mart. Seen in light of SCOT and the concept of closure mechanisms, it can be said that these rhetorical tools are attempts at closing the controversy before it has begun. As noted, one of Pinch and Bijker's mechanisms for stabilizing a technology is attempted through rhetorical closure (Pinch and Bijker 1984, 427). When a relevant social group attempts to achieve rhetorical closure, they will try to convince, and thus recruit, other actors to their group by presenting a clear problem, and subsequently a solution. If the rhetorical closure is successful, this means that other relevant actors or groups perceive the presented problem as being solved by the technology. Mirroring Callon's theory of group-formation, the attempt at achieving rhetorical closure functions similarly to the moments of translation, but whereas Callon's translation describes internal group dynamics, including how material objects are part of these networks, Bijker's closure mechanisms are concerned with negotiations taking place *between* different social groups.

Recalling the three-dimensional framework presented by Moses and Chan, the Beck and McCue article can be said to touch upon both the technical and social dimension of the artefact. The technical aspects come to the fore when discussing the efficiency and results of similar technologies, arguing that Big Data analytics is an effective and demonstrably functional piece of technology. On the social side, they attempt to lower the threshold for fellow law enforcement officials to welcome the technology. By bridging the apparent gap between existing law enforcement practices and predictive policing, the "old" and the "new era" of policing are drawn together (Moses and Chan 2014, 654). This is a way to recruit fellow officers to their point of view, thus stabilizing the artefact as a technologically efficient tool that should be adopted. By presenting the technology as being compatible with existing methods and needs, predictive policing is made out to be a low-cost solution which can be implemented without much trouble (Willis and Mastrofski 2011, 315).[41] Summing up, if law enforcement officials such as Beck and McCue are able to convince other officers (and other groups outside the law enforcement group) that resource allocation is a pressing problem, and that predictive policing is the best solution to this problem, then they have successfully established predictive policing as representative of the actor-network (or social group). If an actor-network stabilizes around predictive policing, they may go on to attempt rhetorical closure, by appealing to other actor-networks. If the closure is successful, the technology can then be adopted without much further ado. After all, if Beck and McCue's arguments are accepted, then the pressing problems will be effectively solved by adopting predictive policing. However, what if some groups refuse to accept the premises of Beck and McCue's argument?

7.4 Technology skeptics

Throughout this thesis, I have shown that some proponents of Big Data technologies have a tendency to emphasize the automated elegance of the data mining process. From the Netflix algorithms to Beck and McCue's endorsement of predictive policing, there have been signs of what Boyd and Crawford have characterized as the "mythological" version of Big Data, where the technology is perceived as giving access to some coveted higher truth. Whereas human actors are prone to errors and misjudgment, the story often goes, the refinement of advanced algorithms allow for decisions and predictions to be produced undiluted by human bias. Following this line of reasoning, while decisions made by human officials or corporations are inherently subjective, the focus on analyzing raw data allows Big Data to produce measurable and objective responses. This supposed objectivity is a significant part of why proponents laud Big Data as a superior technological solution to problems that may not be purely technological. In these cases, the catchphrase of "more data equals better accuracy" seems almost like a truism. A second social group, which I will call "technology skeptics",

[41] This notion is challenged by critics of the technology, who argue that Big Data analytics require a lot more than passing knowledge of computers and police work. I will revisit this point later in the chapter.

have emerged on the basis of challenging the notions of data-neutrality, thereby destabilizing one of the load-bearing pillars of the technology-based argument.

Because these skeptics mainly communicate their views through research and technology reports, and because their criticism is more concerned with using caution with technology rather than attempting to present a certain narrative, my analysis of this group will differ somewhat from the previous section. Although Callon's moments of translation can be discerned in the mobilization attempted by actors such as Boyd and Crawford, the technology skeptics' focus is more directed towards challenging or destabilizing the problematization presented by actors such as Beck and McCue. It may therefore be more useful to examine the technology skeptics and their arguments in light of Dewey's concepts of issue-formation. By challenging the narrative of the techno-optimists, the skeptics are bringing out the inherent conflict of interests that predictive policing represents. This manner of highlighting points of contention is one way of articulating particular issues, bringing together a public that is more about the issue itself, than about the technology for its own sake. Nevertheless, Callon may help us understand how some actors may undermine the attempts at mobilization, through rejecting the process of representation. On controversy, Callon writes "Controversy is all the manifestations by which the representativity of one spokesman is questioned, discussed, negotiated, rejected, and so forth" (Callon 2007, 72). The concept of controversy may be helpful when looking at the actors who are skeptical of predictive policing, and when analyzing the process of destabilization.

7.4.1 The human factor

In their article *Critical Questions For Big Data*, Boyd and Crawford emphasize that the increased reliance on quantification does not mean that Big Data analysis is a value-neutral tool. For all its assurances of dealing with neutrality and objective facts, they argue, it is important to not overlook the considerable human element involved in the process of data mining. In the philosophy of science it is an established idea that researchers are always interpreting data, thereby to some extent inserting their own personality and biases into their research. Deeming an observation as worth studying is a process of selection, and any form of selection will inevitably entail exclusion. Information needs filtering in other to have any meaningful application. The same applies to the process of Big Data analytics. System designers have to make decisions about how to program their algorithms, about which information is worthy of categorization, and how to adjust the parameters. In order to improve the signal to noise ratio, some data takes priority as relevant, while other is left by the wayside. As seen in chapter 4, the aggregation and cleaning of data means that statistical outliers are eliminated to account for errors, which could create biased conclusions that tend towards low variability. In other words, the activity of data collection and analysis has an inherently subjective aspect, and not all data is created equal (Boyd and Crawford 2012, 667). Similarly, Moses and Chan stress the point that there are individual human actors creating the algorithms, deciding the proper method of data mining, and so on (Moses and Chan 2014, 648).

Moses and Chan suggest that the possibility of several teams working with the same datasets, inserting or removing information based on their own understanding and biases, must also be considered. Translation errors between individuals or different institutions is therefore a possible obstacle to predictive policing. Consider, for example, a police officer and a statistician both working towards the refinement of an algorithm to be used in predictive policing. What the officer and the researcher consider relevant to prediction may diverge, and their different understandings and social contexts could result in inconsistent results. Similarly, when the data that is to be analyzed comes from separate sources, each of those sources run the risk of being riddled with errors. If the sources are already error-prone, increasing the amount of data could serve to magnify the margins of error (Bollier and Firestone 2010, 13). On a practical level, the individuals who have to make real-world decisions based on the predictions, such as an officer or a judge, may not be experts on statistical modelling. Even if the predictions or conclusions made by the algorithms are accurate or correct, the results could be dramatic if they are misinterpreted. Thus the proper communication of potential limits and the inner workings of the algorithm, and therefore any inferences drawn, is a necessary feature of many Big Data systems (Moses and Chan 2014, 667).

7.4.2 Technological limitations

A possible problem related to the issue of data interpretation is known as apophenia, the phenomenon of "seeing patterns where none actually exist, simply because enormous quantities of data can offer connections that radiate in all directions" (Boyd and Crawford 2012, 668). This is a matter of misidentifying correlation and causation. For example, areas where many crimes have been reported are likely to have a high police presence.[42] A commonsensical interpretation of this would be that the police are there as a result of the reported crime. If the algorithmic mechanisms aren't properly trained, however, they may interpret the correlation as meaning that more police in an area leads to more crime (Perry 2013, 123). It will often take a human analyst to differentiate between the cause and effect in such scenarios. Similarly, if certain data is missing from the set, the correlations that are being drawn may be lacking a causal foundation (Bollier and Firestone 2010, 16). To borrow an example from Moses and Chan; a large fire is normally associated with significant property damage, a large response from the fire department, ambulances, etc. If an algorithmic tool had access to data capturing both the extent of damage done and the amount of response, but lacked information about the fire itself, the system might deduce that the amount of fire engines at the scene caused the property damage (Moses and Chan 2014, 666).

Another concern raised by technology skeptics is that all predictions are based on registered crime data. However, in order to exist in the crime data registers, a crime must first be reported, and an arrest must be made. It is a well-known issue that not all crimes are reported equally. For example, sexual crimes such as rape are often left unreported. If the crimes were not reported, as far as the algorithms used in predictive policing is concerned, it does not exist. This form of data omission is one of many ways in which being uncritical of source data can lead to larger systemic errors (Perry 2013, 120). Similarly, bias may be introduced into the data rather innocuously, if for example, an officer reports any encountered criminal activity at the end of his shift rather than as they occurred, this might lead to the erroneous assumption that the time of shift rotation is more likely to be filled with criminal activity. In other words, by focusing on the end results (improved crime statistics, for example), proponents of predictive policing may be blinded by the mythological aspects of Big Data.

[42] Note that "have been reported" is important. As I will show, the number of reported crimes do not necessarily correlate with the number of actual crimes occurring.

Even though the technological complexity and the buzz about automated processes guiding each step of predictive policing may suggest otherwise, the computer will not do everything by itself (Perry 2013, 151). Because the system can be extremely complex, in a case where the source data, some parameters, or algorithms are inaccurate or plain wrong, the black boxing of the artefact may prevent the user from seeing these mistakes. According to the technology skeptics, then, the amount of possible mistakes when dealing with datasets such as criminal records may not be worth the measurably improved crime statistics.

On the other hand, proponents of Big Data analysis have claimed that these perceived errors are actually advantageous if they are handled correctly. In a report on Big Data by the Aspen Institute, IBM chief scientist Jeff Jonas responds to the accusations of the error-prone nature of Big Data, countering that bad data is helpful for allowing the system to account for more than one version of the truth. When the numbers are in disagreement, he continues, the analyst must act upon the inconsistencies and adjust his assertions accordingly (Bollier and Firestone 2010, 13). What initially seemed like noise may thus, in the right hands, be converted to more useful data. It should also be noted that none of the problems outlined above are necessary features of any Big Data system. The system can be designed to account for possible errors, have necessary checks and balances, proper oversight by statisticians and other professionals, and so on. As I will show towards the end of this chapter, some proponents of predictive policing claim that there are ways to ensure that biases are made explicit (if not eliminated), and with sufficient information, transparency, and training, those who rely on the technology and its results are able to understand the underlying mechanisms of the system.

7.4.3 Revealing inconsistencies and articulating issues

A common factor of the criticism outlined above is that despite what some techno-optimists claim, the process involved in Big Data analysis is not necessarily unproblematic and accurate. As we have seen, whereas proponents want as much data as possible in order to secure accuracy, skeptics are claiming that more data could also mean greater chances for errors. These counter-arguments can be said to serve two main functions. Firstly, they are an attempt to knock down the deterministic belief that technology is inherently good, by challenging the technological aspects of predictive policing. To borrow a word from Callon, the technology skeptics position themselves as dissidents, refusing to accept the arguments of the proponents (Callon 2007, 73). Rejecting the arguments of accuracy and data-neutrality, the skeptics challenge the representativity of actors such as Beck and McCue; if their arguments are faulty, predictive policing cannot be the focal point of a stable actor-network. By not accepting the representativity of predictive policing, the technology-skeptics bring a controversy to light, thereby destabilizing the technology. If these criticisms are valid, then the negotiation of roles must change; if predictive policing is to be adopted, then proponents of the technology need to address the aforementioned problems.

Secondly, the technology-skeptics challenge the possible practical consequences of implementing the technology. Here we can recognize the concept of publicizing an issue, or attempting to articulate the issue by making it a public matter (Marres 2007, 772). By emphasizing the proven results and historical precedents, actors such as Beck and McCue are de-publicizing predictive policing, or making a non-issue out of it. In their account, predictive policing is a police solution for police-problems, and since its results are proven, little room is left open for discussion. Although they are arguing on a technological basis, actors such as Moses and Chan are articulating predictive policing as a possible public issue when they acknowledge the possible errors that might crop up in a Big Data analysis. After all, the technology is not merely going to be crunching numbers – by extension it will be put into practice by patrolling officers, who may in turn act wrongly on the basis of errors in the data or algorithms. As I will go into in more detail when examining the legality-perspective of the discussion, this may lead to potentially harmful social consequences.

7.4.4 Technology skeptics – Closure mechanisms and destabilization

It is clear that although both the technology skeptics and the law enforcement group are arguing on the basis of technological aspects, their conclusions are in direct conflict and at times contradictory. As noted, representatives such as Beck and McCue attempt to reach closure by stating the artefact's superior efficiency and technological success as a given fact. Skeptical actors, such as Moses and Chan, focus on the argument that predictive policing is not as efficient at finding accurate patterns as its proponents claim, or that the potential gains may not outweigh the risks. By opening the black box of the technology, and pointing out inconsistencies and the possibility of human error, they attempt to demythologize the technology, and re-open or destabilize the representation made by the law enforcement group. In the language of SCOT, the skeptics are attempting to shape the debate by redefining the problem. This closure mechanism is induced by moving the discussion from "how best to implement predictive policing?", towards "is Big Data reliable enough to be used for such purposes?". Actors such as Moses and Chan therefore resist the moments of translation attempted by Beck and McCue. While they may accept the problematization set forth by the technology proponents – that there are problems with police budgeting and that new technology may be a possibly useful tool – the skeptics are not willing to be enrolled into the proponents' social group. Instead, they work from outside the group in order to destabilize the terms or statements set forth by proponents of the technology. This serves both as a way to redefine the problem, but also articulates an issue that Beck and McCue have avoided; namely that predictive policing may have harmful consequences due to the inaccurate and mythologized properties of Big Data analytics.

7.5 The ethical and legal perspective – a question of principles

Although predictive policing can be both lauded and criticized on purely technological terms, this is not the only way to understand or evaluate the technology. As we have seen, technological artefacts should not be regarded in isolation from their surroundings, but rather be seen as embedded in a seamless sociotechnical web. For some groups, then, it does not matter whether the algorithms behind the technology can be trusted, or whether an application such as PredPol is proven effective at preventing crime. In this section, I will look at several actors and social groups that give predictive policing a different meaning by focusing on social principles. The common factor for all of these groups is that they are focused on the appropriateness of predictive policing, or about whether the technology is consistent with the principles of the society that we wish to live in. I have identified the two main perspectives within these principle-minded groups, consisting of actors concerned mainly with ethical principles, and some who focus on legal concerns.

Before leaving Beck and McCue behind, a paragraph from the closing section of their article leads us to the subject of principles. As seen, their article presents a rather straightforward and seemingly unproblematic picture of predictive policing. The final few paragraphs, however, does address some potential problems. In what could be understood as a preemptive move against potential critics, Beck and McCue note the following:

> The 2002 movie Minority Report, may create the impression that "predictive" analytics will be used to target individuals inappropriately for future crimes, or bad acts that they may commit but have not. It is important to note that predictive policing, like any public safety resource or tool, must be used legally and ethically. The analytic methods used in the predictive-policing model do not identify specific individuals. Rather, they surface particular times and locations predicted to be associated with an increased likelihood for crime. Identifying and characterizing the nature of the anticipated incident or threat increase the ability to create information-based approaches to prevention, thwarting, resource allocation, response, training, and policy. These fact-based approaches promise to increase citizen and officer safety alike. (Beck 2009)

This is the only mention that Beck and McCue make of potential concerns with predictive policing, but it opens the door for an alternative interpretation of the artefact. Rather than seeing predictive policing as a tool for doing more effective police work, the principle-minded group interprets the problem of the technology as one of social principles, principles which may be in danger of being violated. The short mention of ethics by Beck and McCue addresses the concern of surveillance and unwarranted targeting of individuals. As noted, this might be an increasingly common worry pertaining to Big Data and other advanced technologies that could be used to violate privacy, but predictive policing in its current form usually does not target individuals.[43] In its most common form, predictive policing is used to assign probability values of events happening in specific areas and timeframes. Because of this, I will not dwell further on privacy issues here. There are, however, two points in the above quote that are frequently challenged by critics of predictive policing. These are the notions that identifying particular locations based on existing data (or "facts") is inherently

[43] In fact, the police in Chicago have used Big Data technologies for targeting individuals. Algorithms were used in order to create a "heat list" of the 400 individuals who were most likely to be involved in a shooting. See Gorner (2013), http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list [last accessed 01.05.2015]

not in conflict with ethical and legal principles, and the notion of predictive policing being a strictly “fact-based approach”. I have already presented the latter objection in the section on technology-skeptics. Now I turn to the group criticizing the notion that identifying locations based on existing data is supposedly unproblematic.

7.5.1 The ethical principle-perspective

One worry that is often aired by principle-minded critics of predictive policing, is that the technology has the potential to further entrench injustices that are already a part of society and the judicial system. When it comes to issues such as racial profiling, the argument goes, the existing crime statistics may already be skewed by institutional or individualized racism, making the data that the algorithms have to work with inaccurate before the analysis even begins. If the existing crime data inaccurately states that minorities are more likely to commit certain crimes,[44] the output will reflect this erroneous input. The anti-surveillance website PrivacySOS, which is run by the Massachusetts branch of the American Civil Liberties Union (ACLU),[45] points to this as a major problem, which is in danger of worsening if predictive policing is widely adopted. They fear that a feedback loop may ensue, meaning that when more police are patrolling minority neighborhoods, it is likely that more arrests will be made there, while similar crimes in other neighborhoods go unrecorded.[46] This means that the data reinforces itself, skewing the stats even further while under the guise of algorithmic objectivity. In this scenario, rather than eliminating injustice, Big Data could have the effect of protecting institutional and systemic racism, by deflecting blame to the supposedly neutral algorithmic mechanisms at work.

In the view of the ACLU, then, the problem with predictive policing has little to do with police resources or crime prevention. Sites such as PrivacySOS are concerned with the civil rights of individuals, which takes primacy over issues such as police budgeting. If

[44] For example, black men are disproportionately arrested for marijuana-related offenses in the US (Levine 2010). In a predictive policing scenario, the algorithms are likely to be unable to account for this discrepancy.
[45] The ACLU is a major civil rights organization in the US
[46] See https://www.privacysos.org/predictive [accessed 11.03.2015]

institutional racism is regarded as the key problem, then predictive policing certainly does not seem to be the answer, according to PrivacySOS;

> If police arrested lots of bankers and lawyers for cocaine use and for hiring expensive sex workers, we might see predictive policing algorithms sending cops to patrol rich suburbs or fancy hotels in downtown areas. Instead, the algorithms simply reproduce the unjust policing system we've got, and dangerously, add a veneer of 'objectivity' to that problem. The information came out of a computer, after all, so it must be accurate! (PrivacySOS n/d).

This kind of data-determinism is, in the view of the ethics perspective, liable to strengthen existing injustices and societal gaps. In the extreme case, there is a chance that the population as a whole will be considered as a disaggregated set of sub-populations, assigning different risk profiles based on race, creed, or political stance, rather than as a single social body (Milakovich 2012, 9). This could undermine the relationship between public agencies and individual citizens, in which individuals are in principle supposed to be treated on an equal basis. Similarly, it could also be a step towards a society where people are judged and treated based on what the algorithms declare us liable to do, rather than what they are actually doing. Related to this, there might be a risk that there is a lack of necessary information needed to make accurate predictions, which in turn may result in unjust or unnecessary false positives (i.e. innocents being apprehended) (Byrne and Marx 2011, 24). Here there are echoes of the arguments made by the technology skeptics. If the data used by predictive policing is already symptomatic of injustice, then the output will be unjust results.

7.5.2 Articulating the ethical issues in predictive policing

The concerns made by the ethically-minded critics of predictive policing can be elaborated by drawing on Dewey's theory of issue-formation. Groups such as the ACLU seize upon predictive policing as a way to articulate what they believe to be deeper social issues. By highlighting and problematizing issues such as racial profiling, they make predictive policing into a public matter. Whereas the group spearheaded by actors such as Beck and McCue might prefer a technocratic and technologically deterministic stance, the ACLU aim to democratize the technology by highlighting its potentially harmful consequences. If racial minorities or low-income neighborhoods run the risk of becoming unfairly targeted as a result of predictive policing, according to the ACLU, these groups have a right to mobilize and join the negotiation of the technology.

Applying Dewey's theory to modern technology as complex as Big Data, raises another important question. The ACLU raise concerns about what they call a "shield of objectivity" being created by the supposedly neutral algorithms behind predictive policing, which implies that the issues run the risk of being black boxed within the complexity of the technology. Consider, however, if the Big Data processes and algorithms behind predictive policing could be rendered transparent and open for inspection. As noted by the technology-skeptics, the neutrality of the algorithms is problematic because it takes a human being to create parameters and adjust the algorithms. The algorithms are not suited to deal with subtleties, which means that the parameters must be explicitly encoded into the system. If a predictive policing algorithm uses race, gender, or other similar factors as a decisive parameter, this must be inscribed in the technology itself. The technology would require these issues to be articulated, provided insight and transparency is possible. If the algorithms are allowed to remain black boxed, these articulations will be de-publicized, but if they are open for inspection, they might provide a possibility to evaluate and bring issues to light that otherwise would be unspoken. The implications of this will be further explored below, when looking at professor Tal Zarsky's defense of the technology.

7.5.3 Group formation and closure mechanisms

As a large organization mainly concerned with protecting the civil liberties of American citizens, the ACLU have been an active voice in the debate surrounding Big Data. Since they have a history of concerning themselves with this and similar technologies, they are a stable network, and thus Callon's moments of translation might be difficult to grasp as they specifically relate to predictive policing. As a civil liberties union, however, it is important to note that the ACLU acts as representatives for actors who would otherwise risk going unheard. The problematization is already in place; "how do we secure the civil liberties of American Citizens?" may be answered by "we organize protests, put the spotlight on violations of civil rights, and act as watchdogs". The ACLU acts as an obligatory passage point for actors who are put at risk by decisions and technologies that could violate their rights, and for marginalized groups who otherwise would not have the resources to mobilize. The moment of interessement can be distinguished as the ACLU articulates the problematic issues with predictive policing, highlighting subjects that may already concern its members (and American citizens in general), such as racial profiling and unfair treatment. This way of spotlighting an issue, is also a way to enroll actors and groups who might otherwise think that the technology does not concern them. Predictive policing is drawn into the group as a potential obstacle to their goal of preserving civil liberties. Thus the ACLU, concerned citizens, marginalized groups, and other at risk of having their rights violated, are all translated into and represented as being threatened by predictive policing. This closely resembles the case of the police-group favoring the technology, but the outcome of this mobilization is the polar opposite of the result of Beck and McCue's process of translation. Rather than predictive policing representing a positive solution to pressing problems, the technology becomes an embodiment of existing societal problems. All the involved actors in the actor-network of the ACLU are displaced, represented by a number of articles by the ACLU, and presented to government institutions.[47]

Upon examining the views represented by the ACLU, certain closure mechanisms can be identified. Whereas the law enforcement group sought to close the debate around predictive policing by declaring it to be technically efficient, organizations such as the ACLU attempt to reopen the debate by destabilizing the technology. They attempt to do this by redefining the problem (Pinch and Bijker 1984, 427). Relevant social groups may attempt to destabilize technological artefacts, by redefining the question of what the technology is actually meant to solve. By moving away from quantifiable and technical questions of efficiency and improved crime statistics, and towards qualitative principles such as civil liberties and equality, predictive policing is presented a tool of potential injustice and possibly even repression. Consequently, predictive policing is not seen as a solution at all, and according to the ACLU, the police should be looking inwards in order to root out institutional injustice rather than

[47] Perhaps most accurately embodied in the ACLU's collaboration with other civil rights organizations, called "Civil Rights Principles for the Era of Big Data". See Calabrese (2014) https://www.aclu.org/blog/when-big-data-becomes-civil-rights-problem [last accessed 01.05.2015]

attempt a technological "easy fix". After all, it seems difficult if not impossible to take ethical principles into consideration when working with quantifiable data, which means that by using Big Data analytics, proponents of predictive policing might be missing a vital part of what policing should be about in regards to ethics and community relations. Again, it is interesting to note that rather than disagreeing on the solution, the groups of techno-optimists and those concerned with ethics and liberties do not even agree on the problem. It seems clear that a discussion based purely on the technological merits of predictive policing, will not lead to any sort of agreement between these groups.

As a side note, although the ethical side of predictive policing is sidelined in Beck and McCue's characterization, this does not mean that it is a non-issue for proponents of the technology. As noted, their article was published in The Police Chief Magazine, and is thus directed towards colleagues rather than a broader audience. In a summary of the First Predictive Policing Symposium (Uchida 2009), representatives for the police, including Beck, stress that it is necessary to properly communicate the intent behind the technology to outside groups. Since community policing depends on maintaining a certain relationship with the actual communities that are being policed, a level of trust must be cultivated. Some approaches to achieve this are suggested, including transparency of intentions and clearly defined mission statements about topics such as which data to include, and where to draw the boundaries about what kind of data should be classified. The general gist of the symposium, however, seems to be that predictive policing is a desirable tool to improve the results of policing, and that the major obstacles include maintaining public trust and communicating the need for the technology to outside groups. I will return to these points in the below sections.

7.6 The legality-perspective

Although the ethically minded group concern themselves with legal principles (of discrimination, etc.), their main thrust of their arguments address moral issues. Moving on from the ethical discussion, I will look at how some actors attempt to represent the implementation of predictive policing as a question of legality. If it can be demonstrated that predictive policing is in conflict with the judicial system, the debate may take a considerable turn away from questions such as efficiency and resource-management. Of course, critics of the technology are not the only relevant actors who have to consider the existing legal framework. Law enforcement tools and techniques must be evaluated in light of what is permissible, and if the technology contradicts legal precedents it must be reconsidered. Proponents such as Beck and McCue likely assume that if the technology is going to be implemented it is bound to be in a form that conforms to the law. As we will see, however, the nature and consequences of predictive policing might give rise to, or articulate, a number of serious legal issues. Important concepts for the legality-focused actors include transparency, accountability, and civil rights. In the following, I will first present some legality-minded critics of predictive policing. I will then proceed to look at how a representative for another group, which can be loosely characterized as principle-focused proponents of predictive policing, comes to the opposite conclusion despite operating within the same legal context.

7.6.1 Predictive policing and the legal system – The critics

As demonstrated in the concerns raised by the ACLU, a main issue amongst critics of predictive policing is that the technology may come into conflict with constitutional rights. For actors who are concerned with technology and the legal system, it is of little matter whether predictive policing provides efficiency, economic benefits, or similar advantages. Unless the technology is examined within a legal context and is found to be consistent with existing principles, it should not be adopted by anyone, and perhaps especially not the police. If the technology cannot be demonstrated to be consistent with the law, then something must change.[48] Let us first examine the legal principle that is perhaps rendered most vulnerable by predictive policing methods, namely the Fourth Amendment. The Fourth Amendment in the US Bill Of Rights reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and

[48] As I will show, this does not necessarily mean that the technology must change. Some will argue that the legal system needs to adapt to the technology, rather than the other way around. This somewhat reflects the dichotomy between technological determinism and social constructivism.

particularly describing the place to be searched, and the persons or things to be seized. (Britannica 2014)

Highly relevant to patrolling police officers, the concepts of "reasonable suspicion" and "probable cause" warrant a closer look, although without venturing too deeply into legal jargon. Intended to protect citizens from becoming victims of unreasonable searches or other infringements, the principle of reasonable suspicion means that if a search or seizure is to be made, the officer making the stop must prove that he or she had sufficient reason to suspect that the subject was engaging in illegal activities. Probable cause, on the other hand, requires the officer to demonstrate suspicion of illegal activities based on his or her police experience, with a degree of certainty that cannot be expected of an average citizen. Probable cause is thus held to a higher standard than reasonable suspicion, and officers are required to demonstrate probable cause in order to obtain a warrant.[49] If reasonable suspicion cannot be demonstrated, any searches, seizures, arrests, or surveillance can be deemed unreasonable and therefore inadmissible in court. Professor of law Andrew G. Ferguson has written several papers on the possible implications that predictive policing may have for these legal principles, and as an authority of the subject he may be considered a representative for the legality-minded critics of the technology.

Establishing and demonstrating reasonable suspicion is not a binary or purely objective exercise. According to Ferguson, the police "must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion" (Ferguson 2012, 286). To decide whether reasonable suspicion exceeds a threshold of for example 50% is subject to predictive guesses, meaning that predictions will be made that a certain individual or group will be at a specific place at a certain time. Much like the predictive policing analytics, patrolling officers make these judgements, although they base their predictions on heuristics and experience rather than number-crunching. In other words, it is not an exact science, and requires informed judgment based on as much available information as possible. A seasoned police officer may be able to justify a search based on years of experience, seeing clear signs indicating criminal activity, and so on. Since one can rarely be completely certain that someone is about to break the law, it is also recognized that

[49] See http://legal-dictionary.thefreedictionary.com/probable+cause [accessed 15.03.2015]

sometimes these predictions will be wrong. If the officer in question is able to demonstrate reasonable suspicion, such a stop and search is within legal bounds, even though the subject of the search has done nothing illegal. Since there will always be a degree of personal judgment involved, cases of questionable suspicion and improbable cause will normally have to be settled through informed deliberation by the courts, based on precedents set by previous similar cases. Ferguson notes that there are no obvious precedents for determining reasonable suspicion on the grounds of predictive algorithms, making such assessments problematic when it comes to cases assisted by predictive policing. When exploring how predictive policing can be conciliated with the Fourth Amendment, Ferguson therefore looks at possible examples that have certain parallels to predictive technologies. Whether the target of a search and seizure is based on individual suspects, groups or profiles, or geographical and spatial areas, reasonable suspicion must be demonstrated in different ways.

7.6.2 Ferguson's argument

Ferguson evaluates the legal precedents of predictive policing by comparing it to existing scenarios, by describing how probable cause can be established. The first scenario he considers consists of the police acting upon a received tip. Precedents from The Supreme Court state that in order to be admissible in court, an informant should be judged by *"veracity, reliability, and basis of knowledge"*, all of which must remain *"highly relevant in determining the value of the tip"* (Ferguson 2012, 289). This raises a question of whether predictive policing systems can be regarded as a reliable informant. Ferguson explains that since any algorithmic predictions are generalized based on extensive data-analysis, it is not equivalent to an informant, who is by definition required to have specific inside information about criminal activity. If predictive policing cannot be treated as an informant, Ferguson notes, then perhaps it can be compared to existing practices of police profiling, the traditional police method of looking for suspects fitting particular descriptions. However, in order to be relevant, profiles have to be specific enough to clearly differentiate suspects from non-suspects, and be relevant to place and time. Although predictive policing produces predictions that are place- and time-sensitive, they do not give particularized descriptions, only general ones such as "potential car thief". More accurately, the algorithms create profiles based on locational data, by for example telling officers to search individuals peering into car windows in a certain neighborhood. This differs enough from traditional profiling that Ferguson concludes that the two methods cannot be treated as equivalent from a legal perspective.

The final predictive consideration examined by Ferguson is based on identifying high crime areas in order to justify reasonable suspicion. As noted, already before the dawn of predictive algorithms, the police were relying on hot spotting in order to apprehend suspects. Although the term “high crime area” has a history of being used to justify probable cause, it is under heavy scrutiny from both scholars and judges (Ferguson 2012, 302). Even the actual definition of the high crime area is not agreed upon even in a legal context (Ferguson 2008, 1594). As pointed out by the ACLU, identifying certain districts or neighborhoods as “high crime” is also liable to facilitate classism, racism, and damage the police’s relation to communities. In addition to this, a Supreme Court ruling has made it possible for the police to arrest subjects without probable cause if the arrest happens within a high crime area, making the concept highly controversial (Fernandez 2015). In addition to the possible ethical concerns, the statistical soundness of using high crime areas to justify probable cause is also questionable. Because these designated areas often contain tens of thousands or more inhabitants, the statistical significance of stopping individuals based on geographical location can be miniscule. The impact of these problems, Ferguson argues, could actually be softened by the technology provided by predictive policing. Take PredPol for example, in which an area of 150 by 150 meters is singled out for patrolling officers. By narrowing down the area of suspicion and the type of crime to look for, officers can be more particular about whom they single out, and as the technology become more precise, the statistical relevance of the smaller areas may become defensible as facilitators of reasonable suspicion (Ferguson 2012, 321). At the same time, this narrowing of the high crime area means that a prediction from PredPol about a car theft will only justify reasonable suspicion as long as the subject is apprehended within that particular 150 by 150 meter area. If the suspect was apprehended just outside the area, the prediction can have no legal bearing on the level of suspicion. This indicates that predictive policing may open even further legal gray areas that must be addressed before it is widely adopted.

Summing up Ferguson's verdict, it appears that no single factor alone is enough to warrant reasonable suspicion. Both tips, profiling, and the identification of high crime areas are considered relevant by the courts, but only as one part of the broader circumstances. In each example the suspicion must be corroborated by observation from police officers, be particularized to either specific individuals, groups/profiles, or a place, and be detailed enough to separate the suspect from non-suspects, as well as be recent enough to be deemed relevant. Ferguson concludes that in order to not breach the Fourth Amendment rights of citizens, a system such as PredPol cannot justify a stop and search on its own. This seems fairly straightforward, and was touched upon as part of the argument that PredPol will simply be another tool for the officers to use. Police intuition, field experience, heuristics, and detective skills will all contribute to corroborate the initial tips that are received from the predictive software. Ferguson argues that it is too early to establish whether predictive policing algorithms are accurate enough to be regarded as trusted sources of information, but he acknowledges the possibility that the technology could open new ways to establish reasonable suspicion, thus shifting the balance of suspicion in the areas it singles out (Ferguson 2012, 305). For example, if you are spotted branding a crowbar in an area where the algorithm predicts a burglary, this might weigh stronger than if you were carrying a crowbar in an adjacent neighborhood, since simply carrying tools is not enough to justify a search and seizure. In other words, by shifting the standard from *probable* to *probabilistic* cause, the legal threshold for apprehending a suspect may be lowered considerably by the introduction of predictive policing (Bollier and Firestone 2010, 34). Although he does not dismiss the possibility of implementing predictive policing in a responsible matter, Ferguson cautions against adopting the technology without taking preventive measures. In a worst case scenario, predictive policing might exploit the Fourth Amendment by lowering the threshold for probable cause and reasonable suspicion (Ferguson 2012, 313).

7.6.3 Using the legal system as a closure mechanism

As with the other groups and representatives examined so far, it seems clear that Ferguson interprets predictive policing technologies by placing it in context of his own professional perspective. By redefining the problem to address whether predictive policing is adaptable to legal precedents, the questions of ethics and technical efficiency take a back seat. Still, the accuracy and trustworthiness of the algorithms are important to Ferguson for deciding whether predictive policing can contribute to establishing probable cause. Interpreted through the legal system, however, the main problem becomes whether the artefact is adaptable and flexible enough to function within existing legal bounds. This is another attempt to open up and destabilizing the artefact by redefining the problem. If predictive policing cannot be molded to fit the legal system, then it might be unacceptable to adopt the technology. Since court decisions are made based on existing precedents, the novel approach of predictive policing might present a problem that is not easily fixed by introducing more efficient technologies.

Rather than letting predictive policing function as an obligatory passage point, Ferguson places the Fourth Amendment at the center of his argument. Similarly to the ACLU, he thus conscripts the civilian population into his group – the Bill of Rights is designed to protect all US citizens. By evoking the Fourth Amendment, Ferguson therefore positions himself as speaking on behalf of everyone who might become impacted by unreasonable stop and searches. The potentially vulnerable citizens who are at risk of being harmed by the erosion of these legal principles do not, however, only extend to individuals who are at higher risk of being stopped by the police. Emphasizing that predictive policing may signal a change of legal standards has implications that potentially concerns everyone. Ferguson therefore lets the Fourth Amendment stand as a representation for the public at large. He articulates the issue to be about legal protection for citizens, and by doing so he explicitly makes predictive policing into a public issue. Consequently, predictive policing should not be allowed to be implemented on only the basis of efficiency or functionality, but needs to be evaluated and restricted in a responsible manner. It should be noted that Ferguson, unlike the ACLU, does not attempt to mobilize the public and encourage citizens to make their voices heard. As he is situated in what could in SCOT terms be called a legality-centered technological frame, Ferguson calls for these issues to be handled by the courts. Again it seems clear that Ferguson lets the legal system, and particularly the Fourth Amendment, represent the interests of American citizens when faced by the issues presented by predictive policing.

7.6.4 The legality-perspective – Adapting to Big Data

In contrast to Ferguson's point that Big Data analytics may be unsuited for police work because they may clash with existing legal principles, the political scientist Michael E. Milakovich suggests using an anticipatory approach in order to accommodate the challenges that Big Data might bring. Besides the training and education of personnel, he suggests that data management should be linked to committed elected leaders and skilled public employees. This is likely to add a considerable cost to the implementation of Big Data technologies, but in order to ensure a context in which transparency and accountability is possible, Milakovich argues that the costs are necessary. Increased sharing of data across sectors call for a joint effort to ensure accurate translation of information, as well as solutions to issues of data security and access. Milakovich goes on to prescribe a continuous oversight and overhaul of regulatory enforcement running parallel to the evolution and spread of the technology. Rather than letting the technology follow its own deterministic path, then, Milakovich argues that relevant legislative decisions must be continuously reevaluated to ensure responsible use of data-mining and similar technologies (Milakovich 2012, 10-11). As Big Data analytics are increasingly being used to predict and prescribe future action, lawmakers and decision-makers must be trained in the workings of the technology, and use their power and knowledge to shape the innovation in a way that is consistent with the principles of society. Rather than approaching the problems formulated by the technology-skeptics – such as the considerable human factor of Big Data – as a critical problem for technologies such as predictive policing, Milakovich suggests that expertise is a possible solution to the problem of making Big Data into a transparent process. As long as the individuals who are actively working with Big Data analytics are sufficiently trained and educated, and this would include police officers and court officials as well as programmers, the seeming impenetrableness of predictive policing might be a surmountable problem.

By suggesting that existing social institutions should adapt to Big Data technologies, Milakovich could easily veer close to technological determinism. However, in adopting an anticipatory stance, he also acknowledges that we must adapt in order to maintain control over the technology rather, than letting it become black boxed or run its own course. Where legal precedents do not exist, they must be anticipated so the potential problems can be handled before the technology is too entrenched to be changed. For Milakovich, the problems facing Big Data therefore seems to be neither purely legal, technical, nor social. By approaching predictive policing as a sociotechnical phenomenon, the potential problems may be solved through a variety of means. The most obvious problem, however, is that these suggested solutions will be resource-intensive and potentially difficult to implement.

7.6.5 Predictive policing and legal issues

Although actors such as Ferguson and Milakovich have different ways of dealing with Big Data analytics, they all approach the technology in the context of existing social and governmental institutions. By problematizing predictive policing as being a question of legal precedents, they change the direction of the debate considerably. In Fergusons view, the fate of predictive technologies should not be decided by technologists, police officials, or civilian organizations, but by a careful deliberation by the courts. Ferguson attempts to evaluate how well predictive policing can stand up to current laws and institutions, advocating that the technology should be monitored and restricted to make sure that it will fit within the existing framework. He cautions against the possible consequences that predictive policing might have for principles such as probable cause, especially if the technology is left unchecked. Thus predictive policing should be regulated to fit the legal system, but it may also serve a different function by putting the existing system to the test. Court cases do, after all, build upon precedents from previous cases, and new technologies may set new precedents.

As mentioned, since the existing governmental institutions may lack the means to solve the conflict of interests between the legal system and the challenges brought by Big Data, actors such as Ferguson and Milakovich take on a role as representatives of the public. This is what Marres, drawing upon Dewey, talks about concerning articulating public issues;

> (…) to articulate a public affair is to demonstrate for a given issue that, first, existing institutions are not sufficiently equipped to deal with, and second, that it requires the involvement of political outsiders for adequately defining and addressing it. (Marres 2007, 772)

What is important here is not whether it is the laws or the technology that needs to change, but rather the act of letting the technology put existing institutions to the test. According to Ferguson and Milakovich, it is not only predictive policing as an artefact that needs to be negotiated, but the very system it will be introduced into. With this in mind, the seemingly elegant solutionism of Beck and McCue seems like a much more daunting challenge.

7.7 The legality-perspective – Alternatives to data mining

Similarly to Ferguson and Milakovich, Tal Zarsky also considers the issue of using data mining from a legal point of view. Zarsky begins his evaluation by acknowledging that currently existing legal principles are unsuited to deal with Big Data technologies, and that data mining "(…) often falls between the crevices of constitutional doctrine." (Solove, quoted in Zarsky 2011, 295). Rather than dwelling on whether it is acceptable to use technology such as predictive policing within the current legal framework, Zarsky asserts that the use of data mining for governmental purposes should be assessed by looking at the available alternatives. In other words, instead of asking how Big Data can be implemented, he questions whether existing or potential alternative methods are any less problematic. In his 2011 article *Governmental Data Mining and its Alternatives*, Zarsky touches on a number of the arguments outlined above, but from a somewhat different angle.

After reviewing a number of impractical alternative ways to determine who the police should subject to searches, including complete randomization, Zarsky examines traditional policing methods. In this model, patrolling officers have to make decisions based on heuristics, supplemented by predetermined profiles constructed by experts (e.g. criminologists, criminal profilers, etc.). Certain choices will be made at an officer's discretion, but these choices will be guided by the expert profiles. However, since these profiles are constructed on the basis of existing cases, they may not be so different from data mining, other than their more limited use of data. Because the profiles are created based on factors that can be clearly communicated in human language, rather than hidden and complex algorithmic factors, the process is interpretable and can be scrutinized and corrected in cases where errors are made. But – and this is the crux of Zarsky's argument – even though the lack of automation in this process lends itself to interpretation, the fact remains that in the end, most of these selective processes can be reduced to choices made at human discretion. If a citizen is stopped by the police because he fits a certain expert-crafted profile, the decision to make the stop will nevertheless always be made by the officer, based on the officer's potentially inscrutable judgement. In other words, "(…) human decisions tend to (a) make use of heuristics and (b) employ hidden biases." (Zarsky 2011, 309). Data mining as a process can avoid these issues, as algorithms do not make use of heuristics, and biases can in principle be rooted out of the data.

We have already seen that members of the groups opposed to predictive policing, such as the ACLU, disagree with Zarsky's notion that algorithms do not have hidden biases. According to these critics, if the data is ridden with biases, so will the output. Zarsky recognizes these points, but rather than seeing it as inherent problems with the data mining process, he mirrors Milakovich in prescribing preventive measures;

> If the data mining process is sufficiently transparent, it can effectively overcome these challenges. Adding interpretability and even causation to the data mining process could allow policymakers to assure that biases are averted. (…) Biases in a central computer code, once acknowledged, could be tackled with ease and identified effectively by external review. (Zarsky 2011, 312).

Since evaluating a set of algorithms is more practicable than continuously monitoring and mitigating the hidden biases of individual officers working in the field, using Big Data methods might actually prevent discrimination rather than increase it. As long as the technology is made sufficiently interpretable and transparent, biases and other forms of unjust discrimination, which would otherwise remain in obscurity at the behest of individuals, may be found explicitly articulated and coded in the algorithms. If problematic assertions or parameters are codified, then they may also be identified and removed.

7.7.1 Articulating issues in coding

Zarsky's argument that any bias in a computer code can potentially be identified, brings us back to the articulation of issues. Although Dewey could not have anticipated the ways in which everything is encoded and codified in the digital era, this aspect of modern technologies puts the concept of issue-articulation into a new light. Let us return to the hypothetical example of the predictive policing algorithm. We know that although the algorithms do not make value judgments, it still needs to operate with parameters that are configured in certain ways. In addition to these basic parameters, machine-learning tools may automatize some of the process, but the main process will still operate and adjust itself based on existing criminal data. Let us take the case of Chicago as an example. The Chicago police have employed an algorithmically constructed "heat list" of the 400 individuals most likely to be involved in violent crime (Podesta 2014, 31). This list is based on factors such as geographical information, previous criminal history, and the social networks of the named individuals. Because these factors are being used, some of the people on the list have no criminal history, and were understandably surprised when they were approached by the police (Gorner 2013). If one investigated the inner workings of the algorithms, it might for example reveal that a particular young man made the list because of living in a violent neighborhood. Since this information would have to be codified in the technology, it can be extracted.

Dewey's concept of issue articulation could potentially be directly applied in this case, given the proper transparency and intelligibility of the algorithms. As per Zarsky's argument, if a young black man is stopped on the street because the acting officer holds secret racist opinions, this might be very hard or impossible to prove. If the algorithms are creating feedback loops based on such initial bias, however, it can be identified and turned into an issue. One needs only look to recent tensions in the US, such as the riots in Ferguson and Baltimore, to see why this could have considerable real-life consequences. If an arrest based on predictive policing results in unforeseen consequences, then an audit might be able to identify the exact node in the algorithms that caused the arrest. Rather than predictive policing algorithms making accountability more difficult, then, with the proper transparency and auditing it might help to single out and articulate systematic injustice. Predictive policing, viewed in this light, could potentially be a powerful representative for articulating public issues. But it could also, as per Ferguson's and the ACLU's concern, be an avenue for further obscuring and de-publicizing these issues.

7.7.2 Zarsky and the ethical perspective

Before moving on from Zarsky's argument, I will briefly look at his rebuttal of the arguments of unjust profiling put forwards by the ACLU. Zarsky's line of reasoning begins with acknowledging that systematic errors and personal biases may already be present in government and law enforcement. By introducing data mining technologies, these errors are not guaranteed to disappear, even if the process is made transparent. However, whereas issues such as systematic racism will always target minorities, errors in a Big Data analysis has an equal chance to affect any grouping, since the system in itself does not differentiate. In other words, any negative effects stemming from predictive policing (e.g. false positives) could impact anyone. In Zarsky's own words, "As opposed to the other feasible alternatives, data mining equally spreads the risk of error among individuals." (Zarsky 2011, 328). In contrast to the ACLU's concern that predictive policing could perpetuate a tyranny of the majority, Zarsky claims that the technology may have the opposite effect. In a somewhat polemical move, he accuses those who oppose data mining of being supporters or enablers of systemic injustice;

> The majority will seek a solution that would allow it to pass the burden on to the weaker minority as much as possible. By advocating alternatives that provide for human discretion, members of the majority will be effectively taking steps to insulate themselves from the disturbance and discomfort of the selection process. (…) Data mining processes, therefore, will not be the majority's favorite. (Zarsky 2011, 328).

It is of course beyond the scope of this thesis to examine the validity of these arguments. Still, the way in which Zarsky turns around a number of the arguments levelled against predictive policing, warrants some consideration. Mirroring how he began his paper, by acknowledging that there are legal issues that must be dealt with before implementing data mining, Zarsky concludes that none of the presented alternatives are ideal or free of error, but that data mining is a lesser evil.

From a STS perspective, we can say that Zarsky attempts to draw the legal and ethical perspectives together in the technology, in an attempt to close the debate. Rather than dwelling on the legal problems, which he assumes can be dealt with, Zarsky proceeds to make the technical, economical, and ethical aspects of the technology converge. By demonstrating the shortcomings of alternative methods, using arguments which are at times based on fear (everyone will be a suspect, etc.), he ends his argument squarely in an ethical frame. The lines of argument are not entirely dissimilar to those of the ACLU, but the ultimate conclusion is diametrically opposed. In one swipe, Zarsky attempts to recruit the other proponents of predictive policing to his own group; this way of problematizing the technology makes Zarsky's group the morally justified ones. Technical aspects such as errors in the system are acknowledged, but their computability has the advantage of being open to scrutiny. Finally, it must be noted that Zarsky does not subscribe to a purely technological determinist framework. He puts weight on the issue of transparency, and like Ferguson and Milakovich he makes a case for making the technological black box open for inspection. The data mining approach might avoid some of the problems of existing methods, but only if emerging errors can be corrected through emphasis on human involvement. In other words, Zarsky problematizes predictive policing by acknowledging the potential pitfalls of the technology, but he simultaneously presents a solution in the form of transparency. These are issues which can be solved "in-house", by having professional auditors inspect the technology. In Zarsky's view, then, predictive policing does not represent a public issue, although its results may benefit everyone as long as the potential problems are sufficiently handled.

7.8 Allocation of resources and available expertise

Law enforcement is of course not the only institution having to deal with the technical complexities of Big Data. Decision-making across many fields of government are being assisted by Big Data analytics, which could ideally assist with making accurate predictions and thus facilitate better decisions. The rapid growth of this technology is challenging for many reasons, and it is telling that in 2012, 90% of all the data available for decision-making analysis had only been created since 2010 (Milakovich 2012, 2). As Big Data analytics become increasingly important in a wide variety of fields, a new area of expertise opens up in the public sector. Simply stated, the people already employed in fields such as health care and law enforcement do not have the necessary skills to understand and operate these systems. Milakovich argues that this shift towards advanced algorithmic decision-making is creating a knowledge gap between what is expected from employees in these sectors in the future, and the competency they currently have. To reiterate; when using advanced analytical tools to make important decisions, it is not necessarily enough simply to act upon the output. The process behind the predictions must be understood by at least some operating personnel, with capability to adjust necessary parameters, deal with the flow of real-time information, and so on. For example, if a cross-agency network such as IBM's Smarter Cities[50] are to be properly implemented, someone must make sure that information is translated properly, and that aggregation accounts for and retains the necessary subtleties across different networks.

Milakovich notes that the implementation of Big Data analytics for governmental purposes necessitates a comprehensive training regime for the end users. It is not enough to simply hand out the new technology and ask people to use it. Ferguson also hints at this when discussing probable cause; in order to have the grounds for a legal stop and search, the patrolling officer must understand why the situation warrants a response. Recall that one of the main thrusts of Beck and McCue's argument, as well as the argument for predictive policing in general, is that police resources are sparse and need to be allocated more efficiently. Besides allowing officers to spend their time on patrol more efficiently, the predictive approach is claimed to have the additional benefit of preventing criminal acts from occurring in the first place, thus freeing up resources that would otherwise have been used to make arrests. It is interesting, then, that the question of expertise may turn this argument on its head. What if Big Data analytics truly requires extensive understanding of the technology, and practitioners are extended to include not just officers, but chiefs, police analysts, judges, jury-members, independent auditors, and so on? In that case, might the necessary training and new areas of expertise require resources that simply are not available in the first place? In an example of cross-pollination between social groups, Uchida (2009) notes that for some police officials these worries are pressing;

[50] A cross-agency information-sharing network, built on Big Data technologies, is being developed by IBM. See IBM (2012)

> Another issue, particularly within the context of shrinking budgets and financial difficulties, is the availability of appropriate resources. Do we have the right people in the right place at the right time? Police executives mentioned the need for civilian analysts and researchers, as well as technology, higher level training and funds. Other executives said that predictive policing is the wave of the future, as it allows for more efficiency and enables chiefs to do more with less. (Uchida 2009, 6).

It seems, then, that the initial argument about resource-allocation is not as unambiguous as initially presented by Beck and McCue. To some actors, the argument of budgeting might thus be a reason to *not* adopt predictive policing, rather than the contrary. Although operating within the same professional context (the realities of law enforcement), the involved actors draw contradictory conclusions. Even though the problem is agreed upon (lack of resources), the solution is up for debate even amongst police representatives. As both Zarsky and Milakovich have argued, in order for predictive policing to be acceptable in a legal and ethical context, procedures and mechanisms must be in place to ensure transparency. This seems like a trade-off that conflicts with Beck and McCue's original statement. On one hand, predictive policing may be implemented using as few additional resources as possible, making the argument about cost-efficiency valid. In this case, there is likely to be a lack of interpretability and proper training of personnel, resulting in errors and decisions made on an unjust basis. On the other hand, one could incorporate evaluation procedures and independent auditors, as recommended by Zarsky, as well as implementing a comprehensive training regime to make sure that everyone who are working with the technology are knowledgeable about the analytical process and related issues. This approach, however, will be costly and resource-intensive, to a point where some might question whether the economic costs will outweigh the gains.

7.8.1 Transparency

Besides the possible economic burden, the task of making the algorithmic process transparent is not necessarily a simple one. For obvious strategic reasons, the police would not want their predictive algorithms too transparent, as it might give criminals an advantage. If one wants the algorithms to be understandable by non-experts, the models have to be simplified. Models that are too simplified may have to sacrifice the accuracy that made them desirable in the first place (Ridgeway 2013, 38). It has also been pointed out that a system where one may be apprehended without anyone really being able to explain *why*, opens the door for increasingly Kafkaesque scenarios.[51] Insight into why one has been selected by the algorithmic process may therefore prove essential if predictive policing is to take civil liberties into consideration. As Ferguson points out, some of these concerns are already being addressed in the pilot programs for PredPol. In the program launched by the LAPD, a blind test has been used to determine the actual effects of the system. In addition, there is a continuous monitoring of the project by independent academics and other experts, who are granted insight into the process and the system (Ferguson 2012, 320). The department uses three years of crime statistics, supplementing the older stats with continually updated crime data to ensure that the predictions are relevant. Similar checks and balances could possibly be built into the system, and be implemented as the technology is evolving and negotiated.

7.9 Summing up

Having presented a wide range of actors, groups, arguments, and issues that both overlap and come into conflict with each other, how can the social negotiation around predictive policing be understood in light of the STS literature? For the sake of clarity, I will briefly summarize the analysis thus far. As the clearest example of an undeniably pro-predictive policing group, we find the law enforcement representatives who are eager to bring the technology into wider use. By representing the technology as a matter of resource-allocation and increased policing efficiency, members of this group take the technical achievements of Big Data analytics as sufficient reason to recommend and support its implementation. Furthermore, by addressing the history of law enforcement methods and tools at their disposal, they argue that predictive analytics is simply a natural evolution of the direction that policing has been taking for the last decades. If CompStat and similar Intelligence Led Policing methods have been measurable successes, the increased efficiency and markedly improved statistics of predictive policing seem to speak for themselves as far as this group is concerned.

[51] Morozov (2013) looks at how increasingly automatic bureaucratic processes may lead to improved efficiency at the cost of sacrificing any understanding of what and why decisions are being made.

The technological merits of predictive policing are not as readily accepted by the technology-skeptic group. By pointing out that Big Data has a tendency to black box the analytical process, these critics are concerned about how human error and biases may be hidden behind a shield of objectivity, especially if the technology is widely adopted. Rather than focusing on the budgetary or statistical bottom line, members of this group emphasize that the technological process behind predictive policing must be scrutinized. If the proponents of the technology are unable to properly address these issues, the skeptics cannot accept the artefact as functional. As a more cautionary supporter of Big Data analytics, Tal Zarsky represents another twist on the technological argument. He acknowledges that the sort of problems that the technology-skeptics are concerned about do exist, but points out that similar problems are already common in traditional policing methods. Zarsky proposes that these problems can be remedied if the technology is made interpretable and transparent, allowing for continuous evaluation of the algorithmic process. If this is implemented into the technology, he argues, predictive policing might actually be a means to reduce systemic injustice. This brings Zarsky's argument into the realm of ethics, where groups such as the ACLU are arguing against predictive policing on similar grounds. These groups are worried about these injustices being further entrenched by becoming black boxed with the algorithms, in some ways echoing the technology-skeptics' point about a shield of objectivity.

Putting aside the technological and the ethical implications, Ferguson and Zarsky represent two sides of the negotiation process within a legal context. Ferguson is apprehensive of the technology because, as he sees it, predictive policing might endanger legal principles such as probable cause. If the technology is accepted, then the result may be a crumbling of civil rights and the erosion of the Fourth Amendment. Zarsky takes a different position, acknowledging the problematic aspects, but arguing that the very principles Ferguson are protective of may already be flawed in respect to existing methods. Shifting the issue back to the technology itself, he emphasizes that whereas current methods leave a significant part of police-work at the behest of the individual officer's discretion, the codified and quantifiable nature of Big Data analytics means that predictive policing could make it easier to identify cases in which civil rights are being infringed upon. As Zarsky sees it, the best way to proceed is to implement predictive policing, but with the caveat that a tailored system of checks and balances is introduced. Both Zarsky and Milakovich point out that with the necessary training of individuals, and a sufficiently transparent system, data mining might be the best solution to the problems facing law enforcement (and other governmental institutions). The issue comes full circle when noting that Zarsky and Milakovich's solutions are likely to be quite costly, both in manpower and in terms of economic investments. Thus the original point made by the law enforcement proponents, that predictive policing is the best solution to the problems of lacking manpower and resources, might collapse upon itself.

7.9.1 Group mobilization and closure mechanisms

Over the course of this analysis I have presented a variety of actors, who belong to or are attempting to form social groups around the artefact of predictive policing. By outlining these actors and groups, I have answered my first research question about who the involved social groups are, and consequently demonstrated how these groups all interpret the technology in different ways. It is clear that there is no single correct definition of what predictive policing entails, or what the technology ought to be. I have described how some of these groups mobilize, and how they employ certain closure mechanisms in order to strengthen their position and stabilize (or destabilize) the technology in their own image. The heterogeneity of the groups, and the breadth of different arguments and conflicts, makes an additional look at this process necessary. In the following, I will outline what I have found to be the major closure mechanisms at work in the process, and show how some of the groups may be closer to a reconciliation than it might initially have appeared.

As demonstrated, a main point of contention concerning predictive policing revolves around whether Big Data produces more accurate results than traditional analytical techniques. Representing a narrative where police technologies have been on a historically steady upward trajectory, the law enforcement group stress that predictive policing is just another tool, and simply a marked improvement over methods already in use. If one accepts technological determinism, this would likely be both the beginning and the end of the discussion. Predictive policing is producing better bottom line results than the alternatives, so it is a natural choice for future policing. By presenting a clear problem, and a technological solution that has been shown to produce measurably improved results, the law enforcement group use a rhetorical closure mechanism. In Callon's terms, they problematize the state of current policing, and present predictive policing as the obvious solution. Thus they are trying to stabilize the technology, making it a matter of technological merit and economic results. Interpreted through Dewey's theory, the law-enforcement group attempts to keep predictive policing as a matter that should primarily concern technologists and the police, thereby shielding the technology from being an issue of public concern.

Rather than outright accepting these arguments on technical terms, however, the social group of technology-skeptics disagree with one of the central premises of the law enforcement group's argument. Even if the bottom-line results improve upon older methods, the technology-skeptics call the inner workings of the artefact into question. By questioning the reliability of Big Data analytics, they are attempting to destabilize the conception of the technology put forwards by the law enforcement-group. They redefine the problem; predictive policing cannot simply be explained away as a question of improving the police's available tools. To the technology-skeptics, the budgetary situation of the police is irrelevant because predictive policing technologies are not as accurate and effective as they were originally presented. The main problem is that predictive policing runs the risk of introducing or magnifying existing problems through their uncritical analysis of data. This is a matter for concern not only to the police, but to the public as a whole. If the police are not doing their job properly as a result of bad data, it affects all of society. Therefore, the technology-skeptics are actively articulating predictive policing as a public issue; the potential consequences of bad algorithms are harmful to everyone. Notably, at the time of finishing this thesis, reports that cast doubt on the supposedly measurably improved results of PredPol are appearing. Towards the end of April 2015, the BBC reported that crime statistics were up in Kent County, despite the initial four-month trial period of PredPol having showed signs of improvements in the area (BBC 2015). Although representatives for the County police department blames lack of proper training in the technology for the increase in crimes, this and similar cases could put additional pressure the technology-based argument.

The ethically-minded skeptics of predictive policing are also attempting to destabilize the technology by redefining the problem. If the argument presented by the technology-skeptics is true, then systemic prejudice will be further entrenched under predictive policing, since the complexity of Big Data is liable to become an impenetrable black box of prejudice. This ethical perspective puts the controversy in a new light; predictive policing might not just be inaccurate, it could be immoral. Zarsky, on the other hand, uses his legal expertise to lend weight to his argument, which tacitly accepts the problem presented by the ethics-group. He finds common ground with the both the technology-skeptics and the ethics-group in that they all see potential data errors as a problem. He does not, however, agree with these groups' proposed solutions (which could be simplified as "do not adopt predictive policing"). Instead, Zarsky suggests that certain mechanisms could be built into the artefact in order to secure transparency, thereby mitigating the concern of inaccuracy and entrenched injustice. He agrees with the law enforcement group in that whereas people may have biases, algorithms do not. Therefore, the premises of the arguments made by the ethics- and technology-skeptic groups are invalid as far as Zarsky is concerned. In an effort to close the issue and stabilize predictive policing as an acceptable technology, he suggests a solution to the problem of inaccuracy, and asserts that Big Data has the potential to solve or at least reduce systemic injustice. Problematizing the issue in a similar way as the ethics-group, but presenting solutions to these problems in the form of built-in transparency-enhancing mechanisms and audits, Zarsky's line of argument represents another example of rhetorical closure.

Finally, I have shown how Ferguson attempts to completely redefine the problem by evaluating predictive policing from a legal perspective. Arguing that the technology might be unconstitutional, he invokes the Fourth Amendment as a representational device, cautioning that predictive policing could harm the constitutional rights of citizens. Referring to the constitution and its related principles as standards that predictive policing must adhere to in order to be acceptable, Ferguson warns against implementing the technology. Moving back to the technological perspective, Ferguson acknowledges that aspects of predictive policing may in some cases be preferable to the alternative. Here, he seems to agree with Zarsky, and rather than outright dismissing the technology, he advocates for adapting predictive policing to better preserve principles such as transparency and accountability. Milakovich represents another way of re-opening the debate, by further elaborating the necessary processes required to ensure that predictive policing is used responsibly. In another twist on the technological argument, he claims that if the technology should reach an acceptable standard of transparency and accuracy, resources must be dedicated to ensure that the operating personnel have the necessary training and expertise to understand the technology.

7.9.2 Back to the issues, or politicizing the artefact

During the course of this analysis, Dewey's concept of issue-articulation has been used to demonstrate how predictive policing cannot be separated from a political context. Most of the groups I have looked at have to some degree invoked the public in their arguments. From the ACLU and Ferguson attempting to represent predictive policing as a source of potential harmful consequences, to Beck and McCue's assurances that the public have nothing to fear from the technology, it is clear that predictive policing embodies certain politically charged issues. We know that the algorithmic processes behind predictive policing operate upon data such as crime records, geographical areas, and concepts such as "high risk areas". Although these factors might be reduced to numbers and graphs within the system of predictive policing, they are inseparable from their broader social implications. Take, for example, the high risk areas. As Ferguson notes, the very definition of a high crime area is controversial, especially because it lowers the threshold for how the police are permitted to act. Ripped straight from the headlines, a high profile case such as the death of Freddie Gray while in police custody, which factored in sparking the 2015 Baltimore riots,[52] can be directly traced back to the concept of the "high crime area";

> There is a Supreme Court case that states that if you are in a high-crime area, and you flee from the police unprovoked, the police have the legal ability to pursue you, and that's what they did (…) In this type of an incident, you do not need probable cause to arrest. You just need a reasonable suspicion to make the stop. (police union lawyer Michael Davey, in Schapiro 2015)

It is, of course, impossible to say whether this case could have been prevented if the arresting officers were using PredPol. It might help illustrate, however, that an algorithm operating with concepts that are tied up in legal and social matters, cannot be depoliticized. When

[52] In April 2015, 25 year old Freddie Gray died from injuries sustained in police custody. Gray was apprehended for carrying a switchblade in a designated high crime area. The case garnered a lot of publicity, raising questions of police brutality and racism, but also about whether the arrest was warranted in the first place (Sterbenz 2015).

Dewey refers to the public forming in order to solve conflicting issues, the issues at hand first must be articulated. The codified nature of algorithmic systems give Dewey's theory a new dimension. As we have seen, the complexity of Big Data systems have the potential to black box these issues within the technology, effectively obscuring the political aspects, and leading to potential problems such as shields of objectivity. On the other hand, if mechanisms and functions are in place in order to secure transparency, the technology might be scrutinized and these articulations can be made public. If a case such as the Freddie Gray death happens while predictive policing is in use, it might be possible to identify the exact data points that led to the arrest, and consequently this information could be used both to assign some form of accountability, and to prevent similar incidents by readjusting the algorithms. In any case, predictive policing could assist in articulating institutional problems, as long as the proper mechanisms and regulations are in place in order to ensure that these articulations are made visible.

7.9.3 Reflections on the use of STS

Over the course of my analysis, I have attempted to give an in-depth account of the process in which technology and social factors constitute each other, thereby illustrating how predictive policing should not be separated from its societal and political context. For my theoretical basis, I have combined the STS methods SCOT and ANT, in order to give a more dynamic and nuanced picture of the process. My use of the theories, however, has not been without certain drawbacks. As noted, the SCOT method is limited by the somewhat static notion of technological frames. By eschewing the use of this concept, in favor of Callon's more process-oriented approach, I wanted to demonstrate how social groups are ongoing processes of continuous negotiation, rather more rigid structural concepts. Because I have chosen to follow actors ranging from large organizations to single individuals, the theoretical consistency has been challenging. One reason for this is that the SCOT theory is often applied to retrospective case studies, where social groups are more clearly defined, while ANT is better suited for ongoing controversies. Therefore, the more rigid SCOT-concept of social groups seems better suited to organizations such as the police or the ACLU, while the more actor-focused ANT is more appropriate for actors such as Zarsky or Ferguson and their attempts to mobilize a network without explicitly defining a group.

In the end, Winner's criticism of SCOT's seemingly arbitrary division of people into "relevant social groups" might still apply to some degree. However, my goal has not been to give a comprehensive account of every actor that might be relevant to the technology. As a means of demonstrating how technologies have important aspects beyond their material functionality, the provisional identification of relevant actors or groups seems justified. The exact constitution of the groups could probably be diced up in many different ways, but I believe that the conclusion of the analysis would be similar. In my case, outlining the diversity of agendas, opinions, and meanings assigned to the artefact seems sufficient. This thesis lays the groundwork for an STS approach to Big Data technologies, but because of its scope, it would be impossible to give a complete account. If I had the time and space at my disposal, a more comprehensive use of ANT might uncover even further political avenues for debate embedded within PredPol. In a few years, if predictive policing becomes a possibility also in a Norwegian context, a more hands-on study of the ongoing discussion would undoubtedly cast further light on the social aspects of the technology. For a case-study based on textual sources, however, I believe that SCOT, ANT, and Dewey have been helpful and appropriate companions.

8 Conclusion

8.1 Reflections on the analysis and suggestions for future research

As Big Data analytics are becoming prevalent in increasingly broader areas of western society, the drive for new technologies often overshadow the practical consequences. Law enforcement agencies around the world are facing pressure, both on political and economic grounds, making technological solutions increasingly attractive because of their apparent efficiency and elegance. Technologies such as body-mounted cameras and GIS tracking are only some of the artefacts that may change the ways that the police work, and with the introduction of predictive policing, new questions arise. Technology scholars and civil rights organizations are questioning the technocratic aspects of applying these technological “quick fixes”, noting that artefacts such as predictive policing could be ignoring underlying social issues, or even perpetuating existing problems, in favor of overeager techno-optimism.

On the other hand, some proponents of the technology are arguing that predictive policing is only meant to supplement already existing policing methods, and should not be interpreted as an easy way out of addressing broader issues. After all, Big Data analytics operates by processing already available data, continuing traditional police work with increased capacity and accuracy. When engaging with this variety of arguments and interpretations of the technology, one could easily conclude that the debate is simply a matter of conflicting views of how technology should be used. The sheer variety of voices and arguments put forth, however, reflects one of the STS-field’s central ideas – that technologies cannot be properly addressed in isolation from their social context. By taking into consideration arguments and concerns presented by actors as diverse as police chiefs, civil rights organizations, and technologists, a picture of predictive policing appears that is much more nuanced than a passing glance might indicate. The controversy surrounding the technology demonstrates that predictive policing cannot be judged solely on its technological merits, the ethical conundrums it raises, or by referring to legal precedents.

In line with Dewey's theory, the conflicting views of the technology provides an avenue where a public may form, since by articulating issues as diverse as racial profiling, techno-optimism, and the flexibility of the threshold for probable cause, a wide variety of actors are implicitly affected by the consequences of predictive policing (Dewey 1927, 27). If these issues are not solvable by reference to existing social institutions, it might be time for a public debate concerning the use of predictive policing, and by extension Big Data technologies for governmental purposes. As these issues are unlikely to go away by themselves, barring a successful movement of rhetorical closure or black-boxing of the artefact, it seems like the time is ripe for public engagement with the consequences of the technology. The White House administration have already engaged with the public concerning the use of Big Data (Podesta 2014), and similar forums are likely to follow elsewhere. Although it is outside of the scope of this thesis, Michel Callon proposes to involve the public in issues of sociotechnical controversy by the use of what he calls "hybrid forums" (Callon, Lascoumes, and Barthe 2009, ch. 1). Applying the ideas of the hybrid forum to Big Data technologies, meaning that laypeople, experts, and politicians interact in order to consider the variety of views and potentially affected actors, could be an interesting avenue to follow up in further research. The sheer complexity of Big Data will undoubtedly necessitate that the participating and otherwise affected actors are sufficiently trained to ensure comprehensibility, but this is not an unsurmountable obstacle. In any case, the sheer magnitude and momentum of Big Data suggests that interaction and proper communication about the technology should take place sooner rather than later. By merit of being an interdisciplinary field, STS provides helpful tools and concepts in order to transcend the boundaries between technology and the social. As the technologies grow increasingly complex, we should take care that we do not take the black boxing of Big Data for granted. If the technology is black boxed, the potential for issue-articulation is liable to vane. With the proper personnel training and transparency-enhancing mechanisms, however, the codified nature of predictive policing could be used to gain further understanding of the social and political processes implicated in its algorithms.

8.2 Concluding remarks

In this thesis I have examined the technological artefact of predictive policing, taking the initial PredPol pilot projects in Los Angeles as my basis. Rather than treating the technology itself as a stable entity, I have unpacked and explained the algorithmic functions that calculate the predictions, as well as looking at some possible practical consequences of its use. Proponents of the technology are eager to implement it for police districts all over the US, and similar projects are already under way in the UK and is being considered in Australia.[53] Since the sheer complexity of Big Data makes predictive policing difficult to understand on a significant level beyond "data goes in, predictions come out", I have dedicated significant space to present the *how* of how it works. My first two research question are concerned with identifying the actors and social groups who are driving the debate around the technology, and highlighting the methods these groups use in order to shape predictive policing in their own image. Representatives for the police, for marginalized public groups, and for the legal system have been considered, and I have demonstrated how these groups interpret both the technology and its potential problems in sometimes drastically different ways. The groups have attempted to mobilize and recruit other actors to their point of view by representing the technology either as a suitable solution to existing problems, or as a source of further problems. Although some of them argue directly against each other, it is not uncommon that the groups do not even agree on what the relevant factors should be when assessing the technology.

With my third and final research question, I wanted to explore how technological artefacts can be inseparably bound up with political issues. When representatives of the police characterize predictive policing as just another tool, they are attempting to avoid any political discussion of the technology. If technology is accepted as simply a material device, then technological determinism might follow, where technologies are only evaluated on their technical efficiency and ease of implementation. By turning to groups concerned with civil liberties, however, I have shown that things are not always as simple as they seem. By embedding issues such as racism and classism into their interpretation of the technology, groups such as the UCLA are attempting to make the technology a public issue. Taking this point one step further, the codified nature of Big Data could mean that underlying social issues are explicitly articulated within the algorithms. The question then becomes whether these articulated issues should be allowed to become public issues, by allowing transparency and insight into the technology. If predictive policing is made sufficiently transparent, these articulations could bring otherwise

[53] As noted in Moses and Chan (2014, 645)

hidden issue into the public light. This transparency will, however, likely come at the price of increased costs, lower complexity, and possibly lower accuracy. Without the transparency, the issues will remain sealed within the black box of the algorithms. It remains to be seen whether predictive policing becomes widely regarded as a successful technology, and if it does, which version of the technology we will end up with. The only thing that seems certain, is that the outcome remains subject to change.

9 Bibliography

Alvino, Chris; Basilico, Justin. *Learning a Personalized Homepage*. The Netflix Tech Blog, 09.04.2015 [cited 15.05.2015]. Available from http://techblog.netflix.com/2015/04/learning-personalized-homepage.html.

Anderson, Chris. *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*. Wired Magazine, 23.06.2008 [cited 10.05.2015]. Available from http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory.

BBC. *Predicting crime 'cut Medway street violence by 6%*. BBC News, 14.08.2013 [cited 12.05.2015]. Available from http://www.bbc.co.uk/news/uk-england-kent-23689715.

BBC. *Kent crime up despite new 'predictive policing' tool*. BBC News, 30.04.2015 [cited 12.05.2015]. Available from http://www.bbc.co.uk/news/uk-england-kent-32529731.

Beck, Charlie; McCue, Colleen. 2009. "Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession?" *The Police Chief Magazine* no. 76 (11):18-20.

Bijker, Wiebe E. 1993. "Do not despair: there is life after constructivism." *Science, technology & human values* no. 18 (1):113-138.

Bijker, Wiebe E. 2006. "Why and how technology matters." In *Oxford handbook of contextual political analysis*, edited by Robert E.; Tilly Goodin, Charles, 681-706. Oxford University Press.

Bijker, Wiebe E. 2010. "How is technology made?—That is the question!" *Cambridge Journal of Economics* no. 34 (1):63-76.

Bijker, Wiebe E, Thomas P Hughes, and Trevor J Pinch. 1987. *The social construction of technological systems: New directions in the sociology and history of technology*: MIT Press. Reprint, 2012.

Bollier, David, and Charles M Firestone. 2010. *The promise and peril of big data*: Aspen Institute, Communications and Society Program Washington, DC, USA.

Boyd, Danah, and Kate Crawford. 2012. "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon." *Information, Communication & Society* no. 15 (5):662-679.

Britannica, Encyclopædia. *Fourth Amendment*. Encyclopædia Britannica Inc. Available from http://www.britannica.com/EBchecked/topic/215219/Fourth-Amendment.

Byrne, James, and Gary Marx. 2011. "Technological innovations in crime prevention and policing. A review of the research on implementation and impact." *Journal of Police Studies* no. 20 (3):17-40.

Calabrese, Chris. *When Big Data Becomes a Civil Rights Problem*. American Civil Liberties Union [cited 27.06.2014]. Available from https://www.aclu.org/blog/when-big-data-becomes-civil-rights-problem.

Callon, M, P Lascoumes, and Y Barthe. 2009. Acting in an uncertain world: An essay on technical democracy (G. Burchell, Trans.). Cambridge, MA: MIT Press.

Callon, Michel. 2007. "Some Elements of a Sociology of Translation." In *The Politics of Interventions*, edited by Kristin; Brenna Asdal, Brita; Moser, Ingunn, 57-78. Oslo, Norway: Oslo Academic Press, Unipub Norway.

Callon, Michel, and John Law. 1997. "After the individual in society: Lessons on collectivity from science, technology and society." *Canadian Journal of Sociology* no. 22 (2):165-182.

Collins, Harry M. 1987. "Expert systems and the science of knowledge." In *The social construction of technological systems: New directions in the sociology and history of technology*, edited by Wiebe; Hughes Bijker, Thomas; Pinch, Trevor, 329-348. MIT Press.

Datatilsynet. *Big Data - Personvernprinsipper under press*. Teknologirådet, 2013. Available from https://www.datatilsynet.no/Global/04_planer_rapporter/Big%20Data_web.pdf.

Dewey, John. 1927. *The Public and its Problems*. Athens, OH: Swallow Press/Ohio University Press. Original edition, 1927. Reprint, 1991.

Dick, Philip K. 2002. *The Minority Report: And Other Classic Stories*. Vol. 4: Citadel Press.

Ferguson, Andrew Guthrie. 2012. "Predictive Policing and Reasonable Suspicion." *Emory Law Journal* no. 62:261-325.

Ferguson, Andrew Guthrie; Bernache, Damien. 2008. "The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis." *American University Law Review* no. 57 (6):1587-1644.

Fernandez, Belen. *Baltimore: On the domestic frontlines*. Al-Jazeera, 01.05.2015 [cited 02.05.2015]. Available from http://www.aljazeera.com/indepth/opinion/2015/05/baltimore-domestic-frontlines-150501052022670.html.

Frampton, Will. *After four months, Norcross police happy with predictive policing*. CBS Atlanta, 09.01.2014 [cited 12.05.2015]. Available from http://www.cbs46.com/story/24198083/after-four-months-norcross-police-happy-with-predictive-policing.

Friend, Zach. *Predictive Policing: Using Technology to Reduce Crime*. FBI Law Enforcement Bulletin [cited 24.09.2014]. Available from http://leb.fbi.gov/2013/april/predictive-policing-using-technology-to-reduce-crime.

Gorner, Jeremy. *Chicago police use 'heat list' as strategy to prevent violence*. Chicago Tribune, 21.08.2013 [cited 01.05.2015]. Available from http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list.

IBM. *IBM Smarter Cities Public Safety—Law Enforcement*. IBM Corporation, May 2012 [cited 29.10.2014]. Available from https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-smartercom_medium&S_PKG=ov16797&S_TACT=103HX07W&dynform=7401&lang=en_US.

Inderhaug, Erik. *Framtidens forebygging*. PolitiForum [cited 16.02.2015]. Available from http://www.politiforum.no/Framtidens+forebygging.d25-T2djGZ9.ips.

Keulartz, Jozef, Maartje Schermer, Michiel Korthals, and Tsjalling Swierstra. 2004. "Ethics in technological culture: a programmatic proposal for a pragmatist approach." *Science, technology & human values* no. 29 (1):3-29.

Khan, Dost Muhammad, Nawaz Mohamudally, and D. K. R. Babajee. 2012. "Towards the Formulation of a Unified Data Mining Theory, Implemented by Means of Multiagent Systems (MASs)." In *Advances in Data Mining Knowledge Discovery and Applications*, edited by Adem Karahoca, 3-42. inTech.

Kile, Meredith. *Predictive policing technology lowers crime rates in US cities*. Al-Jazeera America, 15.09.2013 [cited 12.05.2015]. Available from http://america.aljazeera.com/watch/shows/techknow/blog/2013/9/15/predictive-policingtechnologylowerscrimeratesinuscities.html.

Levine, Harry; Gettman, Jon; Siegel, Loren. 2010. Targeting Blacks for Marijuana-Possession Arrests of African Americans in California, 2004-08. Los Angeles: Drug Policy Alliance.

Linden, Greg, Brent Smith, and Jeremy York. 2003. "Amazon. com recommendations: Item-to-item collaborative filtering." *Internet Computing, IEEE* no. 7 (1):76-80.

Mackenzie, Dana. *Predictive Policing*. Society for Industrial and Applied Mathematics [cited 19.09.2014]. Available from http://www.siam.org/news/news.php?id=1953.

Marres, Noortje. 2005. "Issues spark a public into being: A key but often forgotten point of the Lippmann-Dewey debate." In *Making Things Public*, edited by Bruno; Weibel Latour, Peter, 208-217. MIT Press.

Marres, Noortje. 2007. "The issues deserve more credit: Pragmatist contributions to the study of public involvement in controversy." *Social Studies of Science* no. 37 (5):759-780.

Maryland, University of. *What is CompStat?* [cited 02.03.2015]. Available from http://www.compstat.umd.edu/what_is_cs.php.

Milakovich, Michael. 2012. "Anticipatory Government: Integrating Big Data for Smaller Government." *Internet, Politics, Policy 2012: Big Data, Big Challenges*.

Morozov, Evgeny. *The real privacy problem*. MIT Technology Review [cited 20.10.2014]. Available from http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/.

Moses, Lyria Bennett, and Janet Chan. 2014. "Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools'(2014)." *University of New South Wales Law Journal* no. 37:643-650.

Pentland, Alex, and Andrew Liu. 1999. "Modeling and prediction of human behavior." *Neural computation* no. 11 (1):229-242.

Perry, Walt L. 2013. *Predictive policing: The role of crime forecasting in law enforcement operations*: Rand Corporation.

Pinch, Trevor J, and Wiebe E Bijker. 1984. "The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other." *Social studies of science*:399-441.

Podesta, John; Pritzker, Penny; Moniz, Ernest; Holdren, John; Zients, Jeffrey. 2014. Big Data: Seizing Opportunities, Preserving Values. edited by Executive Office of the President.

Politidirektoratet. 2012. 22. juli 2011: Evaluering av politiets innsats Oslo: Politidirektoratet.

PredPol. *About Predictive Policing* [cited 31.03.2014]. Available from http://www.predpol.com/about/.

PredPol. 2014. *Scientifically Proven Field Results*, n/d [cited 24.09.2014]. Available from http://www.predpol.com/results/.

PrivacySOS. *What's Predictive Policing?* PrivacySOS [cited 31.03.2014]. Available from https://www.privacysos.org/predictive.

Reich, Kenneth. *Predicting Aftershocks*. Los Angeles Times, 15.06.2002 [cited 24.09.2014]. Available from http://articles.latimes.com/2002/jul/15/science/sci-seismic15.

Ridgeway, Greg. 2013. "The pitfalls of prediction." *NIJ Journal* no. 271:34-40.

Ritter, Nancy. 2013. "Predicting Recidivism Risk: New Tool in Philadelphia Shows Great Promise." *NIJ Journal* no. 271:4-13.

Rubin, Joel. *Stopping crime before it starts*. Los Angeles Times [cited 21.09.2014]. Available from http://articles.latimes.com/2010/aug/21/local/la-me-predictcrime-20100427-1.

Russell, Stewart. 1986. "The social construction of artefacts: a response to Pinch and Bijker." *Social Studies of Science* no. 16 (2):331-346.

Schapiro, Rich. *Baltimore police did not need 'probable cause' to arrest Freddie Gray*. New York Daily News, 22.04.2015 [cited 02.05.2015]. Available from http://www.nydailynews.com/news/crime/lawyer-defends-baltimore-police-freddie-gray-arrest-article-1.2195234.

Steen, Marc. 2014. "Upon opening the black box and finding it full: Exploring the ethics in design practices." *Science, Technology & Human Values* no. 3:389-420.

Sterbenz, Christina. *A 'big question' surrounds the arrest of Freddie Gray, which sparked riots across Baltimore*. Business Insider, 30.04.2015 [cited 12.05.2015]. Available from http://www.businessinsider.com/did-police-have-a-right-to-stop-freddie-gray-2015-4.

Technologies, Rose Business. *Data Management Maturity Stages* [cited 26.02.2015]. Available from http://www.rosebt.com/blog/category/database%20management%20systems/2.

Timmer, John. 25. *Why the Cloud Cannot Obscure the Scientific Method*. Ars Technica, 26.06.2008 [cited 15.05.2015]. Available from http://arstechnica.com/uncategorized/2008/06/why-the-cloud-cannot-obscure-the-scientific-method/.

Townsley, Michael, Ross Homel, and Janet Chaseling. 2003. "Infectious burglaries. A test of the near repeat hypothesis." *British Journal of Criminology* no. 43 (3):615-633.

Uchida, Craig D. 2009. A national discussion on predictive policing: Defining our terms and mapping successful implementation strategies. National Institute of Justice.

Williams, Robin, and David Edge. 1996. "The social shaping of technology." *Research policy* no. 25 (6):865-899.

Willis, James J, and Stephen D Mastrofski. 2011. "Innovations in policing: Meanings, structures, and processes." *Annual Review of Law and Social Science* no. 7:309-334.

Winner, Langdon. 1993. "Upon opening the black box and finding it empty: Social constructivism and the philosophy of technology." *Science, Technology, and Human Values* no. 18 (3):362-378.

Yin, Robert K. 2009. *Case study research: Design and methods*: Sage publications.

Yiu, Chris. 2012. *The big data opportunity: Making government faster, smarter and more personal*: Policy Exchange.

Zarsky, Tal Z. 2011. "Governmental data mining and its alternatives." *Penn St. L. Rev.* no. 116:285.