Data-driven policing:

how digital technologies transform the practice and governance of policing

Daniel Marciniak

A thesis submitted for the degree of Doctor of Philosophy in Sociology

Department of Sociology

University of Essex

March 2021

Abstract

Adoption of advanced digital technology is one of the most controversial and fundamental transformations in contemporary police practice. Despite its significance, empirical enquiry of these technologies, and the way they shape and are shaped by policing environments is rare. Drawing on in-depth interviews with officers in a UK police force and ethnographic fieldwork in a large metropolitan police department in the US, this thesis aims to make a significant empirical and conceptual contribution to this emerging field. It reveals the multifaceted character of data-driven technology in policing and the complex socio-technical negotiations that take place in these operational environments.

In the UK case study, data visualisation and predictive policing techniques have been adopted to reduce service demand and prioritise actions in the context of austerity-driven budget cuts. In the US, following a federal consent decree addressing varied civil rights grievances, compliance monitoring requirements have brought about rapid datafication and digitisation of many policing tasks including a radical adaptation of existing CompStat processes. Although both police forces employ similar arsenals of digital tools, these fuel very different types of policing: Within a mind-set of crime-fighting, US applications emphasise targeted surveillance and territorial patrol. In the UK, officers seek a balance between enforcement and finding support through social services.

Contrary to common techno-deterministic descriptions of predictive and digital policing, this research finds complex co-constructions of risk, suspicion, and priorities that are contingent on operational settings. In such settings, calculative and experiential knowledge intersect in discretionary decision-making. Yet the data reveals how technologies also have affordances: risk scores institutionalise a focus on repeat offenders, crime statistics drive competition between districts, and digital records shape the possibilities of policing. In other respects, the socio-technological relationships are often fragile: computer systems crash, display inaccurate information, and officers improvise workarounds. With increasing police reliance on production, processing, and interpretation of data, such insights demonstrate the complex ways police organisations become implicated in the outcomes of digital policing.

Acknowledgements

This thesis would not have been possible without the support of the people around me. I am grateful for the financial support provided by the Human Rights, Big Data and Technology project. My thanks go to the following people:

My supervisors Prof Pete Fussey and Dr Daragh Murray for their continued encouragements, thought-provoking comments, and advice.

Prof Nigel South for his guidance and support as my chair.

Dr Mark Maguire and Prof Eamonn Carabine for their insightful comments during the viva.

Prof Ewa Morawska, Prof Linsey McGoey, Prof Yasemin Soysal, and Dr Anna Di Ronco for the helpful feedback and career advice during the PhD colloquiums.

My colleagues and friends on the Human, Rights and Big Data project for all the interesting conversations. Particularly to Prof Ajay Sandhu for helping me navigate academia and fieldwork.

My PhD colleagues and office mates. You have made me feel at home.

Prof Endre Dányi, Prof Susanne Bauer, and Prof Christian Stegbauer for encouraging me in starting the PhD.

The participants of the surveillance studies summer schools in Kingston and St Andrews for giving me a sense of academic community.

Dr Maria Sapignoli for giving me the room to finalise my thesis while beginning an exciting new research project.

Cath Kent and Penny Castagnino on the HRBDT project, as well as the sociology admin team for their administrative support.

The university library and campus. I have discovered many of the cited readings browsing the library's well-sorted book-shelves and having an office on campus during the first year made my accommodation bearable.

The NHS nurses who kept me well, and the delivery drivers that brought food during the COVID lockdown.

My family for supporting me throughout and challenging me to explain my work to them in plain terms.

Alice for her love and her patience with me.

Most importantly, without the kind participation of the many police officers, police staff, and other interviewees this thesis would not exist. You have greatly broadened my thinking on many of the issues discussed in this work and I hope you find your views represented accurately and fairly.

Table of Contents

1. Introduction

From whistle, to call box, to car, to siren, to radio, to modern-day information technology; technology shapes to a large extent the character of modern policing (Deflem and Chicoine, 2014). Lately, the Black Lives Matter protests spreading from the United States around the globe have reinvigorated calls to 'defund the police' to allocate resources elsewhere (see e.g. Sharkey, 2020; Thompson, 2020; Vitale, 2017; Yglesias, 2020) and caused a backslash to companies producing technologies for the police with Amazon, IBM, and Microsoft halting sales of facial recognition tools (see e.g. Fitch, 2020; Heilweil, 2020). Previously, predictive policing and the use of artificial intelligence fuelled a public discourse on the promises and perils of digital technologies in policing often drawing on utopian and dystopian imaginaries. These debates will shape the direction of law enforcement in the 21st century. Yet, there is a dearth of research into the role of technology in policing that goes beyond evaluating intended effects or theoretical, often techno-deterministic, accounts (Brayne, 2017; Brayne and Christin, 2020; Koper and Lum, 2019).

This thesis situates the concerns for digital technologies in policing among numerous sociological accounts from the last thirty years diagnosing a society increasingly governed by metrics of all sorts: It includes David Lyon's accounts of the routine electronic data collection in a 'surveillance society' (Lyon, 1994), as well as the technologically facilitated 'social sorting' (Lyon, 2003) aimed at influencing and managing populations. It is Michael Power's (1997, 2000) 'audit society' describing a change from direct control to self-regulatory oversight through performance measures created in auditing processes (in the public sector associated with 'New Public Management' (Hood, 1991)). Wendy Espeland and Mitchell Stevens (2008) call for a 'sociology of quantification' analysing the production and communication of numbers and how their implicit valuation intervenes and disciplines. More recently, David Beer's (2016) 'metric power' locates the productive power of metrics shaping what is deemed valuable within the context of sustaining the competitive logic of neoliberalism. Jerry Muller (2018) describes in 'Tyranny of Metrics' the dysfunctional, managerial fixation with numerical indicators aimed at replacing professional judgement and controlling behaviour through penalties and rewards.

There is also a rich literature based on concrete examples of governance by metrics. For example, Oscar Gandy (2009) draws on examples from insurance to housing, health care, and criminal justice in pointing to the racialized, 'cumulative discrimination' inherent to statistically derived categories of risk. Frank Pasquale (2015) describes in 'black box society' how the opaque and biased algorithms employed by the big online companies of the likes of Facebook, Amazon and Google, as well as the finance industry determine our reputations and finances, Deborah Lupton (2016) interprets quantified self-tracking as producing the neoliberal, individualized self that centres on personal management and responsibility rather than social life chances, Cathy O'Neil (2016) draws on a wide range of examples to highlight the damages inflicted by opaque and scaled up 'weapons of math destruction', Virginia Eubanks (2018) describes in 'Automating Inequality' the 'digital poorhouse' of America in which automated, digital, opaque, and unaccountable decision making processes in public services erode social safety, criminalize poverty and intensify discrimination, Ruha Benjamin (2019) tackles with the 'New Jim Code' the seemingly objective algorithms reinforcing racial discrimination, and Charlton McIlwain (2019) traces the history of the use of computers in allocating police forces according to racialized geo-statistics back to the 1960s.

Of course, the role of numbers in how power operates is not new. Ian Hacking (1982), for example, draws on Foucault's concept of 'biopower' placing the increase of categorisation fundamental for population statistics in the mid-18th century, and Theodore Porter (1996), analysing the time from 1830 onwards, identifies a drive toward quantification in the search of creating mechanical objectivity as a resource of power and trust. Criminal justice and law enforcement form an area in which many of these issues at the intersection of technology, society and citizenship are most acute. At the beginning of the 1990s Feeley and Simon (1992, 1994) coined the terms ‘new penology’ and ‘actuarial justice’ to describe a process parallel to this literature: a shift to managerialism focussed on a reduction of policing aims to indicators of internal procedures and a fixation on risks of populations instead of professional assessment of the individual. These accounts highlight the connection between (quantified) knowledge – proliferated by today’s ubiquity of computers – and its capacity for power.

The literature highlighting the power of numbers regularly takes a rather techno-deterministic stance in which calculative devices successfully shape human action or outright replace human decision-making. This is also reflected in the example of predictive policing: champions of the technology not only celebrate a fantasy of efficacy, but they also see it as a step towards eradicating human bias in the criminal justice system; critics, on the other hand, fear a mechanical application of machine decisions imbued with biases hidden in the opacity of a black-box algorithm. These binary perspectives are seldom informed by any empirical engagement with messy operational practices (Sandhu and Fussey, 2020). Contrarily to these accounts, technological practices are rarely as straightforward but rather produce various moments of friction. Prominently, Manning (2008) demonstrates for the use of crime mapping (i.e. spatial statistics) in CompStat meetings that the way technology is used in policing is largely contingent on how it fits with existing processes and power structures. Thus, this thesis contributes closer attention to technologies in practice: to its affordances in officer discretion, to the spatio-temporal conditions underpinning day-to-day police practice, as well as the myriad of breakdowns and fragmentations that occur. Attending to the affordances of technology in discretionary decision making significantly extends the focus on human factors in the policing literature (Dymond, 2019), and the theme of breakdowns not only cautions against the durability of artefacts often assumed in science and technology studies but also challenges accounts of a unified ‘surveillant assemblage’ (Haggerty and Ericson, 2000) and similar accounts relying on the fantasy of flawlessly functioning technologies. Particularly in this last aspect, the argument is somewhat similar to Manning’s (2008). But by tracing police actions beyond strategy meetings into the practice of frontline officers this research goes a long way beyond his study. Including investigatory practices, it further contributes to a largely understudied aspect of policing (see Manning, 2008: 197).

The literature mostly looks at specific technologies, often from a speculative and techno-deterministic perspective. By contrast, this thesis seeks to contribute an empirical understanding of the wider setting of digital policing. Two case studies from the United States and the United Kingdom give unique insight into the richness and diversity of technological practices. The research reveals the myriad ways in which aspects of the organisations and features of the technologies shape each other as well as policing practices including strategic decision-making, discretion, and investigations.

The thesis is structured as follows: The literature review in chapter 2 continues the argument outlined here. Based on the academic discourse and empirical findings discussed here, it develops a conceptual framework that enables the empirical engagement with the dynamic and emerging field of technology in policing. It is followed by a short note on the methodological approach and reflections on the fieldwork in chapter 3.

Based on extensive ethnographic engagement with a large metropolitan police department in the United States, chapters 4, 5, and 6 interrogate the interplay and fragmented nature of technological practice in policing from strategy making, to patrol and calls-for-service, to investigations. The first chapter addresses the idiosyncratic knowledge practices through which crime and accountability numbers are created, interpreted, and translated into actions. The second foregrounds the affordances of technologies for officers on patrol and answering calls-for-service, with a specific focus on the role of police databases in suspicion formation and discretionary decision-making. The third chapter analyses how the technologies' spatio-temporality of recording infrastructure and past police activities shapes the possible avenues for investigations and engages with legal and ethical concerns arising from the unprecedented availability of digital records.

Drawing on in-depth interviews with members of a British police force, chapters 7 and 8 examine the affordances of a data visualisation platform introduced to reduce demand in the context of austerity measures applied to police and social services. The first chapter investigates its role in decision-making and contributes a perspective of co-construction to understand the use of individualised risk scores. The second chapter scrutinizes how the software institutionalises a focus on risky individuals, redistributes knowledge, and reorders performance management.

The last chapter discusses the findings along the lines of data collection, strategic decision-making, day-to-day policing practice, and oversight. It highlights four concerns for future research and police practice: 1) the effects of categorizations on knowledge and organisational structure, 2) attention to temporal affordances of technologies, 3) needed policies for data access and use, and 4) technological fixes may help police cope with demand but cannot address larger underlying social issues. Collectively, these chapters will demonstrate the multi-faceted nature of digital policing practice and contribute an empirical perspective to the wider discourse on the promises and perils of the adoption of new technologies in policing.

2. Literature review

The aim of this chapter is not to give a comprehensive review of all the literature relating to all the different technologies encountered in the following chapters. Rather, the chapter first introduces CompStat – a management system by which mid-level staff are held accountable to crime statistics – and predictive policing – the automated allocation of resources in areas or for individuals deemed at risk – as the basis for the theoretical arguments that follow and as cornerstones of the debate on digital tools in policing. It then picks up the grand narratives identified above to introduce two main lines of inquiry that are central to understanding how technology works in police operational practice and that provide a conceptual toolkit that underpins the analysis of this socio-technological practice beyond assumed effects. The first line of inquiry concerns the organisation of power and its interplay with situated and quantified types of knowledge. Towards this goal, the second section, taking Feely and Simon's (1992, 1994) observation of a development towards 'actuarial justice' as a starting point, uses Latour's (1987) concept of 'centres of calculation' and an empirically informed classification of five associated ways of knowing to develop a theoretical lens through which the quantitative knowledge of governance described by Foucault (2003, 2009, 2010) as 'biopower' can be studied in its practical consequences. Finally, the second line of inquiry introduces discretion, spatio-temporality, and breakdown as theoretical frames for studying police officers' interactions with technology. Following Manning's (2008) empirically founded scepticism towards the changes brought about by the introduction of crime mapping and information technology in policing, these lay the foundation for an empirical counterpoint to the often utopian or dystopian, and largely theoretical narratives on technology in policing.

2.1.CompStat and predictive policing as a lens on technology in policing

CompStat and predictive policing are some of the main technologies discussed in the empirical chapters of this thesis and, as outlined above, serve as entry points to the theoretical framing of technology in policing. This section gives a brief overview of the two technologies and the questions on the role of quantitative knowledge in police governance and officer decision making that they have elicited.

CompStat is a system for police management that combines the regular update of digital crime data with meetings in which 'middle managers' such as district commanders are held accountable to this data and have to justify the actions they have taken to address crime in their areas (Willis, 2014). Introduced by Jack Maple to the New York Transit Police and adopted by William Bratton to the whole New York Police Department when he became commissioner in 1994, CompStat has been credited by its proponents with causing a decline in crime in New York and has been widely adopted (Weisburd et al., 2003). Critics of CompStat have been sceptical towards claims of crime reduction (e.g. Eck and Maguire, 2005; Harcourt, 2001), have highlighted the association with problematic policing strategies like zero-tolerance policing and stop and frisk exacerbated by quantified performance measures (e.g. Bowling, 1999), and have questioned the degree to which CompStat processes have actually transformed police practice (Manning, 2008; Weisburd et al., 2019). Especially Manning's (2008) work is an example of the necessity of ethnographic empirical research to determine the difference between discourse and practice. The issue of effectivity aside, the example of CompStat thus raises questions on the degree to which the public success stories in policing represent meaningful change and highlights the emerging importance of crime numbers not merely for understanding and addressing crime but as a managerial technique by which officers are held accountable.

As an attempt to quantitatively organise police work, CompStat can be interpreted as a precursor to predictive policing (Willis, 2014; Wilson, 2020). According to one of the earliest reports on predictive policing, predictive policing refers to the use of a wide range of techniques "[…] to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions" (Perry et al., 2013: 1). Notorious examples of predictive policing include the company PredPol that sells software for the prediction of areas likely to experience crime and the management of subsequent patrols (PredPol, 2016) and Chicago's now-discontinued "heat list" that provided a risk score for individuals on the department's database (Foody, 2020; Saunders et al., 2016). While actuarial tools like COMPAS and patrol deployments based on crime statistics in the CompStat process have a long history in the criminal justice system (Feeley and Simon, 1994; Harcourt, 2007; Willis and Mastrofski, 2012), increased accessibility, new methods of analysis and automation have spurred interest in predictive policing both from proponents and critics.

Early on, Charlie Beck, then chief of the Los Angeles Police Department, and Colleen McCue (2009) hyped predictive policing as 'the next era in policing' and drew parallels to the increases in efficiencies companies like Walmart and Amazon had achieved through data analysis – a proposition that was all too welcome given budget cuts to policing in the wake of the 2008 financial crisis. The term quickly attracted media reports likening predictive policing to the movie Minority Report and celebrating astonishing crime reductions (e.g. Frangoul, 2013). However, just as much as the term caused hopes for police forces to reduce crime, it spurred a critical debate on the use and misuse of data in policing. With concerns around the quality of the underlying data in terms of errors, underreported crimes, and discriminatory biases, as well as feedback loops focussing attention where it has been before, critics argued that predictive policing may be nothing more than a high-tech justification for racial profiling (Ferguson, 2017a, 2017b; Joh, 2016; Lum and Isaac, 2016; Raso et al., 2018; Richardson et al., 2019; Sanders et al., 2015; Scannell, 2019). Other concerns relate to the lack of transparency and accountability that these systems afford – especially when the underlying algorithms are owned by private companies and protected by copyright law or nondisclosure agreements (Ferguson, 2017a; Joh, 2016; Raso et al., 2018).

Beyond the concerns around predictive policing, mostly voiced in law journals, the academic discourse on predictive policing is mostly limited to either the development and evaluation of predictive policing technologies themselves (e.g. Gerstner, 2018; Mohler et al., 2015; Saunders et al., 2016), or theoretical discussions of the extent to which predictive policing constitutes a turn towards a pre-crime society (Lawrence, 2017; Mantello, 2016; McCulloch and Wilson, 2015; van Brakel and De Hert, 2011; Wilson, 2020; Zedner, 2007) or a new style of policing marked by its public-private relations and termed ‘platform policing’ (Egbert, 2019; Linder, 2019; Wilson, 2019). There are only a few notable exceptions to this: Based on interviews with software engineers, Benbouzid (2019) shows how predictive policing tools, in parallel to CompStat, are designed as a management tool rather than purely serving the purpose of crime control. Kaufmann, Egbert, and Leese (2019) highlight the assumptions around what constitutes a crime that are rendered opaque when analysts point to the ‘objective’ patterns that they reveal. While both constitute important contributions to the discourse on predictive policing, the perspective of software engineers necessarily has a blind spot towards policing practice in which ‘objective’ patterns are dismissed (just as in other contexts, see Asdal, 2011) and senior police officers may reject the software’s management appeal. Accordingly, Ratcliffe, Taylor, and Fisher (2019) accompanying officers on patrol in predicted areas find officers doubting the software’s predictive capabilities, highlighting how they believe their tacit knowledge to be superior, and the instruction to stay within a box would conflict with their perceived duty to assist in calls for service. Yet, the software also helped to break up routines and widen officers' knowledge by sending them to places they would not have visited otherwise. Brayne and Christin (2020) and Sandhu and Fussey (2020) also find that tensions with discretion based on experiential knowledge, awareness of biases and flaws in the predictions, and a perceived increase in managerial surveillance lead to resistance in adoption of predictive policing tools among police officers. Hence, rather than a techno-determinist view in which officers follow a program's instructions, this thesis describes a more complex situation in which officers and algorithm co-construct risk and senior officers are keenly aware of the misrepresentations provided by the counts in their management systems.

Finally, a wider perspective is adopted by Brayne (2017). Based on qualitative research within the Los Angeles Police Department, she describes a general transformation of policing practices towards risk scores, prediction, automatic alerts, and more exhaustive and integrated databases – all facilitated by big data analytics and materialised to different degrees. Her work highlights the importance of looking beyond a single technology and its adoption and paying attention to how the increasing digitization of police work transforms many areas of policing. This thesis follows the same approach particularly in the US case study. Brayne's (2017) work is an important description and analysis of new technologies and the ways they transform policing practice. As it describes a development towards big data policing, it edges close to a techno-deterministic account in which new technological practices replace old practices. In contrast to this argument, this thesis not only provides another case study of technology in police practice but also pays attention to the fragmented nature of technological practice – the ways things break down, the workarounds officers find, the idiosyncrasies in use – and the ways the new knowledge stemming from the datafication of policing has to be translated and brought in line with existing knowledges. Here, rather than a linear development towards big data policing, technologies add to policing, augment existing practices, and shift rather than replace existing priorities.

With few exceptions the current literature on technology in policing is limited in scope and, since it lacks empiricism, rarely addresses technologies in practice beyond evaluations of 'effectivity'. The nascent discourse on predictive policing has brought about not only a critical theoretical discussion of effects of biases encoded in data and feedback loops but also a small number of empirical studies that address questions of officer discretion in the face of 'objective' data and increased workplace surveillance. Building on this work, this thesis contributes two case studies from the UK and the US that shine a light on the ways officers make sense of data and how quantified knowledge from simple crime counts to individualized risk scores are translated into practice, how data reshapes power relations within the police and reshapes who is policed, and the affordances technologies have on everyday police practice including how technologies often do not work the way they are imagined and intended.

2.2. Actuarial justice, biopower and discipline – a new form of governmentality?

Already at the beginning of the 1990s Feeley and Simon (1992) argued that a 'new penology' was developing within the justice system. Instead of focussing on individualistic concepts such as guilt, responsibility and rehabilitation, this new discourse redirected attention to the actuarial management of social aggregates. Apart from a change in language, stressing probability and risk, the authors identified a change in objectives that were now tailored to internal system processes and the deployment of new techniques targeting groups instead of individuals. An example of new objectives is the shift from evaluating performance as achieving societal goals (e.g. rehabilitation) to measuring system functioning on internal indicators such as the average time between arrest and conviction. Feeley and Simon (1994) later renamed this trend more meaningfully as ‘actuarial justice’ and provided some examples of its institutionalisation as well as possible reasons for its implementation. Particularly relevant here, are the risk profiles that were first developed for the detection of potential plane hijackers in 1969 and whose usage was extended to drug couriers by 1974. Although they were ‘riddled with subjectivity and prejudice’, their attempt at rationalising prevention through targeting a population with certain characteristics fitted well with the actuarial approach (Feeley and Simon, 1994: 177). While the (potential) for rationality within those profiles appeals to actuarial justice’s aspect of creating formal systems of rules, criminal profiles are also a measure of prevention and risk minimisation drawing on general characteristics of a population (of drug couriers or hijackers). According to Feeley and Simon (1994: 177f), actuarial justice is constituted by three elements: 1) The target of power becomes the population itself in the form of statistical aggregates, 2) formal systems of internal rules replace individual decision making, and 3) prevention and risk minimisation, not necessarily its eradication, are aimed for. The following interrogates and challenges these three theses in the context of the practices of CompStat and predictive policing.

Do statistical aggregates become the target of power? As the authors argue,

> “This does not mean that individuals disappear in criminal justice. They remain, but increasingly they are grasped not as coherent subjects, whether understood as moral, psychological or economic agents, but as members of particular subpopulations and the intersection of various categorical indicators” (Feeley and Simon, 1994: 178).

Harcourt (2007) describes this emergence of actuarial methods as an individualization of punishment:

> "The individualization movement […] rested on a probabilistic model that attempted to predict likely success of different treatment interventions on the basis of inferences from an accumulation of data points about a particular individual" (Harcourt, 2007: 45).

Harcourt (2007: 19) and Carrabine et al. (2014) locate 'actuarial justice' in a wider body of literature that draws on a Foucauldian perspective of governmentality. Particularly the thesis of statistical aggregates as targets of power resonates with Foucault's description of biopower (interchangeably used with the words 'biopolitics' and 'security'). As the prefix 'bio' suggests biopower has life as its object. Accordingly, many of Foucault's (2010) examples revolve around public hygiene, medical care, and more generally the politics of life and death; and so do most interpretations of the concept (Lemke, 2007; Rabinow and Rose, 2006). With biopower, Foucault describes a form of governmentality that emerges in the 18th century due to the increasing self-regulation of cities and circulation of, among others, people, goods, and plagues between them (Foucault, 2009: 91ff). In contrast to disciplinary technologies, which Foucault (1977) had already explored in *Discipline and Punish*, biopower is not centred on the individual body but rather on the population (Foucault, 2003: 242). What is governed "[…] are phenomena that are aleatory and unpredictable when taken in themselves or individually, but which, at the collective level, display constants that are easy, or at least possible, to establish" (Foucault, 2003: 246). Given the statistical knowledge of these phenomena, interventions do not seek to prohibit (as in sovereignty), or to prescribe (as in discipline), but rather to manipulate the conditions of reality so that 'naturally' occurring events happen (or do not happen) in the desired manner, or, as Foucault puts it,

> "[…] the law prohibits and discipline prescribes, and the essential function of security, without prohibiting or prescribing, but possibly making use of some instruments of prescription and prohibition, is to respond to a reality in

> such a way that this response cancels out the reality to which it responds – nullifies it, or limits, checks, or regulates it.” (Foucault, 2009: 69).

One of the examples Foucault (2009) gives in *Security, Territory, Population*, is the shift from preventing food shortages by controlling prices by constraining storage, cultivation, and exports, to freedom of commerce and a system of import and export tariffs relying on the ‘reality’ of actors’ motivations and the market. While tolerating scarcity for some, it would eliminate revolt triggering food shortages at the level of the population. This same logic can be found in theories of deterrence, whether it is increased sentences aimed at ‘rational’ actors, or the hotspot presence of police patrols in predictive policing. Moreover, to connect this back to Feeley and Simon’s (1994) thesis of targeting individuals as members of subpopulations: Foucault (2009) further describes the emergence of new notions of risk, danger, and crisis within the framework of biopower. The quantitative analysis of diseases at the end of the 18th century brings about risk as the risk of dying given factors such as age, profession, and vaccination; danger as the distribution of this risk across milieus, places, age groups; and crisis as the sudden increase in cases – all of which are used to address disease primarily in those most affected by the disease, instead of separating all the sick from the healthy (Foucault, 2009: 89f). Foucault describes this as a process of ‘normalization’ in which

> “[…] we have a plotting of the normal and the abnormal, of different curves of normality, and the operation of normalization consists in establishing an interplay between these different distributions of normality and [in] acting to bring the most unfavorable in line with the more favorable” (Foucault, 2009: 91).

Thus, the use of risk scores to prioritize those likely to re-offend (see section 7.1) or the identification and targeting of rises in crime numbers in CompStat (see section 4.2) fall squarely into these knowledge practices.

To clarify, what would be the population targeted by such biopolitics? Multiple scholars have argued that predictive policing practices target disproportionately poor and black communities and equated it to a high-tech justification for racial profiling (Ferguson, 2017a, 2017b; Joh, 2016; Lum and Isaac, 2016; Raso et al., 2018; Richardson et al., 2019; Sanders et al., 2015). The software-sorted geographies (Graham, 2005) and social sorting (Lyon, 2003) inherent to predictive policing targeting areas and individuals could thus be interpreted as a functional element of the institutional mesh between 'hyperghetto' and prison as described by Wacquant (2009). While these accounts contribute an important perspective on the socially unequally distributed consequences of policing (a perspective that particularly section 5.2 on stop and search will take up), they perhaps overstate the racist intentionality behind the production and use of these technologies. The populations explicitly targeted by quantitative technologies can be racist (see e.g. McIlwain, 2019; Oosterloo and Schie, 2018), but they do not need to be for racist outcomes to occur through encoded biases and feedback loops[1]. Instead, the racially disparate outcomes of knowledge that deals with populations (in the strict statistical sense) of crime events highlights the indeterminacy of measures based on biopolitical knowledge and the importance of empirical research into their situatedness in police practice.

Foucault's project is one of describing the changes in the knowledge of governing, in the 'raison d'état', rather than the practice. As he says in *The Birth of Biopolitics*,

> "I have not studied and do not want to study the development of real governmental practice by determining the particular situations it deals with, the problems raised, the tactics chosen, the instruments employed, forged, or remodeled, and so forth. I wanted to study the art of governing, that is to say, the reasoned way of governing best and, at the same time, reflection on the

[1] Even more so, proponents of predictive policing like Brantingham et al. (2018) argue that it does not entail more bias in police actions.

> best possible way of governing. That is to say, I have tried to grasp the level of reflection in the practice of government and on the practice of government. In a sense, I wanted to study government's consciousness of itself […]" (Foucault, 2010: 2).

Consequentially and in contrast to the argument in *Discipline and Punish*, Foucault (2009) somewhat decouples the governmentalities of sovereignty, discipline, and security from the practices employed by them. For instance, he argues, torture associated with sovereignty could also be interpreted as having a disciplinary effect on those watching, and harsh bodily punishments for minor offences would possibly occur because of their probability and hence within the framework of biopower. The other way around, mechanisms of security would also rely on juridico-legal structures as well as disciplinary mechanisms (Foucault, 2009: 21f). Thus, while pointing to the logic of governmentality based on statistical populations, the concept of biopower leaves the ways this knowledge is translated into practice undetermined. At best, this opens the process of translation for empirical investigation, at worst it invites techno-deterministic arguments that assume the governing of populations to be successful or at least consequential (for this same critique of techno-determinism levelled against Feeley and Simon's (1994) argument see the discussion of the second thesis below). Accordingly, Hacking argues that some of the biopolitics Foucault describes, like tax incentives for large families, are unlikely to have had any of the desired effects (Hacking, 1982: 289). Therefore, to provide an empirical lens for the creation and use of quantitative knowledge in policing, this thesis draws on concepts from actor-network theory, specifically 'centres of calculation' (Latour, 1987), 'obligatory point of passage' (Callon, 1999), and 'centres of translation' (Callon, 1986; Law, 2003).

With 'centres of calculation', Latour (1987) describes how inscription devices are used to establish a self-perpetuating loop of fact gathering. The example used in the book is the creation of maps in Europe based on the information brought back by explorers who then could make use of these maps to gather more data more easily (Latour, 1987: 215ff). As the maps produced in this manner are of use for the navigators, the centre of calculation can become an ‘obligatory passage point’ (Callon, 1999). That is, to access maps collated centrally a navigator may be required to contribute to charting new territories. The passage point can control access, the distinction of inside and outside (see Law and Bijker, 1992: 294). Consequentially, ‘centres of calculation’ describe an asymmetrical configuration of a network affording power to the centre (Law, 2003; Porter, 1996). Law and Hetherington (2000) further qualify this asymmetry: the centre as obligatory point of passage allows for the accumulation of knowledge at a distance (or surveillance) implying manipulations of scale in reductions and simplifications as in the statistics relevant to biopower. Simultaneously, it may act at a distance (or dominate) by delegating through something that holds its shape such as drilled soldiers or paper documents – Latour’s (1987) ‘immutable mobiles’. To distinguish these two functions Law (2003) refers to the creation of representations (maps, statistics, etc.) in one place as ‘centre of calculation’ (the incoming side) and to the production of effects on the periphery as ‘centre of translation’ (the outgoing side) (see also Callon, 1986), linking knowledge accumulation and power. An example of this configuration can be found in hotspot types of policing in CompStat systems where crime reports are centrally processed to map crime densities and direct patrol officers accordingly – if they subscribe to the problematisation of this ‘obligatory point of passage’ and believe that to reduce crime means having to patrol where most crime is and to know where most crime is one must map it.

This last qualification, the need for the periphery to subscribe to the centre in the example, points to centres of calculation/translation being not only historically contingent (Law and

Bijker, 1992: 305) but also unstable and contested[2] - as demonstrated in the various breakdowns of relations described throughout the empirical part of this thesis (and the centrality of breakdown as concept further explored below). Nonetheless, ‘centres of calculation/translation’ and ‘obligatory passage points’ can serve as a heuristic device in unravelling the ways knowledge is accumulated and put into action – particularly in the case of statistical knowledge and biopower.

Through the empirical lens of the coming chapters, it is possible to distinguish at least five different ways of knowing that are enabled by centres of calculation. The first two are not strictly related to practices of calculation and are hence discussed in more detail further below.

1) Command and Control: This is the direct command and control of multiple agents enabled by the simultaneous connection of the centre to its agents. In policing, this can for example be the sergeant monitoring and assigning calls for service, as well as checking and approving reports (see chapter 5).
2) Archive: With all the information coming together in centres of calculation, they are in a good position to function as archives. The archive, as conceptualized by Waterton (2010), is in a structurally equivalent position:

> “[Archives] build upon deeply held, spatially segregated, cultural understandings of knowledge whereby certain forms of ‘raw data’ are gathered ‘in the field,’ through experience of life and of the world. Data are then condensed and curated in places ‘set apart’—the monasteries, science parks, ivory towers, the back rooms within museums, and research centres—the places where, nowadays, databases are built. The enlightenment panoptic

[2] Law (2003), for instance, views the various competing modes of ordering (enterprise, administration, vision, and vocation) he identified in *Organizing Modernity* (Law, 1994) as competing centres of calculation/translation.

> project of assembling all knowledge in one place has overwhelmingly informed the archetypal archive […]" (Waterton, 2010: 648f).

Drawing on Derrida's (1998) *Archive Fever*, she describes the archive as an 'epistemic time machine' that stores past and present experiences for (imagined) future use. Such an archive, or the police's databases, come with questions and conflicts around what should be recorded, how should it be recorded, for how long should it be accessible, who should have access, and how is it accessed? These are just some of the questions that are supporting the analysis, particularly in section 5.2 and chapter 6. While the knowledge contained in archives may be retrieved through individual records, centres of calculation also offer different means of access establishing the remaining three forms of seeing/knowledge.

3) Aggregation and Reaction: Centres of calculation allow for the aggregation of categorised information into statistics. The categories used for counting create new 'objects' that can be addressed, such as the crime rate for 'types' of crime. Thus, the categories used have consequences (see Bowker and Star, 1999). Hacking (1982: 292) therefore argues that the main change brought about by population statistics is perhaps not the effect of the political measures they provoked, but rather the creation of categories bringing about new ways of 'conceiving the person' – such as the category of 'risky' individuals. In the case of crime statistics, the numbers are regularly doubted and the underlying systems of classification are contested (Bialik, 2016; Maguire and McVie, 2017). Yet, CompStat and, within a different epistemology, predictive policing make extensive use of crime statistics to focus police activity. The underlying reasoning closely relates to theories of deterrence and incapacitation. Sections 4.2 and 4.3, and

chapter 7 explore this process and how the priorities produced through crime numbers are translated back into action.

4) Attributing Causes: Beyond the ‘reactivity theme’ of policing in which priorities are decided according to recent events and crime spikes (as in the previous epistemological arrangement), Manning (2008) hoped to find a theoretically informed analysis of why crime spikes occurred and a problem-oriented response aimed at solving the underlying issues. Although he did not find this in practice, more recently programs like ‘risk terrain modelling’ which loosely fall into the predictive policing category try to link aspects of a city’s spatial make-up, such as the presence of bars or the quality of street lighting to locations of crime (Caplan and Kennedy, 2011; Kennedy and Dugato, 2018). Similarly, problem-oriented policing aims to identify and address the causes of crime patterns (Braga, 2014; Goldstein, 1979). The attribution of causes is relevant for the translation of quantitatively derived priorities into action (see section 4.3)[3].
5) Algorithmic Discovery: This final way of knowing is arguably a more recent development and can be related to a discourse on the epistemic value of machine learning, big data, data mining and associated keywords. Examples of big data analysis are manifold: Google using search terms to predict flu trends (Mayer-Schönberger and Cukier, 2013: 1ff), Target using purchase patterns to individualize advertisements (Harford, 2014), and mass surveillance by the NSA (Lyon, 2014). Beyond the technical discussion stressing challenges of data processing (Chen et al., 2014; Hu et al., 2014; Sagiroglu and Sinanc, 2013; Ward and Barker, 2013), perspectives from outside this

[3] Causation here is used in a different sense than traditionally discussed in criminology. Instead of the broader question of the aetiology of crime (‘why is crime’) and criminology’s debate between individual and structural factors of crime (e.g. Young, 1997), the question is more focussed on the practical answers to ‘why is crime here’ or ‘why does this person commit a crime’.

discussion stress how big data is different from traditional research (and hence the logic discussed above):

> “Big Data analytics enables an entirely new epistemological approach for making sense of the world; rather than testing a theory by analyzing relevant data, new data analytics seek to gain insights 'born from the data'” (Kitchin, 2014a: 2).

Data is analysed with the goal of prediction in mind, calling on patterns and correlations instead of causality, and trading uncertainties in sampling for errors in measurement (Mayer-Schönberger and Cukier, 2013: 11ff). Big data challenges traditional social research as to who can legitimately produce knowledge, which methods are scientific and what counts as proper data (Levallois et al., 2013). On the other hand (social) science questions the mythology that comes with selling big data services:

> “[...] the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy” (boyd and Crawford, 2012: 663).

This clash in epistemologies between one where knowledge is not really necessary as long as ‘it works’ and one that wants to give reasons to experience, does also extend into policing and criminology with Berk (2013) arguing that machine learning techniques could capitalize on complex patterns in data and discover unexplained aspects to the aetiology of crime, and Chan and Bennett Moses (2016) problematizing the reliance on correlation over causation and the opacity of the analysis. Algorithmic discovery can be central to predictive policing approaches where data patterns are automatically detected and transformed into the prediction of risky areas or individuals. In the case of big data collected from mass surveillance being employed to identify potential offenders this may take decidedly different forms from traditional approaches. Traditionally officers form their suspicion during observations and contacts by a combination of stereotypes, prior contacts, incongruities with what is normal or incongruities within a story, and nonverbal clues such as body language; which factor contributes to what degree is disagreed upon though (Johnson and Morgan, 2013). As data from mass surveillance contains information about everyone, the process by which suspicion is raised is somewhat different. According to Amoore and Piotukh (2015), the process of analysis needs to generate a threshold of perception so that the results are reduced in a way that they can be displayed in one place.

> “Understood thus, the little analytics are instrumental in what is called *target discovery*, the defining of a political threshold of perceptibility where a person [or object] of interest comes into view” (Amoore and Piotukh, 2015: 354).

Within policing this has the potential to transform the way police decides who to investigate. "[...] suspects can emerge from the data for purposes of investigation. These suspicious persons and activities can appear even if police do not seek a particular person for a particular crime. Nor do they need to begin the collection of data, *if data is already being collected all of the time*" (Joh, 2016: 21). While none of the technologies discussed in this thesis are as ‘advanced’ as those that inform this debate, the risk scores discussed in chapter 7.1 have similar properties in that they are opaque to the officers, leaving them second-guessing the reasons for some of the ratings. This highlights again the non-techno-deterministic role of these technologies and the necessity to study users’ understandings of the outputs.

It is certainly possible to order these elements in a chronological fashion that reflects epistemic shifts from 'analogue' policing, to the introduction of information technology and the first CompStat meetings, to a form of 'Big Data policing' that resides somewhere between the present and the near future. Accordingly, Sarah Brayne (2017), in one of the very few detailed empirical engagements with digital technologies in policing, analyses to what degree this development has already played out in the Los Angeles Police Department. While this is a useful perspective in rendering visible how these technologies are 'new' compared to 'traditional' policing, it creates a narrative of displacement in which one supersedes the other (see also section 2.3.1 on discretion below). But in practice, these different modes of operation of centres of calculation are entangled and coexist. The centres themselves are, at times, separated and incoherent producing different scores for the same purpose or holding different information on the same individual. For example, justifications for predictive policing models and the variables they include rely on either an assumption of criminals as creatures of habit returning to the same locations and committing the same types of crime or on rational choice theory allowing to model a criminal's decision making (Perry et al., 2013: 2f). Threat scores for individuals may incorporate psychological theories about personality. Theory informs data selection, data patterns inform theory, theory explains ex-post, and theory is disregarded if patterns do not seem to make sense, and so on. Similarly, algorithms that highlight risk may transform what records are reviewed from the archive and the way the archive is constructed may influence how algorithms can operate. Palantir's (2013) mixture of information retrieval and manual annotation is an example of such an entanglement (see also Brayne, 2017: 986f). A key research question for the analysis in the following chapters is then how biopower associated with the last three modes of operation interacts in centres of calculation with other forms of knowledge, particularly the intimate knowledge of individual cases and officers' tacit knowledge of the environment that they operate in (see particularly sections 4.3 and 7.1).

Interrogating the way biopower operates also means that its operation is not taken for granted. Just as tax incentives for large families may not have had any of the desired effects (Hacking, 1982: 289), it is unlikely that officers give up their discretion in planning their shifts without any kind of resistance, that they surrender their personal knowledge of the place to the aggregated knowledge of the analysts. There are indications that this is why a predictive policing program was dropped in Burbank (*Los Angeles Times*, 2016). Finally, even if statistics successfully mobilise action, it may not always be clear what effect the action has on the statistics targeted – as demonstrated by practices aimed at influencing the recording of crime rather than the occurrence of crime and the debatable 'success' of CompStat (see e.g. Bowling, 1999; Muller, 2018; Weisburd et al., 2019).

As argued here, 'centres of calculation' provide a useful concept for analysing how biopower operates (or fails to operate) in practice. This conceptualisation is markedly different from its use by Haggerty and Ericson (2000) in their description of the 'surveillant assemblage'. Instead of describing the operation of biopower, the authors relate 'centres of calculation' to the Panopticon and disciplinary power (additionally drawing on Deleuze and Guattari, 1987). Disciplinary power operates through technologies that are used to govern the soul as opposed to the punishment of the body (Foucault, 1977). The famous metaphor for these technologies is the Panopticon. A prison designed in a way that the warden in the central watchtower can observe all the inmates in the surrounding cells, but the inmates are unable to tell whether they are being watched at any given time. This hierarchical observation then leads to an adjustment in inmate behaviour (Gutting, 2005: 82f). While this is the well-known part of disciplinary control, it extends to a normalizing judgement – enabled through said hierarchical observation – that places those who are judged on a ranked scale in comparison to others instead of directly judging someone's acts. This plays out in regular examinations leaving a paper trail that in the end allows for these comparisons to be made (Gutting, 2005: 84ff). Haggerty and Ericson (2000) claim that modern surveillance employing computers uses these (formerly paper) trails to create 'data doubles' that integrate data from various institutions already central to Foucault's account, such as health sector, police and education, and that are rendered mobile for comparison in various 'centres of calculation'. While the authors do not argue for a new prefix for the Panopticon[4], they do argue that these 'surveillant assemblages' entail control:

> "Data doubles circulate in a host of different centres of calculation and serve as markers for access to resources, services and power in ways which are often unknown to its referent" (Haggerty and Ericson, 2000: 613).

Interestingly, this contains precisely the point that Norris and Armstrong (1999) make regarding the inapplicability of the Panopticon to modern surveillance systems. They argue that CCTV is unlikely to entail anticipatory conformity because people can evade the gaze, are often unaware of being monitored, and wrong-doing is not necessarily followed by any kind of response (Norris and Armstrong, 1999: 91ff). Furthermore, as Fussey (2002) argues in the same context, Haggerty and Ericson's (2000) account ignores the often fragmented nature of surveillance systems and overly stresses their convergence. Fussey (2013), building on Foucault's *Security, Territory, Population* lectures, further stresses that 'security' is always partial as it is predicated on allowing circulation so it can be monitored and that the mechanisms to do so are heterogeneous, fragile, and contested. The calculative practices described within the 'surveillant assemblage' are thus perhaps better understood within the framework of biopower as outlined above. Disciplinary power, on the other hand, can serve as a way to understand the second way in which numbers have effects by turning the gaze away from those who are the supposed

[4] Haggerty (2006) problematizes the widespread use of the Panopticon as metaphor with ever-changing prefixes that indicate that something different is meant.

targets of surveillance to the control of the surveillers and hence the managerialism Feeley and Simon (1992: 452) associate with actuarial justice.

The disciplinary orientation of hierarchical monitoring, ranked judgement, and consequentially subjectification in the form of anticipatory conformity, is central to many of the accounts of data-driven managerialism where numbers increasingly become internalised indicators of success (e.g. Beer, 2016; Espeland and Sauder, 2007; Muller, 2018; Power, 1997). Deleuze's (1992) 'societies of control' can serve as an illustration here. He makes a distinction between moulds and modulation that describes the difference between disciplinary societies and 'societies of control'. While prison, family, school, factory, and so on, as institutions of the disciplinary society, were rather separate entities that functioned as different moulds and provided an order of time and space, the modulations of societies of control designate an ever-changing process of striving to attain something, be it the next bonus on the income sheet or yet another certificate of education – or a better indicator value such as lower crime counts. Note that this conceptualization does not necessarily contrast formal systems of decision making with individual decision making but rather entangles the two (see also section 2.3.1 below). Furthermore, while these techniques are built on the idea of normalization and hence statistical knowledge of biopower – those that fall below the average receive closer supervision, those that are above average are rewarded (see also sections 4.4 and 8.2.1) –, the mechanism is closer to discipline and the 'surveillant assemblage'.

At first glance, the second thesis of 'actuarial justice' – formal rules replacing individual decision making – seems to be easily met by CompStat and predictive policing. CompStat provides a formalised process of allocating patrol resources that takes such decisions out of officers' hands. Similarly, Benbouzid (2019) argues that more than a technology of crime control, area-based predictive policing software is a management tool that allows for the "rational" allocation of patrol and its monitoring. For individual risk scores, Feeley and Simon's (1994) observation is exactly the fear frequently voiced by critics: biased risk scores replacing professional judgement, the offenders' grouping becoming more important than the individual circumstances (e.g. Ferguson, 2017a; Joh, 2016; Schlehahn et al., 2015) – a fear that also matches the first element of a turn towards aggregates (see above). However, there are clear limitations to such an account. Technical systems seldom merely replace individual judgement but rather transform it, shape it, create resistances, and often have unintended effects (see section 2.3.1 below). The 'actuarial justice' thesis – as well as many other accounts of disciplinary power operating through metrics – just assumes the uninterrupted control by formal systems, as Leonidas Cheliotis argues, it includes an "[…] unstated presupposition that misleads the new penology thesis into a dystopian cul-de-sac, that is, the perception of penal agents as executive automata or docile bodies entrapped in the 'iron cage' of an over-rationalized criminal justice system" (Cheliotis, 2006: 314). Accordingly, Brayne and Christin (2020) show that the influence of risk scores on decision making varies with the institutional role of the decision-maker. Legal professionals would, for instance, be more likely to overrule scores than law enforcement personnel. This highlights the need to empirically study the power relations that technical solutions are embedded in, as well as the way in which they shape these relations.

Willis and Mastrofski (2012) argue concerning CompStat that the program was not adopted in a drive towards a technical-rational process but rather as a means of appearing progressive while having little influence on police's actual performance. From their perspective, a neo-institutional approach as developed by Meyer and Rowan (1977) and Scott (1995) is more likely to explain the adoption of CompStat as a presentable "solution" to external pressures. Manning (2008) makes the same argument claiming that the crime analysis in CompStat does not bring any fundamental changes to the reactive nature of policing. Accordingly, he argues

Ericson and Haggerty’s (1997) assertion that police focus on managing risk and enhancing security would be premature and flawed given the many empirical resistances to such programs (Manning, 2008: 262). Both, Manning (2008) and Willis and Mastroski (2012) underline that systems designed to control may not have the intended effects as they would be assumed by the ‘actuarial justice’ thesis. However, this research also points to a common shortcoming of research into technological changes in policing: the authors focus on the presumed effects of the technology and thereby become impervious to other changes. Manning (2008), for example, comes to his conclusion without examining any of the practices that follow from the CompStat meetings that he observes. This is despite speculating that the CompStat process may be contributing to a shared knowledge of best practice and the creation of new information infrastructure (Manning, 2008: 248ff). Not seeing a change in the reactivity theme of policing, he is not asking if that which is reacted to has changed. In UK policing the House of Commons Public Administration Select Committee found in 2014 that the ‘target culture’ of policing (brought about by a series of reforms informed by the New Public Management ideology (de Maillard and Savage, 2012; Guilfoyle, 2012)) had generated perverse incentives to mis-record crime and diagnosed a flawed leadership model in conflict with the policing code of ethics (Public Administration Select Committee, 2014). Already in 2000, Maguire (2000) warned that since the Thatcher government, the pressure to demonstrate ‘value for money’ and the Audit Commission’s stress on targeting criminals was leading to “[…] a *strategic, future-oriented and targeted* approach to crime control, focussing upon the *identification, analysis and ‘management’ of persisting and developing ‘problems’ or ‘risks’* (which may be particular people, activities or areas), rather than on the reactive investigation and detection of individual crimes” (Maguire, 2000: 316) – raising questions of privacy, proportionality, police ethics and priorities (Maguire, 2000). Contrary to the supposed cosmetic changes in US policing, this suggests that the formal systems described by Feeley and Simon (1994) can have profound effects on policing. The question that arises is to what extent this plays out in an increasingly quantified environment brought about by digital technologies. What is needed then is an empirical analysis of the human-technical relations that make up the managerialism described by Feeley and Simon (1992, 1994) going beyond the binary division of professional judgment and rational systems. The 'actuarial justice' thesis, together with the idea that metrics provide modulations of control, can inform a sensitivity towards potential shifts in internal power dynamics – although perhaps in unintended ways.

Finally, because the allocation of resources through CompStat and predictive policing is, at least according to its proponents, intrinsically geared towards preventing crime from happening (by whatever policing strategy that is chosen), it seems natural to assume that its application is in line with the last element of actuarial justice: prevention and risk minimisation. Depending on the policing strategy chosen, one could also argue that it does not address causes of crime; that it does not aim to eradicate crime but only tries to minimize its occurrence. In this sense, predictive policing and CompStat are completely congruent with the risk management approaches described within the context of actuarial justice and new penology. However, one might question the extent to which this is a new orientation. Lawrence (2017) provides a historical analysis tracing pre-emptive policing and arrests based on character and intent back to 1750 and the beginnings of policing in the United Kingdom. Directly challenging accounts by Zedner (2007), Ashworth and Zedner (2014), and McCulloch and Wilson (2015), this criticism of diagnosing a new turn towards pre-emption also applies to Feeley and Simon's (1992, 1994) diagnosis, as well as to many other works that fall into the same line of argument (e.g. Mantello, 2016; van Brakel and De Hert, 2011). Not only is pre-emption not a new phenomenon, but outside of quantified risk assessments, anti-social behaviour orders (ASBOs) introduced by New Labour in England, Scotland and Wales with the Crime and Disorder Act 1998, now replaced with the less discussed criminal behaviour orders (CBOs) (Brown, 2020), have caused wide debate in (British) criminology (Ashworth and Zedner, 2008; Burney, 2008; Crawford, 2009; Di Ronco and Peršak, 2014; Donoghue, 2008, 2012; Millie, 2008; Simester and Hirsch, 2006; Squires, 2006, 2008). ASBOs and CBOs are civil court orders aimed at preventing future 'antisocial' behaviour under threat of criminal punishment. They can impose duties and restrictions on individuals that range from prohibiting begging in a specified area, being drunk in public space, congregating with a group of a specified size, carrying a knife, or wearing clothing with an attached hood (Home Office, 2017). This legislation has clearly a pre-emptive angle, as Donoghue puts it, "[…] antisocial behaviour policy is quintessentially 'risk' assessment. And these assessments can be contextualized as attempts to render future happenings as controllable" (Donoghue, 2008: 346). Consequentially, and in parallel to the argument above, rather than just locating predictive policing and CompStat within a "new" trend for pre-emption, the thesis will pay attention towards how technology participates in shaping (existing) prioritisations aimed at prevention (see e.g. section 7.1.2 on the use of CBOs in the context of risk ratings). The question underlying this analysis is how the situated knowledge of police officers and their appraisals of a person's 'criminality' – the form of pre-crime highlighted by Lawrence (2017) – interacts with the quantitative risk scores that are the basis to the more recent diagnoses of a turn towards pre-crime.

All in all, this discussion of 'actuarial justice', 'biopower', and 'centres of calculation' opens a set of four interrelated questions: 1) how is quantitative knowledge created in police organisations? 2) How is this knowledge (associated with 'biopower') translated into practice and what is its relationship with officers' tacit knowledge? 3) What is the role of quantitative knowledge in (managerial) oversight? And 4) what consequences do different ways of connecting the past to the future (archive, memory, risk scores) have in practice?

2.3. Technology and practice

While the previous section dealt with more abstract concepts that help to describe the organisation of knowledges and power in policing, this section outlines three theoretical frames that support the analysis of the socio-technical practice of policing: the role of technology in discretionary decision making, the consequences of technologies for the spatio-temporality of policing, and the often ignored issue of breakdowns and fragmented use of technologies.

2.3.1. Discretion

The decision to intervene for example in the form of a stop, the degree of intervention as in the decision to search, the choice of consequences between none, warning, fine, and arrest, the recording of an interaction – discretion is a key element of police work. A common concern in the literature on technology in policing in general, and predictive policing in particular, is the question of its effect on police officers' discretion. This is reflected both in arguments of those championing technologies as eradicating human biases from the criminal justice system, and those that fear a mechanical application of machine decisions imbued with biases hidden in the opacity of a black-box algorithm. This tension mirrors a long-standing debate in legal scholarship as well as in policing research on the role of laws, regulations, and policies in shaping or curtailing police discretion. This section first sketches out this debate, then gives an overview of empirical research on discretion particularly within the context of suspicion formation in stop and search practices, and finally, argues that the question of discretion is necessarily an empirical one. As such discretionary decision making is the core of the analysis particularly in sections 5.2 and 7.1.

The most prominent text on discretion in the legal debate is probably Davis' (1969) *Discretionary Justice*. The author voices a since often repeated concern that bureaucratic discretion could lead to arbitrariness, inconsistencies, and injustices:

> "I think the greatest and most frequent injustice occurs at the discretion end of the scale, where rules and principles provide little or no guidance, where emotions of deciding officers may affect what they do, where political or other favoritism may influence decisions, and where the imperfections of human nature are often reflected in the choices made" (Davis, 1969: 1).

He argues that discretionary powers should be curtailed to find a better balance with legal rules by issuing publicly accessible guidance and policies that limit and structure discretion, as well as instating oversight mechanisms to enforce these. Pepinsky (1984), however, argues that such a curtailing of discretion solely represents a move by society's ruling class to force police to enact laws controlling the underclass. Contrastingly, he highlights the value of police discretion in attenuating the force of the law with respect to the needs of the (poor) communities they serve.

Two observations stand out from this exchange: the debate centres on 1) who is the legitimate final arbiter? Is it the police officer or is it the lawmakers? As Pepinsky's (1984) argument demonstrates, curtailing police officer discretion solely means moving it elsewhere, whether that is lawmakers, or, as in the case of arguments around the influence of algorithms, the technologies that are assumed to control discretion. However, these movements may play out mostly in theory while any limitations on discretion may have several unforeseen consequences in practice, as argued further below. The second central question is, 2) what makes a fair decision? Is it the equal application of laws to everyone as in the example of automated traffic enforcement (Joh, 2007), or is fairness dependent on taking the circumstances of the individual into account and affording compassion (see section 5.2 for officers arguing the latter)? As Joh

(2007) concedes, the social expectation for law enforcement is regularly one that focusses on the spirit rather than the letter of the law:

> “[…] perhaps a legitimate objection would arise […] from [the people’s] view that there is a meaningful distinction between technical legal violations and abiding by the purpose for which the laws exist. Traffic laws exist to make illegal unsafe driving, a standard that is perhaps best judged by a person rather than by a machine” (Joh, 2007: 231).

Beyond the discourse around the advantages and disadvantages of police discretion, there is both a theoretical argument as well as empirical research that questions the tendentially binary conception of discretion versus no discretion. In the theoretical argument, drawing on Dworkin’s (1977) *Taking Rights Seriously*, discretion is a concept that always stands in relation to something, as he describes:

> “Discretion, like the hole in a doughnut, does not exist except as an area left open by a surrounding belt of restriction. It is therefore a relative concept. It always makes sense to ask, ‘Discretion under which standards?’ or ‘Discretion as to which authority?’” (Dworkin, 1977: 31).

Accordingly, Evans and Harris (2004) argue (with regards to the discretion of social workers) that those fearing a loss of discretion conceptualize discretion solely in what Dworkin (1977) refers to as the ‘strong sense of discretion’: not being bound by the standards of an authority. Stricter oversight mechanisms and technologies are seen as restricting decisions. However, as the authors stress, these arguments ignore the far greater role of discretion in the ‘weak sense’: interpreting the rules as officers see fit. As such, more rules could paradoxically result in more discretion.

Based on empirical work, Lipsky (2010) coined the term ‘street-level bureaucrats’ in 1969 to describe the structurally equivalent position of workers in different areas of public service faced with a gap between ideals and overwhelming workloads that causes them to employ their discretion to find coping mechanisms tolerated by the system:

> "At best, street-level bureaucrats invent modes of mass processing that more or less permit them to deal with the public fairly, appropriately, and thoughtfully. At worst, they give in to favoritism, stereotyping, convenience, and routinizing-all of which serve their own or agency purposes" (Lipsky, 2010: xiv).

Lipsky (2010) tendentially takes the same position as Davis (1969) in highlighting the dangers of discretion. He even describes CompStat as a successful restructuring of police officers' actions through incentives and sanctions based on strategically chosen indicators (Lipsky, 2010: 227). While such a perspective hardly takes into account the various unintended consequences of technologically enabled systems like CompStat (as discussed further below), his account does highlight empirically that discretion is employed as interpretation of and in relation to the rules rather than denoting a vacuum within which officers decide freely. Crucially, this refocuses question 1) from above ('who should be the final arbiter?') onto the empirical factors that steer the extent of discretion and the conditions of its use. Without knowing when and how officers exercise discretion, attempts to transform and 'improve' it are futile.

So, what are the conditions? Highlighting the gap between aspirations and overwhelming workloads, Lipsky's (2010) analysis is built on the human and organisational conditions of the work of street-level bureaucrats. As Dymond (2019) observes, much of the literature on police discretion also focusses on these human factors. An example of this is the literature on one of the most prominent areas for police discretion: stop and search. Johnson & Morgan's (2013) literature review summarises the factors influencing this decision as officers' stereotypes, known persons and locations, incongruency of observations, and non-verbal cues[5]. Quinton (2011) finds for police in England and Wales that officers rely overwhelmingly on stereotypes and routinely conduct unlawful stops – underscoring the need for empirical research that goes beyond assumed relations between law and discretion. What is missing from this literature is an appreciation of the role of technologies in officers' decision making. Dymond (2019) calls for more attention to the agency of nonhumans and the socio-technical networks in which decision-makers are embedded. In her research these are the unintended consequences of Tasers for use of force situations; in the analysis presented here, these are going to be the consequences of technologies rendering information from simple records of previous police encounters (section 5.2) to automated risk scores (section 7.1) available to officers.

The conceptual frameworks used within science and technology studies offer a sensitivity to the role of technology in police practice addressing the gap in policing research that has so far focused on the constraints of formal procedure, culture, and regulation. This approach stresses the active role technologies play as part of social assemblies. Technologies, as Hutchby (2016) argues, can be conceptualised to possess *affordances* that shape their use in a non-deterministic way. Artefacts do not determine their use through some inherent properties, nor do their uses depend solely on the users' interpretation of the object. To take a simple example from the fieldwork presented here, a police radio is designed to enable communication over distance. Hutchby (2016) argues with reference to Norman (1990), that designers impart properties on things that make certain interpretations of their uses more likely – the officer knows that the

[5] These factors are similar to the categories of suspicion Norris and Armstrong (Norris and Armstrong, 1999) found for CCTV operators: "categorical: suspicion based merely on personal characteristic such as dress, race, membership of subculture group[;] transmitted: surveillance initiated by someone else e.g. police, store detective or member of the public[;] behavioural: suspicion based on behaviour, i.e. fighting, public display of drunkenness[;] locational: suspicion based on a person's location, e.g. walking through a car park with a high rate of theft late at night[;] personalised: suspicion based on personal knowledge of the person surveilled[;] protectional: suspicion based on fear for persons [sic!] safety, e.g. woman late at night at a cash machine[;] voyeuristic: monitoring based on prurient interest" (Norris and Armstrong, 1999: 112).

buttons on the radio are meant to be pressed. However, because it is heavy and bulky, one of the interviewed platoon officers adds to this its potential use as a weapon. Hence, the radio's affordances also stand in relation to the user's interpretations. But it would be unlikely for the officer to try and prepare her dinner with the radio – the set of affordances an object can have, that is the ways in which it can be interpreted, are limited[6]. The goal of this research is to interrogate these affordances of technologies in police decision making.

One productive way to think of power from this perspective is argued by Law (1991) in his essay *Power, Discretion, and Strategy*: he differentiates a productive and enabling 'power to' from a controlling and limiting 'power over'. Both can be present at the same time and can be stored in objects. For example, money simultaneously allows one to obtain something and accordingly make someone else do something (possibly encountering resistance). At the same time, having money means having a store of power (Law, 1991: 178f). Similarly, Winner's (1980) famous example of Long Island Bridge – designed by Robert Moses to be inaccessible

[6] Hutchby (2016) tries to make an argument for a middle ground between realism (inherent properties) and constructivism (user's interpretation). The limits of interpretation that things pose constitutes the main point of departure of his argument from the constructivist reference point that he finds in Grint & Woolgar's (1997) *The Machine at Work*. Yet, the problem with Grint & Woolgar's (1997) perspective is arguably a different one. After all, the limits of interpretation are as much a construction as the interpretations themselves which could be accounted for within their constructivism. Therefore, the actual underlying problem is epistemological and methodological: Whose interpretations can be studied? The social constructivist perspective outlined by the authors draws back into second order accounts – interpretations of interpretations. This leaves no room for new interpretations of what things do that are not already existent. In fact, Grint & Woolgar's (1997) criticism towards ANT is exactly this, the creation of new interpretations of things which they condemn as a form of essentialism (Grint and Woolgar, 1997: 28ff). This position seems to unnecessarily limit research to the analysis of explicated interpretations and excludes the articulation of original observations. Perhaps a more useful understanding of social constructivism is given by Latour (2005) who himself tries to solve the issue of a false dichotomy based on a misunderstanding of 'realists' interpreting 'constructivists' as arguing that things do not exist since they are (socially) constructed. "When we say that a fact is constructed, we simply mean that we account for the solid objective reality by mobilizing various entities whose assemblage could fail; 'social constructivism' means, on the other hand, that we replace what this reality is made of with some other stuff, the social in which it is 'really' built. An account about the heterogeneous genesis of a building is substituted by another one dealing with the homogeneous social matter in which it is built. To bring constructivism back to its feet, it's enough to see that once social means again association, the whole idea of a building made of social stuff vanishes. For any construction to take place, non-human entities have to play the major role and this is just what we wanted to say from the beginning with this rather innocuous word." (Latour, 2005: 91f). From this perspective, Hutchby's (2016) description of affordances lays squarely within a social constructivist approach.

for public transport thereby making Jones Beach inaccessible to minorities and low-income people relying on such transport – first had the intended effect but later, with the decline of car prices, as Law (1991: 175f) argues, transformed into a source of 'power to' access Jones Beach. The affordances of an object can change over time when the socio-technical relations they are embedded in change. It also means that the power effects designed into an object are never certain; the relation is non-deterministic[7]. Furthermore, the idea that power is stored in objects allows for the description of unequal power distributions and, crucially, actors' capability for discretion (Law, 1991: 169f). This discretion is not to be interpreted as being unbound by rules, as in some of the conceptualisations discussed above, but rather as the calculation of a multitude of relations:

> "[…] it is, I suggest, sensible to avoid making an overall decision about whether a given agent is, or is not, a power. This is because most agents are typically treated and experienced as powers from some points of view, whereas they look like authorities from others. Accordingly, the distinction (or continuum) is best treated as a relational matter. Again, and more importantly, there is the issue of calculation. Should a habit etched into the mind (or the body?) be treated as a calculation? Is there not, in fact, a large territory between explicit calculation on receipt of signs on the one hand, and 'automatic' response to the input of signs on the other, a territory that may pertain to both of these" (Law, 1991: 171f)?

From this perspective, the police officer's discretion is the effect of the socio-technical network that constitutes it: in the example of a traffic stop, this is the law that sets conditions for legitimate stops, the stereotypes and ways of looking for incongruencies that are trained, acquired

[7] Law highlights this: "[…] though the organisation of physical materials may be directed by (frequently conflicting) strategic concerns (in the narrower, intentional sense of the term), the effects of these arrangements may turn out to be other than what was expected" (Law, 1991: 174f). This addresses criticisms like the one by Woolgar & Cooper (1999) that target the primacy of intentionality in Winner's (1980) account (not to mention the possible factual inaccuracies).

or from experiences outside the job, and it is also a long list of technical devices that enable the situation: from the uniform signalling authority, to the siren used to stop the car, to the sergeant's reminder to stop cars in a certain area because of a spike in the crime statistics, to the database revealing an outstanding warrant – and many more factors. Not only renders this perspective the multitude of non-human influences visible (without neglecting the role of human actors), it also overcomes the structure/agency dualism inherent to arguments for or against discretion. As Law (1991) puts it, "agents are both sets of relations, and nodes in sets of relations" (Law, 1991: 173). Instead, the question becomes an empirical one of carefully identifying the agents that make up an officer's discretion – intended and unintended power effects, human and non-human agents. It becomes an effort of filling Dworkin's (1977) doughnut of discretion and this research aims to particularly add the influences of technologies on officer discretion.

If discretion is the outcome of a set of relations that form the officer, then where does this leave the two starting questions of who should exercise discretion (law vs police officer) and how it should be exercised (equally vs contextualised)? The binary distinction in the first question becomes a question of whether the influence different actants have in the officer's discretionary calculation is in a 'good' balance, that is it produces largely hoped-for outcomes. By paying closer attention to what makes up a discretionary decision, this research problematises discretion and thereby opens it to scrutiny – without necessarily prescribing what a 'good' balance would be[8]. Similarly, the second question of applying the same rule to everyone vs. attenuating it to circumstance is already implied in the first: the law is associated with the equal, unbiased

[8] This thesis thus adopts a social constructivist perspective that for its critique turns power from explanandum into explanans. Refuting criticisms of social constructivism being uncritical (Winner, 1993), the aim is to extract the contingencies of the present – to turn 'matters of fact' into 'matters of concern' or, in Foucauldian terms, to problematise (Latour, 2004, 2005, 2008; Rabinow and Rose, 2003).

application of morality, and the police officer is associated with deciding based on situated knowledge. Again, the question is one of balance and power dynamics – from systems intended to check officer actions discussed in sections 4.4 and 8.2.1, to officers' ethical dilemmas in decision making (see section 5.2). The increasing prevalence of algorithms in decision making has brought about a vigorous debate on questions of responsibility, accountability, transparency, and ethics of such arrangements (for an overview see Mittelstadt et al., 2016) – all of which revolve around the distribution of agency between humans and non-humans. When discretion is distributed as suggested here, an accusation could be that such an approach dilutes responsibility. However, the argument seeks to separate the (empirical) question of the factors of discretion from the (moral) question of responsibility. Indeed, a human actor like the software developer may be ascribed responsibility for an unforeseen consequence of the software, or a police officer may be ascribed responsibility for enacting an automated instruction[9]. Problematising discretion, however, may provide clues to reconfiguring the network for a 'better' outcome[10].

While there has been considerable research into the human factors that affect officer discretion (as described above), there has been little research on discretion in the context of technologies. Some of the exceptions are Brayne and Christin (2020) who find strategies of resistance among law enforcement and legal professionals fearing devaluation of their experience and managerial surveillance, and Sandhu and Fussey (2020) reporting officers' intention to maintain their intuitions in the face of mostly area based predictive policing systems perceived of as patronising

[9] This could be taken even one step further, as also the question of how responsibility is ascribed is an empirical one. And thus, wherever there is a chain of command, even disregarding non-human actors, there are systems in place that seek to assign responsibility. Thus, the question is what makes a 'good' system of accountability.

[10] In this sense, Rubel et al.'s (2019) insistence on human responsibility – describing all else as 'agency laundering' – can be reinterpreted as urging to find an address for such a reconfiguration of the network.

and imbued with problematic biases. While these studies tendentially concern the replacement of subjective decision making with ‘objective’ predictive policing tools and thus construct a binary opposition between the two, the data presented in section 7.1.1 adds to this research by instead suggesting a co-construction of risk between software and officers’ experiential knowledge. Furthermore, section 5.2 draws attention to the role digital technologies play in discretion for comparatively low-tech solutions like access to the police database on on-board computers in police cruisers.

2.3.2. Spatio-temporal conditions of practice and knowing

Particularly discussions of predictive policing provoke a closer examination of the spatio-temporal patterns of policing. Prediction comes with a clear orientation towards potential futures and area-based predictive policing, just as CompStat, aims at identifying spaces for intervention. Beyond these examples, the introduction of new technologies is often associated with hopes for increases in efficiency and time savings (Koper and Lum, 2019). Furthermore, police technologies, as exemplified in the possibility for feedback loops in predictive policing (Ensign et al., 2018; Lum and Isaac, 2016), encode the spatiality of policing or create their own spatialities, as in the case of sensor networks like CCTV (Graham, 2005).

In *Security, Territory, Population*, Foucault (2009) argues, as described above (section 2.2), that the new knowledges of biopower emerge in the context of the problem of circulation. Power shifts from controlling everything within the walls of the territory to controlling the flows through the territory,

> “[…] it was a matter of organizing circulation, eliminating its dangerous elements, making a division between good and bad circulation, and maximizing the good circulation by diminishing the bad” (Foucault, 2009: 34).

Elden (2007) highlights the spatial categories that not only underpin the statistical devices that create populations (cartography and statistics develop together (Elden, 2007: 575)) but are also central to the way that circulation is controlled. At the time of the Holy Roman Empire,

> “This no man's land is beginning to be perceived as an open space traversed by men and things. Squares, markets, roads, bridges, rivers: these are the critical points in the territory which police will mark out and control” (Pasquino as cited in Elden, 2007: 578).

The knowledge practices in CompStat and predictive policing seem then an almost obvious instance of minimizing ‘bad’ circulation based on geo-statistics (aimed at) determining the territoriality of police presence. Indeed, much of the field of environmental criminology seems to be concerned with the spatial segmentation of populations (e.g. see Eck and Weisburd, 2015; Weisburd, 2016). Perhaps an even clearer link, that includes spatial statistics as well as the spatiality of control points discussed by Pasquino (1991) above, are the license plate readers discussed in section 6.5, in which case their positioning was decided upon based on ‘hot spots’ of shootings. Where the categorisation of spaces and the monitoring of movements through spaces is automated, these can be thought of as ‘software-sorted geographies’ (Graham, 2005) much in the same way as the ‘social sorting’ (Lyon, 2003) of populations. In this thesis, spatiality serves as a perspective from which two different ways of translating the calculative knowledge of space into practice can be interrogated empirically: First, how does it relate to and interact with the tacit knowledge of officers, and, hence, how is it translated into practice (see particularly sections 4.3 and 7.1.2)? Second, where this knowledge is translated into infrastructure like the license plate readers, how does this material spatiality influence policing (see chapter 6)? These are crucial questions that will be interrogated empirically through rare and sustained access to the policing environments in which these technologies are deployed. Moreover, whether it is the spatiality of recordings from networks of sensors or the patterns of police presence, the spatiality of policing becomes encoded within databases for future use simultaneously shaping the conditions of what is knowable in the future. The archive, as referenced earlier, takes on the spatial qualities of the network that feeds it.

As discussed above, the archive in the form of databases and paper records functions as an ‘epistemic time machine’ (Waterton, 2010) and is essential to the circulation of knowledge in centres of calculation. As such, it is the precondition to all the aggregations that enable the control of populations. The archive is essential to constructing the futures that are to be policed – at least within the technological arrangement of predictive policing. As Lawrence’s argument (2017) on pre-emption suggests, police officers will always have had ideas about who to target and which areas to target based on situated knowledge. Thus, as discussed in the context of discretion, the question becomes how these imagined futures relate to each other in practice.

When it comes to policing practice, another dimension of time becomes relevant for the analysis in the coming chapters. As Koper and Lum (2019) note in their overview of research into policing technologies, technology is often adopted under the assumption that it will increase effectiveness and efficiency. Even more so, efficiency is the main ‘frame’ by which officers of all ranks perceive the value of adopting new technologies (Lum et al., 2017). The ‘more with less’ argument for predictive policing – Beck and McCue’s (2009) article in *The Police Chief* is one of the earliest instances of this – illustrates this tendency well. However, the question of whether introduced technologies afford any time savings is perhaps formulated too narrowly. Based on the intuition that technologies rarely work as planned and rather transform when they are put into action (see e.g. Latour, 1990), the wider question of how they reshape the temporalities of policing comes into focus. This can become particularly important when technologies break down and thereby cause interruption.

Further insight for this study can come from Kavanagh and Araujo's (1995) concept of 'chronigami' which, drawing on actor-network theory, explicitly includes non-human actants[11]. What the authors describe as a relation between artefacts (but also routines, habits, customs, etc.), inscribed with programs of action by planners, and users, who may or may not subscribe to these temporalities, can be interpreted as a temporal form of affordance. For example, the surveillance cameras discussed in section 6.4 regularly overwrite the saved footage creating a pace to which detectives must adhere if they want to utilise them. Furthermore, processes (temporal zones in a network of multiple times) compete in 'trials of strength' to conscribe actants (Kavanagh and Araujo, 1995: 109f). The computer-aided dispatch, for instance, aims to enrol a police officer engaged in another activity in an emergency call by alerting them with a sound cue to a new call. The idea of 'trials of strength' also applies to the competing versions of the future described above.

2.3.3. Breakdown and workaround

Finally, a short note on breakdowns: Not only does a lot of the literature on technologies in policing (particularly critical, techno-deterministic narratives that stress the danger of total control) assume that technologies just function as imagined without any resistances and transformations in practice, it also frequently assumes that the technology works as advertised. Yet particularly police departments are regularly filled with legacy information systems that must be maintained and brought into alignment with newer solutions. While failures and resistance to the adoption of technologies in policing have received some attention in the literature (see

[11] Few approaches in social theory take non-humans into account (Nowotny, 1992). Perhaps the most amenable definition of time for this project can be found in Norbert Elias' relational approach: "For him the word time is a symbol for a relationship which a group of beings endowed with the capacity for memory and synthesis establishes between two or more continua of changes, one of which is used by them as a frame of reference or standard of measurement for the other" (Nowotny, 1992: 427).

e.g. Fussey, 2002, 2013; Koper et al., 2014; Manning, 1992; Sandhu and Fussey, 2020), and, perhaps most prominently, Manning (2008) has pointed to the fragmentation of police information systems (Manning, 2008: 74ff), there is little research on the practice and consequences of dealing with the continuous breakdown and need for maintenance of technologies. What follows is a short discussion of the notions of maintenance and repair in science and technology studies that provide a framework for analysing this aspect of technology in policing.

As Denis and Pontille (2019) describe, actor-network theory used to focus on successful technologies but neglected the amount of necessary maintenance work. Only more recently, scholars have focussed on the practices of maintenance and repair and this newly emerging area questions and repositions some of actor-network theory's underlying assumptions: it challenges the binary distinction between mundane functioning and breakdown as well as highlighting the fragility, decay and vulnerability of materiality in contrast to its supposed durability[12]. Breakdowns, together with accidents and controversies, have been discussed in actor-network theory as moments in which the mundanity and taken-for-grantedness of technologies collapses; instructive in revealing its inner workings and problematising them anew. Repair and maintenance studies qualify this further:

> "Even at rest, artefacts are not as sealed and stable as they may appear […]. The ability for technologies to remain the same and to be taken for granted by most of their users requires a constant work that such terms as 'black box' and 'immutable mobiles' seriously understate" (Denis and Pontille, 2019: 286).

[12] However, while durability is a prominent argument in ANT, already Law (1992) cautions, "[…] durability is yet another relational effect, not something given in the nature of things. […] the argument about durability is attractive and has much merit – but it needs to be handled with caution" (Law, 1992: 387).

The authors note that some forms of malfunctioning visible to those who maintain the technology are never even experienced as such by its users. An example of this is the data work performed by the analysts linking different databases in the background (see section 4.1). To add to this idea, the research presented here shows how not only for some the technology is just working while others work constantly to hide its fragility, different users will also put up with different levels of hiccups and inconvenience. Consequentially, various forms of workarounds develop where users enrol alternative technologies for their goals leading to a fragmentation of technological practices. Graham and Thrift (2007) point to this idiosyncrasy of repair, and the role of breakdowns for adaptation and improvisation[13]. Technology's adoption, or the less human-centred version of 'interessement' (Callon, 1999), is rarely homogeneous, especially in the absence of training. A fragmented version of the binary between crisis and for-grantedness develops in which technologies are problematised and reshaped by some and not others.

Lastly, breakdowns, as well as attention to maintenance work, are methodologically useful in the way they have always been to actor-network theory: they render the roles technologies play visible. As Star and Ruhleder (1996) point out,

> "The normally invisible quality of working infrastructure becomes visible when it breaks; the server is down, the bridge washes out, there is a power blackout. Even when there are back-up mechanisms or procedures, their existence further highlights the now-visible infrastructure" (Star and Ruhleder, 1996: 113).

[13] Beyond this, Graham and Thrift (2007) and Jackson (2014) highlight the importance of breakdown and repair for the process of innovation, whether that is through the knowledge gained from how things break and overcoming the issues problematised in breakdowns, or the knowledge gained from developing processes for recycling broken artefacts. "[…] repair occupies and constitutes an aftermath, growing at the margins, breakpoints, and interstices of complex sociotechnical systems as they creak, flex, and bend their way through time. It fills in the moment of hope and fear in which bridges from old worlds to new worlds are built, and the continuity of order, value, and meaning gets woven, one tenuous thread at a time. And it does all this quietly, humbly, and all the time" (Jackson, 2014: 223).

2.4.Conclusion

To conclude, the use of technologies in policing has recently elicited a growing debate on its uses and misuses – a debate that, as Brayne (2017) highlights, remains largely speculative. Important issues like officer discretion, which have received wide attention in past research, are poorly understood empirically within the context of technologies in policing. Using Foucault's (2003, 2009, 2010) lectures on 'biopolitics', Latour's (1987) 'centre of calculation', Law's (1991) perspective on discretion, and the concept of 'affordances' (Hutchby, 2016) this literature review provides a theoretical framework to challenge existing, techno-deterministic accounts and to address empirically the question of how technologically mediated knowledge production shapes police practice and informs routine decision-making from strategy, to patrol and investigation, to oversight.

3. Method

This thesis adopts a social constructivist perspective in a) tracing how police create, process, interpret, and negotiate calculative knowledge and how it is reconciled with officer’s experiential knowledge, and b) studying the affordances of technologies in police practice. For this purpose, I use primarily interviews and observations to study officers’ perceptions of technologies and their engagements with them.

Christin (2020) differentiates three possible ways for studying algorithms that apply to predictive policing in particular but also to other data visualizations studied here: 1) algorithmic audits studying in- and outputs quantitatively often to reveal discriminatory impacts (e.g. Lum and Isaac, 2016), 2) cultural and historical critiques situating algorithms in political, racial, and economic formations based on adverts, industry publications, and journalistic materials (e.g. Benjamin, 2019; O’Neil, 2016), and 3) ethnographic studies that interrogate technologies in practice (e.g. Brayne and Christin, 2020). The latter strategy is best suited to move beyond the techno-deterministic and speculative narratives prevalent in the literature described above (Brayne, 2017; Sandhu and Fussey, 2020) – the overly generalizing cultural and historical critiques, and the decontextualised ‘fetishism’ of algorithmic audits (Christin, 2020; Monahan, 2018). Even though not an ethnography in the classical sense of a long-term empirical engagement with a group of people (Fassin, 2017), this thesis does follow its inductive logic and employs semi-structured interviews with individuals and groups, participant observation, and review of relevant documents in the form of policies, press announcements, laws, and more. Collectively, these approaches provide a ‘thick description’ of the operational settings and officers’ interactions with technology. To contextualise discretionary decision-making during stops, the analysis in chapter 5.2 also draws on quantitative data analysis of publicly available police data.

The following first outlines the choice of field sites and how access to them was negotiated, it then thematises the challenges of the practical work and finally describes the process of analysing the data.

3.1. Field sites and access

The language of ‘sampling’ common to method textbooks suggests that researchers have a choice in selecting who to study, and even more, reminiscent of quantitative methodologies, that chosen cases are comparable, or at least exemplary. However, it is commonly acknowledged that gaining access to police departments is challenging (see e.g. Monahan and Fisher, 2015), turning the question of how to choose a case into one of how to access it. Moreover, as will become visible from the contrast between the two cases analysed here, the technological assemblages and their affordances for organisational power relations and individual decision-making differ considerably from department to department. The goal of presenting these two cases is not to make generalizable claims about technological practice in other police departments but rather to problematise it and raise wider issues for discussion that may or may not (yet) apply elsewhere[14]. Thus, although the process followed for this research could be characterized as ‘illustrative’ or ‘evocative’ sampling (Mason, 2002: 126), or, better, ‘opportunity’ sampling followed up with ‘snowball’ sampling asking for further contacts (Patton, 2015: 284ff), it is perhaps best to describe how access to the two case studies discussed in this thesis was achieved, and why the two locations are of value.

[14] See Rabinow & Rose’s (2003) perspective on Foucauldian critique.

The United States and the United Kingdom became research sites for this project as the main locations in the early academic and public discourse on predictive policing[15] which closely links the two countries. CompStat, often portrayed as the precursor to place-based predictive policing, comes out of the New York police department (Willis, 2014; Wilson, 2020) and, drawing on a common literature in environmental criminology, predictive policing developed in parallel between efforts by researchers in London with first tests in Manchester (Johnson et al., 2009; Maguire, 2018) and in various projects funded by the National Institute of Justice in the US (National Institute of Justice, 2009). Within this context, the US police department studied here has been one of the early adopters of CompStat in the past and recently introduced many new digital tools in the wake of a consent decree requiring increased reporting and oversight, and the UK police force has served as a testing bed for adjusting a commercial, US based Big Data analytics platform to policing which now bundles all its data and makes it accessible to every officer. Thus, the two police forces provide unique insight into the digital transformation of policing.

The first case study is set in a large metropolitan police department in the United States with over 1200 police officers. In 2017, one year before the fieldwork, the city had one of the highest crime rates in the US. The department has undergone and is undergoing major cultural change having been placed under a consent decree with a federal monitor ensuring that policies and procedures are in place that bind the department to constitutional forms of policing. A lot of the technologies discussed here, such as body-worn cameras, electronic police reports, and

[15] This does not mean that the application of predictive policing is limited to the US and UK. Predictive policing can also be found, for example, in the Netherlands (Oosterloo and Schie, 2018; van Brakel, 2016), and Germany (Egbert, 2018; Gerstner, 2018). Even more so, while at times these are later adoptions inspired by UK and US approaches and translated to local contexts, some of these have been developed in parallel – at times even earlier – based on the new availability of digital crime data. Examples for this are KeyCrime deployed already in 2008 in Italy (Mastrobuoni, 2020) and PreCobs to which the developer claims to have had the idea in 2000 (Ifmpt, 2018).

field interview cards, were initially adopted to monitor compliance and had later found additional uses. This situation makes the department unique in having a well-developed corpus of policy documents regulating the use of technologies, and, at the same time, many officers that are learning to use new technologies who can tell of the changes they bring about.

Access to the department was enabled by the head analyst serving as gatekeeper to the organisation and making introductions to various units. I first met the head analyst at the IACP conference in 2017, a professional conference and exhibition, where he had presented the department's compliance monitoring. I had visited the conference because of articles about predictive policing I had identified in the IACPs monthly magazine and had been able to organize several other interviews at the conference's location which could not be included here for lack of space. In several Skype calls with the head analyst I (later together with thesis supervisors Prof Pete Fussey and Dr Daragh Murray) developed a research proposal that would allow us to study officers' engagement with technologies and provide feedback to the department (see Appendix 11.1). This was approved by the chief of police and the head analyst facilitated wide-ranging access to officers in different sections of the organisation and of varying ranks. I carried out ethnographic work over four weeks, of which the first week was conducted as mostly interviews and two ride-alongs together with the thesis supervisor. These first interviews were instrumental in securing further access for the following weeks. In total, the fieldwork comprises of interviews with 49 officers and at least 39 hours of observation in three districts and at headquarters. It includes five ride-alongs with platoon and task force officers, as well as time with district detectives. I also observed four CompStat meetings at district and headquarter levels.

The context of the consent decree in which external and internal observers had scrutinized the compliance of officers with legal and policy standards, in addition to the aim of gaining a picture of the whole organisation within a relatively short time frame presented a challenge of needing to continually negotiate access[16]. The way a sergeant introduced the department's anonymous job satisfaction survey is an illustration of this apprehension towards information collection: "Now, this is about the federal monitor tryin' to find out what we think about the department" – suggesting for officers not to take part. Despite this, I achieved good access to many parts of the organisation and officers were open to sharing their perspectives with me. I built on the preparatory conversations with the head analyst to get a sense of the department's culture before arrival, identified key interlocutors in advance from organisational charts and sought to become conversant in acronyms and other elements of the department's language to build rapport. Apart from introductions by the head analyst and approaches via email, officers regularly introduced me to further people to speak to, and, while 'hanging around' by the station, officers I had met previously would offer me to accompany them. By the end of the month, officers were accustomed to me being around, as illustrated by this fragment from a conversation between multiple officers:

> "Does he have a body camera too? They need to get you a body camera, and a gun, [crosstalk]. Look, every time he comes, we're gonna give him something extra. Next time, he's gonna have a taser. Then a whole duty belt, then a uniform, then a badge, then he's just gonna be a police officer, and he's gonna be like, wait what's going on" (Task Force Officer 7, District B).

The second case study is a mid-sized British police force with over 2500 officers. The force is a pilot force for the digitisation of policing and the use of individualised risk scores for prioritisations. In the context of this research, I had made a list of police forces in the UK which according to media reports were using predictive policing and I had contacted multiple of those

[16] Although not helped by the context, this is common for ethnographies of police (see e.g. Marks, 2004).

forces via email for interviews. Again, these interviews provided a wider context but could not be included in this thesis. At the end of these interviews I would ask whether the interviewee was aware of any other forces I should speak to and this police force was named multiple times as being ahead in its technological capabilities. Thus, this case could be an indication of the future direction of British policing. I contacted the force through an address for general enquiries and was given the opportunity for a first interview with the Business Intelligence Manager responsible for the data visualisation platform. At the end of this interview, I asked if I could speak to some of the users of this software. After submitting a formal research proposal (see Appendix 11.3) and confirmation from the College of Policing that such research would be valuable, I was introduced to 10 ‘power users’ of the software via email. I was able to arrange interviews with 6 of them (with non-responses from the others). A seventh interviewee joined one of the interviews. While the interviewees covered a wide range of police functions, there are of course limitations in a) the low number of interviews, b) the lack of observations, and c) their characteristic as ‘power users’ (early-adopters who gave feedback to the developers or ranked high in the automatically recorded measures of engagement with the software). But they provide a rare glimpse into the effects a central data platform that allows officers to do their own analysis can have on policing in the future.

While each case could stand on its own, various contrasts between the two allow deeper insight into the kinds of questions the use of digital tools in policing gives rise to. In this, this study follows what Ragin (1992) refers to as a ‘case-oriented’ approach to comparative research that sets boundaries around the places and times studied, as opposed to ‘variable-oriented’ comparison examining cases in their variation along pre-defined variables. As Becker (2014) argues, comparative reasoning through cases allows social research to identify factors that explain the relationships obscured in conventional social research, to identify new variables, and ask new questions. For instance, the relationship between officers and technology is often portrayed in a techno-deterministic way in which the technology dictates officer action, while this research demonstrates the messiness and entanglements of that relationship as well as pointing to the affordances that become particularly visible in the contrast between technologies employed in the two locations. The reasoning by analogy, central to Becker's (2014) approach to developing more general ideas about how society works and common to science and technology studies, reveals for example the shortcomings of the concept of 'centres of calculation/translation' (and need for reformulation) where suddenly centre and periphery are not as clearly distinguishable anymore (see chapter 8). Such an approach is, as Becker (2014: 121) highlights a never-finished analytical process: the findings provide starting points for understanding what happens elsewhere but cannot explain it fully. As he writes, "close observation invariably shows that, even in the most ordinary situations, more than a few easily measured variables are at work and that everything in the situation has some effect on what happens next. If any one of those things isn't there or, better put, is there in a different degree or in a different form, the result (the next events that happen) will differ" (Becker, 2014: 2).

3.2. Dynamics of interviews and fieldwork

Interviews were carried out as ethnographic interviews employing a conversational style and accompanying observations made in the field (Patton, 2015: 432). I used a list of questions to loosely guide the topics I would cover (see Appendix 11.2 and Appendix 11.3).

In the UK, interviews lasted around an hour each and were audio-recorded. The officers seemed keen on explaining their work to me and interviews developed as conversations – usually in a pattern of initial questions according to my interview guide and questions for clarification, followed by a more open discussion for the last 20-30 minutes of the interview. The main limitation of these interviews lies in officers' hesitance of showing me what they would do in the software out of a concern for sensitive data. Consequently, in some interviews, I had to rely on my notes and memory of a 'scrambled' version of the software I had been shown in the first interview. Some of the officers also dealt with the problem by not opening any underlying case files but showing the top-level data visualisations.

The ethnographic work in the US was of a different character. As Souhami (2020) notes, police ethnographies contain repeated tropes of (moral) challenges the researcher needs to overcome to gain the trust of her interlocutors and tales of physicality, risk, and endurance. While I could tell stories of risk from some of the participant observations in the US, these would not contribute much to the aim of this thesis. After all, these moments of 'action' are part of police work, but they are typically not the moments of engagement with information technology and traffic stops are, although officers stressed the possible dangers, more routine interactions. Perhaps the ethnography in the US department is less of a classical police ethnography and more of an ethnography of technology use. Apart from gaining access, the main practical challenge was gaining officers trust – however, given the relatively short duration of fieldwork and reliance on interviews, not in the usual ways of 'building rapport' or partaking in morally questionable jokes and actions[17]. Some officers displayed initial scepticism towards me. For example, one commander asked half-jokingly, "You are not from the KGB, are you?", and another officer's gaze seems to check for weapons. Especially given the context of the consent decree and to prevent being seen as a 'spy' for senior officers (Souhami, 2020), I would assure officers that I would anonymize them, and I adjusted my note-taking behaviour according to how it seemed to be received (some seemed suspicious while others seemed to read it as me being

[17] Indeed, Souhami (2020) questions the necessity of this for short term engagements.

interested in what they had to say). I would also explain the purpose of the research and, to legitimise it, refer to the value for the department. In one instance it felt as if the officer was taking part solely because he was ordered by a senior officer (Ericson (1982) also describes this problem). In this case, I ended the interview early. As participation in interviews was often spontaneous, I would sometimes speak to officers of different ranks in which case sometimes hierarchical dynamics entered the conversation with officers deferring to their seniors. Generally, however, officers were very forthcoming and became more so over the course of the interview. In one case the interviewee told me at the end of the interview,

> "Ok, I was very apprehensive about this meeting because, I mean, you've probably dealt with enough police officers to know that we're distrustful of people who want to find out how we do things. But this was very pleasant" (Major Case Narcotics Detective).

Police can be an intimidating environment (Marks, 2004: 873). While not the case in the UK department, there were two instances of being surrounded by trained task force officers in the US that felt intimidating for their stature alone. However, given my positionality as a white male researcher from the UK, this felt never problematic and I was not challenged even when I asked critical questions – as opposed to a black, female interviewee from a software company interviewed for this project who, in a different department, was aggressively asked whether she was 'pro-police'.

An issue that existed, for both the US and UK police departments, was the difficulty of following the coded language officers use in referring to tools, crime types, radio codes, and organisational structures in abbreviations and numbers. Over time I became more familiar with this vocabulary through a mixture of asking for clarifications with officers that seemed keen to explain their work to me, and carefully reading policy documents and other publications.

3.3. Analysis

In the evening or while ‘hanging around’, I completed the short notes I had jotted down during interviews and observations. Later I typed them out and collected them together with the transcriptions of the audio recordings. I then exploratorily coded this data first in NVivo, adding categories for anything that seemed interesting (see Appendix 11.6 and 11.7 for the codes). I then printed these categorised quotes and arranged them spatially into clusters. Beyond attention to knowledge/power relations and the aim of taking technology seriously, these categories inductively produced the framework of analysis. The final thesis is the result of an iterative writing process in which sections were repeatedly rearranged to make sense of the data.

3.4. Ethics

The research underwent thorough ethical review and was granted approval through the university’s ethics procedures. As the research in the United States was funded through and aligned with broader work in the ESRC funded Human Rights, Big Data and Technology project at the University of Essex, it additionally received a higher level of institutional approval required for research projects in accordance with the ESRC’s framework for research ethics (Economic and Social Research Council, 2015).

In the UK, I provided interviewees with a consent form and an information sheet (see Appendix 11.4 and 11.5), explained the purpose of the research in general terms, asked for permission to record the interview, and stressed that they could choose to not answer questions or withdraw from the interview completely at any time. One interviewee was at first concerned that he could not speak for the force and I reassured him that I would report views as officers’ personal views, and that they and the force would be anonymised. Consequentially, he consented and all interviewees in the UK agreed to audio-recordings of the interviews.

While carrying consent forms was not practical in the US department, I clearly explained the purpose of the research, asked for oral consent, and pointed out that participation was voluntary.

Audio-recordings were transcribed by me, and, in case of some of the US interviews, a vetted transcriber who signed a non-disclosure agreement. To protect participants and allow them to speak freely, all transcripts were anonymized, and no interviewees are named in this thesis. Personal information was stored in a locked container separate to the data.

As mentioned above, dangerous situations were not central to the research and risk to the researcher was minimal. I wore a bullet-proof vest during ride-alongs with task force officers.

Data Part 1. Practices of data policing in the US: From strategy and oversight to patrol and investigations. Preface to the US case study

The following three chapters comprehensively interrogate the data and digital technology practices in a metropolitan US police department. It is organised into three chapters: the first chapter details the idiosyncratic ways in which crime and accountability numbers are created in the backrooms of the department and how they – and the social practice of CompStat meetings that they are embedded in – drive priorities. CompStat meetings are held weekly both at headquarters where the districts have to report to the chief and at the district level where lieutenants and sergeants report to their respective commanders. Meetings largely consist of communication of updates, discussion of crime and clearance rates, and narratives of individual crimes. In addition to this core of the original CompStat meetings as for example described by Manning (2008), meetings also contain an element of compliance monitoring demonstrating the multi-dimensional uses of police data. This chapter particularly pays attention to the ways in which the statistical knowledge of crime negotiated in these meetings has to be translated into strategic instructions for and by officers – often through its contextualisation in officers' tacit knowledge of crime in their districts. Here, data open spaces of subjectivity and instrumentality in its interpretations and in its translation into practice. The analysis also reveals an underlying tendency for crime trends to support territorial responses to crime rather than the targeted policing of serial perpetrators favoured by many in the department. For both compliance and crime data it further problematises how the categorization inherent to counting equates difference and invisibles connections across categories.

The second chapter investigates the affordances of technologies used by officers on patrol or responding to calls-for-service. These include radio dispatch, databases, and electronic forms.

Looking at frequent breakdowns and the various workarounds officers find to them, the analysis here demonstrates the highly fragmented nature of technological practice in policing where fractures in the technological infrastructures are complemented by the unevenness of adoption and enthusiasm among officers - an overarching theme of this and the third chapter. The main contribution of this chapter lies in unpicking the role of databases in structuring interaction and suspicion formation during stops, adding a crucial non-human element to this area of research. A central element of this is a rising tension between officers' empathy and leniency towards the stopped individuals, and the recordings of previous stops pushing towards enforcement and an amplification of deviancy.

In addition to the fragmented nature of technological practice, the third chapter pays special attention to the spatio-temporal affordances of technologies in investigations and proactive police work. These render the past available for investigations in unprecedented detail but are often bound to the specific spatiality of the infrastructure of police practices. Another aspect are the ways the use of these technologies structures the temporality of investigators work where the continual overwriting of recordings requires instant action or where data overload consumes many hours of work. The technologies and types of data discussed here are police databases, social network charts, body worn cameras, video surveillance, license plate readers, social media, and phone data. Lastly, this chapter also engages with some of the legal and ethical concerns around these technologies. Concerns include the easy accessibility of information on social media and the use of fake profiles for this purpose, as well as the curation of evidence and the question of how much evidence is enough.

The separation of these three chapters is a heuristic device to communicate the analysis. However, the practices described regularly engage with each other. As an illustration: numbers in the backroom inform strategic instructions, these are interpreted and implemented by officers on the streets, they produce reports which are used in turn to produce numbers; the reports, however, also form the starting point for detectives to investigate. The same tools are used by different parts of the organisation for different purposes and what is fed into the systems at one end is used by someone else at another. The following quote form the Chief of Police illustrates this,

> "[They] are the eyes and ears of the department. So, when they go out there […] and they stop a car and they go three people in it that's probably insignificant to that police officer. But it's really important for them to be able to accurately capture that information and sometimes they don't do a good job of doing that. And, if they mess up, they put the wrong colour car, or they make that mistake, you know, it's not a onetime mistake; I mean we pay for that later. But that information is really critical. It really is. […]. […] we do need to constantly remind our officers how important it is that those stops get [recorded]. Because it really can make or break a case, six months, a year later" (Chief).

The fragmentation of technological practice is partially related to the organisational split into districts with a high degree of autonomy. Officers at different levels have access to different systems and are embedded in different contexts of their use. Particularly for detectives, relationships with neighbouring departments, as well as state and federal agencies, allow some to have unique access to databases and tools the department itself does not own.

Given this fragmentation and the various interrelations, there is not one order that could describe and explain the actions of everyone and everything in the department. There is not one centre of calculation/translation that controls the whole organisation. Rather the findings resonate with John Law's (1994) theorization in *Organizing Modernity* based on an ethnography of Daresbury Laboratory: He argues that in contrast to the modern impulse of seeking total order, the social world is complex and messy. Order would only ever be aimed at in constant, never-ending processes of order*ing* and organisations would be shaped by a multiplicity of contradictory, interacting, incomplete, and materially heterogeneous orderings based on different ways in which the organisation is imagined. Thus, what would be obvious ‘centres of calculation and translation’ (Law, 2003) in chapter 4 – the CompStat meetings, the analysts, or the compliance monitoring team – are not quite successful in monopolising the aggregation of information and directing action. Looking more towards the periphery in chapter 5, the analysis demonstrates that both, the translation of central instructions from the emergency call centre has points of friction (despite forming one of the core ordering principles of police work) and the reporting of information into the central database or to a senior officer comes with its own challenges. More importantly, the discussion of officer discretion highlights the *part* the (central) database plays in discretion without determining it. The influence exerted here looks a lot more like the flexible strings connecting puppeteer and puppet than a direct translation of commands (Latour, 2005: 214ff). More successful in ordering action are the ‘obligatory passage points’ (Callon, 1999) created by the various technologies posing as central to solving cases and thereby structuring the spatio-temporality of detectives’ work as analysed in chapter 6.

What follows is a short description of the different functions present in the police department to facilitate the analysis in the following chapters: The police department is separated into multiple districts that are controlled by commanders who can set strategic priorities for their areas. Every district has three shifts of platoon officers, each led by a sergeant. Their main task is to answer calls-for-service. In the districts observed for this study the number of officers per shift was around twelve. In addition to platoon officers, each district would have a handful of task force officers working in two shifts, each led by a sergeant. Task force officers perform proactive policing in the form of patrols and surveillance mostly targeted at drug crimes. They set their own shifts and do not need to respond to calls-for-service. Finally, districts have ‘District

Investigatory Units' (DIUs) composed of detectives investigating property and persons crimes within the districts. Not all capabilities are available in the districts. Another division exists between the districts and the headquarters. At the headquarters, "central" detectives are tasked with investigating major crimes such as murder, bigger narcotics cases, child sexual abuse, or domestic violence. Another central function is a task force put together to address the city-wide problem of armed robberies. The headquarters would also host a group of analysts creating crime statistics, writing reports, and maintaining data systems. The administration, from compliance department to the chiefs of police overseeing all the districts and detectives, are located at headquarters.

Lastly, the technological practice interrogated in the following chapters is also conditioned on levels of adoption. Formally, one would expect uniform access to and use of databases and technologies by officers in the same position and with the same security clearance level. To some extent this exists with detectives having, for example, access to systems for background checks that ordinary officers could not use. However, access and adoption of different tools varies considerably between different sections of the organisation and individuals in the organisation. Partly this is due to several factors including training that is in progress and has only happened for parts of the organisation, individual preferences, or outright resistance. Whether the variation is systematic is outside of the scope of this research. Some officers suggest that older officers would be less likely to engage with new technologies compared to younger officers. Especially, senior officers of the armed robbery task force credit their younger officers with innovating by using social media for investigations. Others argue that differences would rather be down to individual preference. Despite regularly differentiating between the "old way" and the "new way", officers stress that they would make use of every technology available to them[18]. Both younger officers that rather stick to pen and paper, and older officers that are perplexed at the technological illiteracy of some of their colleagues have been part of this research.

4. Numbers that count – strategy and accountability through numbers

This first chapter consists of four main sections that interrogate the role of data in strategic decision-making and accountability. The first section details the efforts of crime analysts to unify and streamline databases, data processing, and dissemination of results – in other words, to improve the production of representations and the translation of effects on the periphery (Law, 2003). These require political engagements with those that control data in- and outside of the department, as well as those that use the data outputs. Efforts to streamline contrast with various idiosyncrasies in counting found in the districts. Here, parallel counting systems of various sophistication exist as the centrally provided data is no deemed fit for the plethora of ways in which commanders base their decision-making on them. As much as there is not one 'objective' way of counting crimes, there is not one 'objective' way to derive priorities and strategies from crime numbers. The status of different representations produced in 'centres of calculation' (Latour, 1987) and how to transform them into actions is messy. This is the focus of the second section. In the context of CompStat meetings, crime data open spaces for subjectivity and instrumentality. Data is used to motivate competition for lowering crime counts and it is selectively interpreted to ascribe crime reductions to police actions. In setting priorities and instructing supervising officers, commanders navigate between an aggregated knowledge of *crime* and the details of individual *crimes* communicated through the hierarchy. Where

[18] This suggests a possible disconnect between the narratives of age related differences in technology use described also by Côté-Boucher (2018) and the actual practice.

commanders base instructions mainly on crime patterns without tying them back to the underlying crimes, they risk promoting untargeted strategies like stop and search – strategies that, as this section outlines, officers criticise for being ineffective and causing tensions with the community. The third section analyses how priorities are translated into action by frontline officers. It describes the limited success of top-down communication of areas for patrol which often fail to connect with commonly maintained tacit knowledge, the horizontal communications that enable more long-term case building strategies based on surveillance, the information overload caused by a system supposed to streamline information sharing on things to look out for from detectives to patrol officers, and finally how assigning detectives to specific types of cases renders connections between those cases opaque. The final section on supervision through data mirrors many of the issues developed in the previous sections. Where counts have a close relation to the underlying infractions, they trigger clear reactions and succeed in centralising compliance management. But where they are based on the false equation of officers into categories supposed to enable comparison, the data becomes useless and supervisors stress the need for supervision in direct contact.

4.1. Data work – from crimes to crime

A lot of work is necessary to turn the steady inflow of police reports and other files into computable data and thereby allowing for the manipulation of scale that comes with the statistical accounts fundamental to the knowledge at a distance in centres of calculation (Law and Hetherington, 2000). This section first addresses the data politics that are associated with the analyst role. Analysts must solve political issues of negotiating access to data sources and integrating data systems, ensuring the quality of data input, managing expectations, and pushing for adoption of the tools they develop through training. Despite all these efforts, districts are still maintaining their own idiosyncratic ways of counting crimes resulting in competing orderings (Law, 1994). This is addressed in the second section that outlines how different understandings of the centrally provided data and the data's collision with operational purposes lead to a plurality of approaches.

4.1.1. Data politics - gathering and disseminating data

The central data visualization platform is a testament to the success of the analyst section in bundling previously disparate data and making it accessible across the department. Multiple officers mention how now they have insights into what happens in other districts that previously were unavailable to them. Even more so, a whole infrastructure for tracking compliance data had been created only in the context of the recent consent decree. As analysts are trying to maintain and expand the current capabilities they have to negotiate with others in- and outside of the department for access, and to ensure adoption by the officers that ultimately are feeding new data into the system. That is, the analysts are busy in maintaining and extending the ties that form their 'centre of calculation/translation' (Callon, 1986; Latour, 1987; Law, 2003). This section outlines the struggle they face in integrating disparate systems from databases and software that impart resistance to integration, to organisational units within the department and agencies outside having little interest in providing data, to the data itself being messy. The strategies they employ to counter these resistances range from scripts that copy data into their own systems and clean the data, to negotiation, to a combination of training and control. Some of the limits of their success manifests itself in the idiosyncratic ways crime statistics are used and maintained in different districts described in the next section. It also constitutes a running theme throughout this chapter with officers often finding their very own ways of using (or not using) the systems they are equipped with.

The department’s own data is held in multiple, separate systems which partially overlap and all require separate logins from officers. To change this, analysts had to negotiate access to these databases – access they would often only get through workarounds:

> “[…] people don’t want to give you direct access to their database but you can go on and download Excel spreadsheets, so then I have to make scripts that have this really weird work around to automatically download these spreadsheets and go put them in our SQL database. So, I feel like a lot of what I do is coding […] to try to get things to work together and line up” (Analyst 1).

In other cases, they would be unsuccessful as they would not have the clearance necessary to see data accessible to detectives, such as residence and financial histories.

Given these issues with internal data it is unsurprising that analysts, and the chief of police for that matter, struggle using data from other agencies within the criminal justice system, such as the jail, the courts, or the district attorney. What a district commander attributes to “piss games” between mayor, district attorney, sheriff, and police, is seen by the chief in terms of a lack of incentive to spend money to change existing systems so they could interoperate.

> “I’m not aware of any legislation that we have that prevents us from sharing data. It’s just that we create these little fiefdoms […]. […] to be able to share that data they do have to spend some money. So, why would they spend money for something that doesn’t really benefit them? And [data sharing would benefit] the public as a whole, but the way we’ve sub-divided everything, that’s when it starts getting complicated” (Chief).

Sometimes the data required for the analysis requested by others in the department would just not be available. Officers of the armed robbery task force had asked for a way to automatically identify possible robbery series. However, without any labelled data as to which crimes were probably committed by the same perpetrator, the analysts are unable to carry out any machine learning. Yet, the officers also did not want to manually label the data. Consequentially, analysts have to manage expectations of what is possible and with what effort. This example also highlights the human work that is behind all data, whether that is labelling data, as in this case, or just the daily recording of information in various forms (see section 5.3).

Having successfully acquired data and made it available in tools for officers, analysts are confronted with maintaining the system and driving adoption of its use. These tasks are interrelated as the training of officers would inform the quality of data input into the system. Analysts would have to clean the data as in the case of misspelled names:

> "[…] I spend a lot of time […] name cleaning, because […] they have a lot of open text fields[.] I have a Python script that goes through all the names in our database and basically figures out if there's duplicates and puts them into one. Marks them as this is actually one person" (Analyst 2).

Generally, electronic forms, although in principle being able to request very specific data from their users, cause trouble where they are not used as intended by their authors (the trouble goes both ways as officers' problems with the forms show; see section 5.3). As the analysts complain,

> "It's mostly that people get to type in whatever they want" (Analyst 3).
>
> "Or the fields do exist, they're just not used properly. […] They'll put it in the freeform narrative section when it should be fielded in the weapons or the vehicles section" (Analyst 1).

For this reason, and to drive adoption of their tools, analysts are engaged in training officers. The training works by recording the use of all digital tools and frequent checks. Here, two analysts discuss a training approach heavily reliant on monitoring the use of digital tools implying a power relationship between analysts and officers in which analysts push officers to adopt tools who are perceived to resist change:

> Analyst 1: “Tracking every use. Every time they click on it, we know”. [Laughing]
>
> Analyst 2: “We're giving them a quiz next month too”.
>
> Analyst 1: “I don't mean to be all big brother about it. We're not telling them beforehand”.
>
> Analyst 2: “We're just showing up”.
>
> […]
>
> Analyst 1: “Then they'll be motivated to do it for the next time, because we're going to go back a few times and do a few follow-up”.
>
> […]
>
> Analyst 2: “We were super nice the first time. This time we're going to be a little—“
>
> Analyst 1: “Still nice”.
>
> Analyst 2: “We'll be nice, but we're... [Laughing]...showing them we mean business”.

Apart from this combination of training and control, analysts use design to motivate adoption. For example, they would strategically employ visualization to increase uptake. In the case of social network analysis reports disseminated to detectives for violent crime investigations, the graphs are designed to be interactive and visually compelling (even though this does not convince all detectives as discussed in section 6.2):

> "[…] I think when you're trying to sell it to a detective; they don't want to see something that's just static and not very compelling. We were doing the diagrams in Analyst's Notebook[19] as a stopgap solution for a while and cutting and pasting it into the body of the email, doesn't really enhance the investigation and people weren't really using it so we had to come up with something different" (Analyst 1).

4.1.2. Idiosyncrasies in counting

Crime counts are crime counts – or are they? With a central data platform in place, it is surprising to see that not all district commanders rely on it in the same way. While the chief of the operational policing section has direct access to the analysts at headquarters, different districts have developed and maintained their own ways of accumulating, aggregating and interpreting crime statistics – their own little 'centres of calculation/translation' providing alternative orderings (Latour, 1987; Law, 1994, 2003). This contrasts with the analysts' struggle above to unify approaches to crime numbers and highlights the existing resistance to this. The head of crime analysts suggests that this is due to past errors in the data that had eroded trust. But beyond this, the examples below show that the changes in counting systems are reflecting the different purposes the numbers are put to, legacy processes that are protected, and varying awareness of issues with the central system. This section unfolds the idiosyncrasies in dealing with crime numbers that exist in different districts. While all of them attach a lot of importance to the numbers, approaches vary from ignoring glitches in the central data system, to keeping one category of arrests separate, to a complete parallel system of counting crimes.

In District C, the deviance from the central system is minor but reflects that changes are made where it does not resonate with local purposes. Here, the lieutenant creates his own sheets with

[19] IBM i2 Analyst's Notebook is software standard in policing investigations. It is used to render networks and map evidence temporally and geospatially. Examples are mapping phone calls or financial transactions.

crime counts and percentage changes for the district. On one of the printed sheets, he notes that he would be using dispatch codes for his crime classifications rather than the categories used in the central system as these are operationally more important. For example, in the central system misdemeanour arrests included ‘catch and release’ arrests for violations like running a red light. These would be irrelevant for strategic decisions. The two types of arrests would be separate in the dispatch codes that he uses.

A bigger deviation is visible in district B where a whole parallel counting system is maintained. Every Sunday, a detective in district B creates a report on the recent crime statistics for the district commander. Some of the columns in the report are titled “CompStat”, indicating it had been used already before the new data platform had been launched that renamed the CompStat meetings. The detective explains that the crime counts in the case management system would be way off what he would calculate. For instance, he has 30 incidents in his weekly count while the software shows only 6. Over a year the software would miss around 200 crimes. The central data visualisation solution, separate from the case management software, would also be of little use as it would regularly go offline on Sundays for updates – exactly when he would need it. Furthermore, the district’s detective lieutenant points out that while the central system’s inaccuracies would be mainly due to it updating too slowly for their purposes. It would also occasionally count events twice. Hence, the detective would create the statistics manually. He would start with the department’s report log which was “like gospel” (Detective 1, District B) and includes all reports written in a day. He would then compare this list with electronic police reports held in a separate system. These would not be accurate for statistical keeping as the recorded date was the date of the report rather than the date of occurrence which would have to be extracted from the report itself. Then he would check the record from the computer aided dispatch and look for signal changes where a call had been attended but it had been unfounded.

Altogether, he would filter crimes that had occurred further in the past, unfounded calls, and include crimes for which the report had not been submitted yet. Finally, he would compare these numbers against a spreadsheet filled by sergeants. Just as the analysts above he would have to deal with errors in the data. Even after multiple conversations about it, some sergeants would still change cells and he would have to correct it. “Everybody reads it different; everybody reports different” (Detective 1, District B). There would always be human error, irrespective of the amount of training. Lastly, some error in the data could not even be avoided by this meticulous cross checking of different reporting systems: Not all crimes in the district would be recorded by the district’s officers. Crimes reported online would be recorded by a central unit and the university in the district had its own police force. Both would enter the systems with significant delay making it impossible to include them in weekly crime statistics.

All the complications that this detective encounters in producing the weekly crime count demonstrate the amount of decisions that had been taken, implicitly or explicitly, in creating the official crime counts for the central data visualisation system. While in the long run, these numbers are likely to converge, the time frames from responding to a call to records on the various systems seem to introduce sufficient variance and delay in the weekly crime numbers for the district to create its own. Apart from fuelling divergent accounting practices, this highlights an important time dimension to data: in its Latin origin data are givens. The detective’s experience, however, demonstrates that to arrive at a state of ‘givens’, there needs to be a process of giving – the recording and transmission of information by a variety of actors. With cases being discovered until long after they occur, this production process approaches its end only asymptotically. Consequentially, decision-making is always based on more or less incomplete data.

In contrast to District B, officers in district A use the statistics provided through the central data dashboard and the case management system. They seem unaware of the reasons for why sometimes the statistics shown in these programs would not match with the cases they remember. During one CompStat session, the detective sergeant for property crimes notices missing data in two categories: “For some odd reason it’s not showing the business burglary we had last week”, and then a little later “I don’t understand why property snatching is empty” (Detective Sergeant, District A). Yet, the rank is held accountable to these numbers by their commander and the lack in knowledge on how the data are compiled potentially leads to prioritisations that are not warranted by the data. This case suggests a need to explain the limitations of data visualisations to those who use them for decision making as discussed in the next section.

4.2. Making strategy – between crime counts and crime accounts

This section addresses the ways in which crime data informs policing strategy highlighting the variability of knowledge types that complicate the functioning of ‘centres of calculation’ as ‘centres of translation’ (see the ways of knowing differentiated in section 2.2). It starts out with an account of specialised analysis performed by analysts that successfully informs policy change. The two following sections interrogate the consequences that routine data analysis in the form of crime statistics has for setting priorities and instigating competition. From the allocation of patrol to the prioritisation of certain investigations, commanders often base their strategic decision making on the crime statistics available to them either through the department’s data dashboard or their own record keeping as described in the previous section. The interpretation of this data opens spaces of subjectivity and instrumentality. Commanders balance and translate between the technically mediated knowledge from crime statistics and the knowledge of individual incidents communicated through the hierarchy. As a result, practices vary between districts.

4.2.1. Specialised analysis

Before discussing the main avenue for numbers to inform day-to-day strategy, this section looks at the specialised analysis prepared by analysts to inform strategic decisions. These reports provided to commanding officers are targeted at instigating change. They mobilise the 'objectivity' of data analysis to change systems. Despite this fundamental influence and their successes, analysts are frustrated by cases where the currency of 'objectivity' does not gain traction highlighting the multitude of other logics that may conflict with their analysis.

One example of successfully implemented policy change based on data analysis is a new fine system for false alarms. As an analyst describes,

> "[…] so they actually created a fine system where I think it's either two strikes or three strikes you're out and then you get hit with a fine. Since that was instituted, the incidence of false alarm calls just dropped off 50% in the 12-month period that was implemented" (Analyst 1).

Other analysis pushes for a more proactive approach to repeat domestic violence "[…] because the pattern is that domestic violence will progressively get worse over time. We'll typically see ten [verbal altercations] and then a[n assault]" (Analyst 1). The aim is to send social workers before a case would escalate and thereby also reduce the number of hours officers would spend on domestic violence related calls.

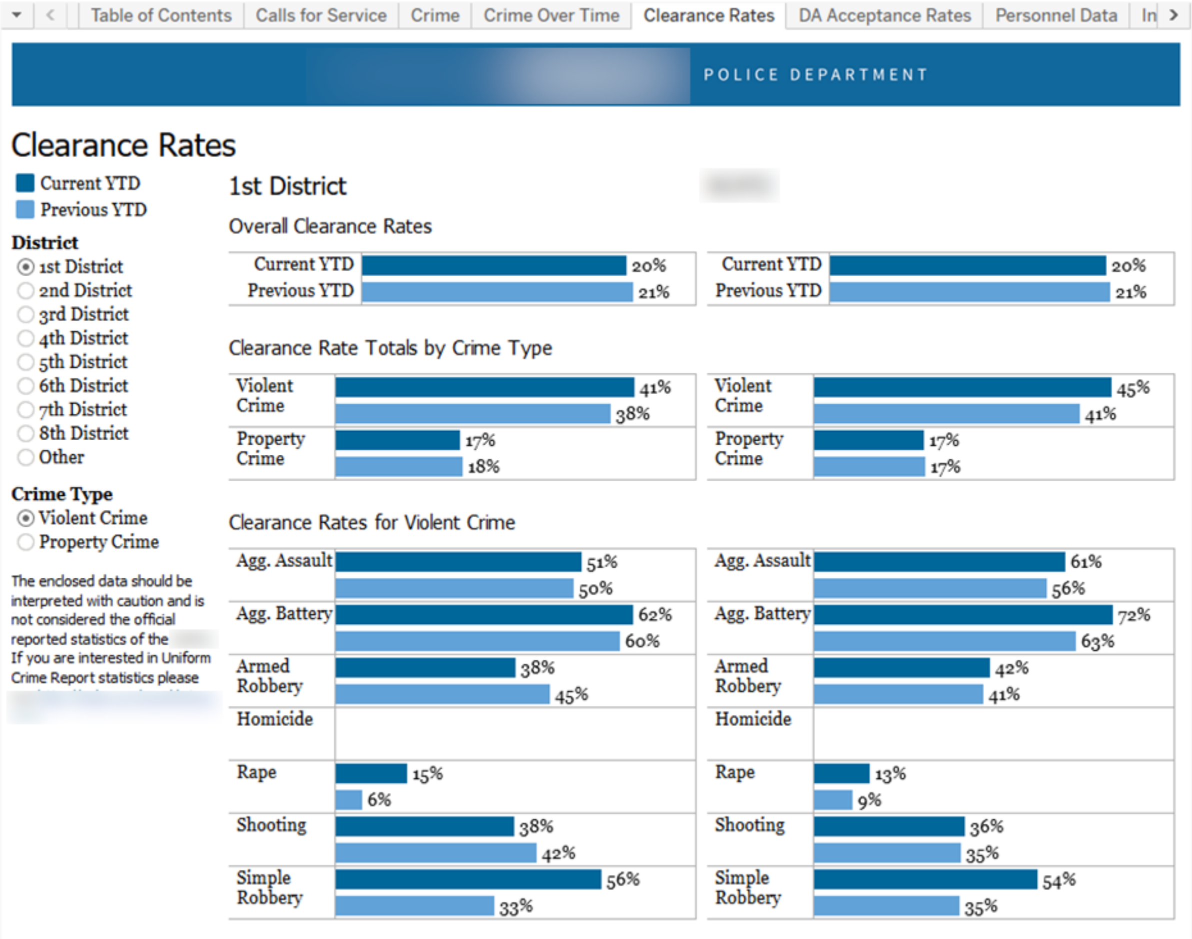
Paradoxically, while these examples and the data dashboard informing strategy decisions as interrogated in the following sections demonstrates analysts' success in influencing decision making, analysts feel that they have little influence in shaping policy:

> "I wouldn't say to date that we've played a huge role in shaping policy in any really meaningful way. Largely because I think the data doesn't always line up with what people want to see" (Analyst 1).

This juxtaposition of ‘data as it is’ and ‘what people want to see’ presumes a primacy of ‘objective truth’ versus subjective political priorities or knowledges. However, as the following sections demonstrate, the translation of crime statistics into actions is often less straightforward than analysts expect.

4.2.2. Instigating competition

CompStat meetings are an organisational management tool through which officers are held accountable to the crime statistics within their areas of responsibility. These meetings can instigate competition between different organisational units for example on who has the lowest crime rate – a form of ranked judgement central to the managerialism Feeley and Simon (1994) associate with ‘actuarial justice’. This competition may be wanted for figures concerning accountability but can be detrimental to strategic decision-making when commanders increase problematic strategies like stop and search to influence a number that may depend on factors outside of their control. The process is technologically supported by the department’s data visualization platform which displays rates and trends compared against the previous year and against the whole department (see Figure 1). This section reveals how numbers open spaces for interpretation and valuation that can drive competition between districts and priorities within districts. Some commanders mostly ignore the data dashboard, others let it inform priorities of what needs attention, and yet others instrumentalise it to measure performance.



Clearance Rates

■ Current YTD
■ Previous YTD

District
● 1st District
○ 2nd District
○ 3rd District
○ 4th District
○ 5th District
○ 6th District
○ 7th District
○ 8th District
○ Other

Crime Type
● Violent Crime
○ Property Crime

The enclosed data should be interpreted with caution and is not considered the official reported statistics of the [redacted] If you are interested in Uniform Crime Report statistics please [redacted]

Figure 1. Crime trends as displayed in the department's data visualisation platform.

In the past, as a detective in district B describes, CompStat meetings based solely on crime numbers had been “bastardized” when they had been turned into “a numbers game between the leaders”. With the inclusion of compliance monitoring (see section 4.4) and change in management style this had become less of a problem. Accordingly, the chief stresses cooperation between the districts:

> “[…] we’ve gone back and forth. Like, we used to have a lot of tension and now everybody really gets along. There’s a really good, big spirit of cooperation […]. Every once in a while, we get in a fight and I kind of have to remind everybody like, ‘There’s way more bad guys to go around’. […] we don’t need to be fighting about who’s arrested and who’s working which case […]” (Chief).

Yet, the way officers speak about crime numbers reveals how closely their perception of success and failure is linked to them. They frequently say things like, “we’re looking good, we’re down”. Note that it is not the crime numbers being “down” but “we”. Complementarily, officers from a district reporting a crime increase during the CompStat meeting at headquarters attribute it to bad luck (“once we get lucky that’s going to get better”) and try to move through their presentation quickly to avoid scrutiny. The data opens space for interpretation, and this is instrumentalised by officers when they associate crime reductions to police action.

However, the chief does not reinforce this focus on numbers as performance indicators and rather asks for details on the crimes and possible ways additional resources could help in addressing the problem – at headquarters’ CompStat meeting, the crime numbers set priorities but do not indicate performance. This is quite different in district A’s meeting where the detectives’ clearance rates, and the platoon and task force officers’ numbers of arrests, written reports, issued citations, vehicle and pedestrian stops and FICs are reported as performance measures – measures that senior officers are held accountable to by their commander against the context of the whole department’s figures:

> “This is what is holding up our clearance rates. […]. Let me show you, we’re pretty much ahead in every other category except that. […]. Our overall clearance is 4% over anyone else but this one is killing us. […]. This has been continually holding us down for the entire year. […] That’s not acceptable. Is our crime so different than the others? What’s going on?” (Commander, District A).

Given this focus, it is unsurprising that the CompStat meetings in District A make ample use of the department’s data visualizations. As indicators of performance, the crime statistics also drive priorities. Based on the statistics of the last four weeks the commander decides, “[…] armed robbery is our problem right now” (Commander, District A), and asks the sergeant to focus efforts on a suspect for a series of cases. Similarly, the property crimes sergeant is asked to focus on an uptick in residential burglaries.

However, the presence of a data visualization tool does not determine a competitive environment like the one in District A. While the violent crimes sergeant in district B mentions an increase in crimes compared to the previous year, the commander is more interested in the detailed account of what was known about the recent crimes. The priorities seem to be set by whatever crimes are currently occurring. Only at the end of the meeting, as kind of a routine check, a spreadsheet titled “CompStat” is opened (paradoxically, this spreadsheet is created because of a lack of trust in the numbers provided centrally; see section 4.1.2). This spreadsheet includes the crime counts for the past week and numbers of arrests. The commander asks for more ‘good’ arrests instead of ‘catch-and-release’ arrests that are handed out for violations such as running a red light. At least in this meeting, this is the only way that officers are held accountable to crime numbers.

4.2.3. Balancing information and strategies

This section sets out a heuristic distinction between two epistemologies at play in commanders’ strategic decision making: an epistemology of *crime* that deals with changes in crime statistics, and an epistemology of *crimes* that deals with the characteristics of individual incidents. The quantification of *crimes* into *crime* is argued to render links between cases invisible and pull attention towards patterns *within* crime categories. The section discusses maps as a translation device between the two epistemologies with a tendency to elicit territorial responses. It finally highlights officers’ criticism towards untargeted patrol strategies that are often a consequence of strategies based on an epistemology of *crime*.

While the department’s data dashboard is intended to make issues visible and manageable, it creates a new problem in that the data must be interpreted. As the chief describes,

> “The tough part is that we […] started to collect all of this data on all of these different management issues. And then how do I analyse that? All the data is given to me, I’m not a data person and I got a million thing[s to do]. […] all this raw data is just flying by you left and right. I try to look at some of it when I can, but it needs to really be condensed into something that I could do. Some type of way when a data is boiled down to: this is the problem, and this is what we’re seeing, and these are maybe some things we can do to fix it” (Chief).

Just as crime statistics inform prioritisation to differing degrees, as described in the previous section, the ways commanders decide which actions are to be taken are based on crime statistics in different ways and to varying extents. For instance, some commanders fixate their priorities on different numbers than others: The commander in district A describes using four- and eight-week comparisons instead of the standard 365-day comparisons to identify strategic priorities in the following way: “It’s not an exact science, it’s an art form” (Commander, District A).

There are two ways in which crime statistics can motivate action: a) an increase is important because more crime is the opposite of the police’s goal, and b) an increase may point to a series of crimes perpetrated by the same person or a similar underlying reason. In the first option, the knowledge of *crime* in general is the direct cause for action. Such an epistemology of *crime* can only entail untargeted action such as patrolling areas more intensively. Statistical ‘reasons’, that is reasons operating at the same level as crime rates, such as changing socio-economic conditions or ‘non-reasons’, such as random variation, are not considered. The second option, on the other hand, means searching for what causes a change in the crime rate. While a decrease is strategically attributed to past police action, a crime increase has to be explained. Reasons are sought in the stories that officers report on the crimes. Can they be connected into a series? Or, are there crimes that given the available evidence are likely to be solved and are therefore of less concern? This epistemology of *crimes* brings the crime statistics back into a frame of reasoning familiar to officers working on these cases. Contrary to the first approach this entails targeted action such as investigations or surveillance.

Quantifying *crimes* as *crime* can both add and subtract information. It adds information when the numerical pattern allows for making connections between cases. This is the case when an increase in crime prompts the search for underlying reasons such as a serial offender. However, it can also subtract information when the numerical aggregate is not linked back to the individual cases. This happens when crime counts drive untargeted action without consideration for the underlying crimes. Even more fundamentally, crimes need to be categorized to become countable. This means compartmentalising them and obfuscating the links that may exist between different 'types' of crime. A detective in District B describes how commanders would be "losing a lot of valuable data" by discussing only violent crimes in their weekly meeting and ignoring the connections with other crimes. The type of case is leading the decision-making rather than the criminals linking those cases. Similarly, the way cases are presented at CompStat meetings, crime counts suggest focussing on changes *within* crime categories: in the context of a recent increase, the commander in District A asks if there was a serial perpetrator *within* armed robberies. Patterns that cross these categories are easily missed. Last but not least, there can be errors in classification interfering with this prioritisation by crime type:

> "[…] a few weeks ago, there was a situation where there was a robbery that didn't get included in the list of robberies that needed to be talked about because the perpetrator implied that he had a weapon – as opposed to actually showing the weapon. […] I don't fault [the analyst] for not knowing but an implied weapon in a robbery is exactly the same as actually showing

> somebody the weapon. But she didn't know that so it wasn't included" (Major Case Narcotics Detective).

Apart from stories, maps are another device that allows to connect both epistemologies. Maps help identify areas of *crime* for patrol and connect isolated *crimes* into series of incidents connected by their spatiality. In district B, officers deliberate where and when to deploy patrols based on an interactive *crime* map[20] that is part of the department's data visualization dashboard. The property crimes detective sergeant in district A brings a physical map marking zones that he would like to see patrolled because of recent concentrations of auto burglaries. He identifies the crimes of opportunity mentioned above as those *crimes* that are not co-located with others.

Maps render spatial patterns visible (the commander in district A praises the newly introduced maps for making before unnoticed problems traversing district borders visible), but they can also distract from a view in which criminals are the focus and instead focus attention on 'criminal' areas. This falls directly in line with November et al.'s (2010) distinction of interpretations of maps as *mimetic* or *navigational* devices. Using maps for navigation means continuously relating between features on the map and direct observations. In the context of crime maps this means that the map guides through the crime data giving importance to some clues over others. But above all, a navigational use requires the establishment of a relation with officers' knowledge of the underlying *crimes*, possibly supported by an awareness of how the maps are constructed. Consequentially, the maps can be used in different ways, different officers will identify areas of risk differently. Contrastingly, in the, as the authors argue mistaken, mimetic

[20] Just as with many of the other technologies introduced further below, uptake of the crime maps varies from commander to commander. In district A, the only crime map is a physical board presented by one of the detective sergeants. The commander in district B makes use of the interactive map circling those areas officers should be focussing on, as does one of the commanders presenting at headquarters. Yet another commander finds the maps of little use as the colour scheme ("It's all gray and brown") would make them difficult to navigate.

interpretation of maps, maps have a direct resemblance with the territory they depict. As such a *crime* map depicts 'criminal areas' that the commander instructs their officers to target. In this vein, District A's commander speaks of 'taking back' an area and maintaining authority in an area. Similarly, District B's commander uses a map of patrol locations over the past two weeks to identify if patrols had shifted crime away from targeted areas. When commanders do not seek to translate the clusters of *crime* into reasons within an epistemology of *crime (*i.e. interpret maps *navigationally),* then the spatial rendering of crimes invites a spatial response in the form of untargeted police patrol. Fighting *crime* is territorial. However, in a second step officers regularly translate these territorial instructions into more targeted approaches based on their tacit knowledge (see section 4.3).

In practice, both epistemologies coexist. The allocation of police patrols according to where crimes are clustered is as common as prioritising investigations based on accounts of individual crimes or commonalities between them. The reasoning can also mix when only those crimes that can be linked through a suspected reason are targeted with unspecific patrol. The property crimes detective sergeant in district A, for instance, distinguishes auto-burglaries that could be part of a series from those that he suspects to be crimes of opportunity. The latter do not receive any further attention. Similarly, crime can receive both targeted and untargeted actions. The commander in district A asks the detective sergeant for violent crimes to have his detectives retrieve video evidence as quickly as possible on selected cases, as well as ordering some of the locations of recent crimes to be patrolled. Some of the mixing of approaches is due to the ambivalence of the patrol function between unspecific deterrence and territorial control on the one hand and intelligence gathering related to specific crimes on the other.

The quantification of crime renders connections between crimes invisible, drives prioritisation of police work by crime types, and, when not translated back into an epistemology of *crimes*, produces untargeted patrol strategies. In this way the constant availability and easy accessibility of crime statistics, as well as their embeddedness in the organisational procedure of CompStat meetings, stabilises a type of policing that many interviewees condemn. Patrol can entail rather unspecific stopping of persons and vehicles that seem suspicious in order to eventually come across someone responsible for crime in an area. By contrast, targeted operations aim at observing suspicious persons until enough evidence is collected to be sure that they are involved in crimes. From the chief to officers of the armed robbery task force to district task force officers, interviewees criticise the ineffectiveness and negative consequences of untargeted operations and contrast them with approaches that target specific offenders. Lieutenant and sergeant of the armed robbery task force distance themselves from an untargeted 'flooding the streets' strategy employed since the 70s that was inspired by New York Police's broken windows policing:

> "[…] are you familiar with the term jump out work? So, in other words, up till recently, in the last five years here, jump out work is: you get a unit, you get in an aggressive street, you get a sergeant and ten guys, they go out every night and they look for criminals, they look for guys standing on the street corner dealing dope, holding guns, they look for armed robbers, they look for different things like that. You see three or four guys on a corner, you think one of them has a gun, you jump out on, jump out work. It leads to a lot of arrests of drugs and narcotics, leads to a lot of chases, a lot of shootouts, different things like that" (Lieutenant, Armed Robbery Task Force).

They see the strategy as failed because a) it caused tensions and loss of trust in the community,

> "when you're stopping a lot of people for minor violations […], they might be good, honest people, but they maybe didn't stop all the way at the stop sign or they didn't put their blinker on and you're stopping them because you're just trying to find some crime to charge somebody with, you lose the public's trust […]" (Sergeant, Armed Robbery Task Force).

and b) it was ineffective as criminals, if caught, would be caught for only one crime,

> "[…] it affected crime in a specific area for a short period of time. The people that you got for those cases never did any significant jail time, unless there was some extenuating circumstance, they had multiple felony convictions" (Lieutenant, Armed Robbery Task Force).

and crime would be suppressed only momentarily:

> "[…] you got to have a part of your response that's trying to catch the guys, because you could look at 10 different problems and always over deploy 10 problems, and what that does though is it drives your problem out of there or makes them quiet for a day or two, but if you never catch the criminal [the crimes continue]" (Sergeant, Armed Robbery Task Force).

Citizens recording police encounters on their phones, complaints against the police, and institutional pressures of a consent decree increasing scrutiny and the introduction of body worn cameras, according to the task force's lead officers, add further pressure to change the department's style of policing.

Consequentially, as the chief describes the new strategy is to focus on serial perpetrators,

> "Who do we need to target? You know, we know anecdotally that only a small percentage of people are causing a lot of crime in the city. […] And then how do we […] use that information to build a case against those individuals and get them off the street, you know?" (Chief).

Some units, notably the armed robbery task force and district A's task force, have the legal and technical knowledge to build these kinds of cases largely based on diverse forms of surveillance: covert surveillance, video surveillance, license plate readers, and, prominently, social media. These techniques are explored further in chapter 6. In contrast to untargeted patrol, the armed robbery task force lieutenant argues that this targeted strategy would be more successful,

> "[…] if you focus your attention on the crimes and the criminals committing them, you'll be much better off than just throwing a big wide net and seeing what you caught. The term is shooting a shotgun in the dark, turn the light on and see what you hit and go pick it up, so to speak, it doesn't help with reduction of crime. Look at the crime, solve the crime and understand who's committing the crime and then focus on those people and those groups of people and you'll be much better off with reduction of crime" (Lieutenant, Armed Robbery Task Force).

4.3. Translations – priorities between crime counts and situated knowledge

Strategic priorities, developed as set out in the previous section, need to make their way to the frontline officers who enact them. This section analyses four interconnected arenas of translating priorities into action. The first arena is roll calls – briefings at the beginning of each shift in which senior officers, among other information, give instructions to officers. Here, officers are told which zones to patrol given the decisions taken in CompStat meetings. However, officers rarely get to know the reasons why they are supposed to patrol these areas. Tacit knowledge of recent events and the social dynamics driving spatio-temporal crime patterns is maintained through informal contacts and, at times, helps to translate patrol instructions that otherwise go ignored. The second arena are horizontal briefings in task force units specialised in gathering information through surveillance to build bigger cases. Instead of needing to translate knowledge operating at the level of *crime*, these work with detailed knowledge of *crimes*. Consequentially, connections between crimes become visible. Briefings and mobile phone chat groups help maintain a common knowledge of operations. Third, is a system of BOLO ("be-on-the-lookout") emails intended to order the information flow between detectives and frontline officers. Officers' observations can be crucial to detectives' investigations and the knowledge contained in BOLOs could – and perhaps senior officers conveniently assume they do – transmit the detailed information that is lacking from roll calls in the first arena. Yet, the system is burdened with information overload (some detectives seem to see the number of BOLOs as a measure of productivity), information is often irrelevant (as every email reaches the whole department), and emails are irretrievable once needed (poorly labelled emails are impossible to search). As a result, practices fragment with districts and individual officers finding their own workarounds with print outs and derivative digital tools. Finally, prioritisation of cases for investigation by detectives is compartmentalised into crime types. Apart from causing frustration for detectives working the same kinds of cases repeatedly, this type of prioritisation runs the danger of concealing connections between cases that cross crime types and that are necessary to build bigger cases as is done in the second arena.

4.3.1. Patrolling areas – translation into action

This section contrasts the often insufficient, formal communication of areas to target as developed in the CompStat meetings with the diverse channels of informal communication that enable a common awareness of recent events. This commonly maintained knowledge helps in translating instructions to target zones within the district with patrols because they give officers an idea of what to look out for – they link the instructions at the level of *crime* back to individual incidents of *crimes*. Furthermore, this informal information sharing allows officers to build their own tacit knowledge of spatio-temporal crime patterns that informs their personal decisions on where to patrol.

The patrol function is shared between platoon officers, who have to balance it with answering calls for service, and task force officers, who operate more independently patrolling areas or gathering intelligence to build cases. This gives task force officers the chance to build up more detailed tacit knowledge of their area as discussed further below. At the beginning of every shift, officers receive a briefing from their superior officers in a roll call. Roll calls differ from unit to unit (and day to day): some focus solely on instructions such as reminders to use digital tickets and assign radio codes, others contain an element of training. Among this information are also instructions to patrol zones within the districts. However, these instructions are infrequent, especially in contrast to the importance the identification of areas takes in CompStat meetings. Surprisingly, despite its availability, senior officers make no use of maps and graphs visualizing recent crime in the department's data visualization dashboard. Officers are frequently only told to patrol certain zones without any additional context. Consequentially, multiple officers do not know where these locations are and why they are supposed to patrol them. In one observed case an officer asks for clarification why an area is to be patrolled and the sergeant does not know either. Even task force officers, who are supposed to do proactive policing, would often struggle to translate the instructions into action, as one of them explains,

> "[In roll calls and briefings] it is normally disseminated from the top down saying, 'Hey, around this area right now this is going on. Around this area that's going on'. But I would like to be able to know a little bit of history of the place before I'm going there" (Task Force 3, District A).

Apart from an obvious breakdown of communications caused by a reference to zones that are taken to be clear to everyone, this reveals the problem that patrolling areas poses to officers on the frontline: Zones create an epistemological gap. Individual cases, including details on actions, perpetrators, motives, etc. are collected, stripped down, and centrally aggregated into a new thing: a pattern on a map. However, this pattern needs an explanation to be acted upon. Sometimes senior officers do this by linking patrol instructions to information on concrete cases. For example, during roll call, the sergeant in district A tells the officers to patrol an area because of an armed robbery on the previous night. She wants them to go to the location of the incident whenever they have free time, especially after dark since the lighting there was bad.

However, these concrete instructions are rare compared to just naming street blocks or alphabetically named zones.

These unclear instructions fall together with 1) a lack of time to patrol because platoon officers mostly answer calls for service:

> “I don’t have time to drive [up there just to write my reports]” (Platoon Officer, District B),

and, as already mentioned above, 2) doubts concerning the efficiency of visible patrol as a police strategy itself:

> “[…] it's like, you know, having a cockroach problem in a large apartment building. You get the cockroaches out of one apartment, but they've really just gone to the other apartment. […] So, I mean, it is beneficial, but at the same time […] that's not going to solve […] the problem” (Platoon Officer 7, District A).

Taking these issues together, it is not surprising that many platoon officers seem to ignore instructions to patrol areas.

Some of the confusion around which areas to patrol and what to look out for can be resolved through personal contact with the district detective sergeants and lieutenants who advise the commanders on which areas to patrol in the first place. Some of them would visit roll calls from time to time to explain why they would want certain zones to be patrolled. However, the relation between platoon and detectives differs between districts. A platoon officer in district B complains that information would “not transition very well” from the District Investigatory Unit (DIU) to platoon officers. They would get a list of zones that are “hot” without anyone explaining the reason. She describes the problem as a “downstairs-upstairs mentality”. There is some reason to take this quite literally with detectives located on the floor above platoon officers. This makes encounters and therefore information exchange between the two groups unlikely. By contrast, all rooms are on the same floor in district A. Even more so, the room used for roll calls is the same room used for all briefings: MAX sessions, task force briefings, platoon roll call. It is also located on a circular corridor that passes through the room. Hence, not only platoon officers would pass through the roll call but also detectives and task force officers, giving opportunities for chats. Consequentially, the "downstairs-upstairs mentality" seems to be less prominent in district A. Here, the detectives' sergeant comes into some of the roll calls explaining zones and recent cases thereby bridging the information loss. The transition of information from detectives to platoon and task force officers is also relevant for more targeted policing strategies discussed in the next section.

Informal communication channels, like those mentioned above, help sustain a real-time knowledge of what is happening within the district in lieu of centrally provided updates[21]. The roll call rooms provide a space for encounters and informal exchange. Not only does every platoon shift begin here, the roll call rooms in districts A and B also contain racks for the officers' body worn cameras forcing officers to return to the roll call room to drop off their cameras. This provides a chance for exchange between officers from different shifts. Commonly the returning officers would be asked how busy it was outside and, particularly while the new officers are waiting for the roll call to start, they would share a short story from their shift. Generally, patrol officers within the same shift, friendships formed in the academy, task force officers and detectives in the same district would often tell each other about what

[21] The literature on suspicion formation regularly assumes officers to possess experiential knowledge and 'cultural' influences are reduced to learned stereotypes and heuristics (see e.g. Johnson and Morgan, 2013; Quinton, 2011). However, as the analysis highlights here, this experiential knowledge is largely maintained in continued exchange with others.

happened during their shifts. This supplements officers' awareness of incidents during their own shifts gleaned from listening to what is communicated over the radio.

Especially for task force officers for who a substantial amount of work consists in patrol, this commonly maintained knowledge is conjoined with officers' tacit knowledge of spatio-temporal crime patterns in their districts. The self-description as "detectives of the streets" (Task Force 3, District A) embodies this aspiration to gather information on criminal activity in the present as opposed to detectives focussing on criminal activity of the past. This knowledge both helps translate areas of priority into action – possibly irrespective of the underlying crime statistics – and overwrite areas of priority where other, more concrete factors may outweigh abstract instructions. As an example of the tacit knowledge, a task force officer in District B explains, crimes would happen when people were drunk out on the streets after festivals, crimes would be associated with the location of certain clubs, and weekends would generally be busier.

However, task force officers' tacit knowledge goes beyond locations and times by including the social dynamics in their district. These could be specific community events creating opportunities for conflict,

> "So, like people gather around, […] and that's where if you wanted to go there and hurt somebody or confront somebody, you know they're gonna be at a community event […]. So, we have to be able to figure out when that's gonna happen and who's having an […] argument or something to beef in […]" (Task Force 1, District B).

or the dynamics created by shootings when specific persons would be involved:

> "if there's a shooting or a murder of who we call a 'player', somebody who's involved in street life, somebody who's heavy, then you're going to see an uptake in violent crimes" (Task Force 3, District A).

This type of single-event knowledge laying out paths of causation between different incidents is not reflected in the general crime statistics. But it can be used to tie spatial patterns back to potential perpetrators and thereby to more targeted action.

In the absence of any clues from this type of knowledge, task force officers attempt to build new knowledge by increasing surveillance in an area. As a task force officer describes,

> "[…] we'll set up surveillance […], and we'll have certain target areas during that time period, and we'll try to utilise the cameras or individual officers using surveillance vehicles or cameras. Even utilising officers maybe who are under cover […] so we try to find who is committing the crime" (Task Force 3, District A).

This strategy is chosen over untargeted approaches like visible patrol or stop and search. Yet, without any information on what has happened in a zone to warrant extra attention (as commonly the case for platoon officers), such a strategy is impossible and leaves only untargeted policing strategies that are widely criticised (see above). Where the priorities set by *crime* counts are not translatable into an epistemology of *crimes* and a desire to identify causes for the crime patterns, the two approaches collide. Perhaps there is no formal communication of what to look out for in zones assigned during roll calls because senior officers rely on an email system by which detectives send out this kind of information and officers are expected to update themselves (which as section 4.3.3 below shows is near impossible). A platoon officer describes this expectation but concedes that officers would often only know why certain zones are to be patrolled if they handled the crimes there:

> "It really is dependent upon you to look at your emails and just draw your conclusions from […] what the emails are put out there for the bulletins. A lot of times we don't really know unless you handled that crime […]" (Platoon officer 7, district A).

4.3.2. Targeting individuals – building cases together

The short-term prioritisation of zones for activities from patrol to exploratory surveillance, as described in the previous section, has a counterpart in longer term targeted operations aiming to build bigger cases on individuals. The exploratory surveillance detailed in the previous section can be a starting point to such case building if it does not immediately stop with the identification and immediate arrest of a suspect. This section details the aims of these operations and shows how communication structures like the informal exchanges above help maintain a common understanding of the cases and connections between them.

There are two units that I come across who operate by longer-term intelligence gathering: 1) district A's task force, when not bound by other day-to day priorities, employ conspiracy charges to build bigger investigations. They would connect individuals via social media (see also section 6.6) and gather video evidence (see also section 6.4) for a prolonged amount of time in order to then gain plea bargains. The involvement of narcotics would often lower the threshold for additional forms of surveillance. Officers argue that District A was in a unique position having three sergeants who had previously worked similar cases in a now dissolved multi-agency gang unit. They would understand prosecutorial culture and would know what works well in court. This institutional knowledge seems to be lacking in district B. 2) The armed robbery task force, being more flexible as an independent unit, use a similar approach in targeting armed robberies, shootings, and auto-theft. Here, the institutional knowledge is maintained in a close working relationship with the district attorney's office.

While the initial motivation to create the armed robbery task force came from a high number of armed robberies, the task force's strategy is driven by the tacit knowledge of *crimes*, which in turn reveals the interconnectedness of crimes that is lost in the crime numbers. Investigations unfold a network of actors and build evidence against them instead of arresting the first person of interest. As the lieutenant describes,

> “So, our main focus in this unit is serial robbers, guys who commit multiple robberies, serial shooters and we assist homicides and high profiles. With that said, we realised, when we started working these robberies, that these cars and guns that are being taken, stolen cars and stolen guns from cars, are being directly linked to the robberies and the shootings based on the tools they need to do it. […] so, we started focussing our time a little bit on the guys who are giving them the tools […]. We’re trying to […] [get] the prosecution of these guys to look at it a little through that lens, rather than just, it’s just a guy who got stopped in a car that he might have borrowed from somebody” (Lieutenant, Armed Robbery Task Force).

This approach reveals the connections between different types of crime – connections that are at danger of being concealed by crime statistics that need to categorize crimes to make them countable.

When working together towards a common purpose, districts’ task force units are small enough to enable direct information exchange between members. This horizontal information flow akin to the informal communications described in the previous section is necessary to work a common investigation in which individual officers may focus on separate persons of interest. This is particularly evident at the armed robbery task force where briefings are markedly different to the platoon and, to a lesser degree, also to the district’s task forces. The lieutenant describes a less hierarchical from of briefing:

> “[…] in the old days you’d have a sergeant who kind of ran units, this is what we’re going to do, this is our focus, and it was kind of cut and dry. Here, in our unit, everybody has an equal say when we have our briefings. At the end of the day, the sergeants and myself have to make a decision as to what we’re going to do because eventually it comes back on us, you know. But

> everybody talks and everybody does. When these guys go out in the field, we're not micromanaging them, we're not directing them to go do certain things" (Lieutenant, Armed Robbery Task Force).

Whereas task force and platoon officers' common knowledge of what is going on is maintained through random informal connections (see previous section), these communications are made more accessible and reliable by these in-person briefings. In addition, the briefings are supplemented with a common chat group that officers access on their phones. This makes communication possible at any time and makes it visible to anyone in the group. It also allows for the exchange of media files that transport information like a photo of a car which would be difficult to convey in an oral briefing and which is maintained in the phones' storage for possible later use. The accessibility of information on what to look out for is crucial, as the next section shows. The chat group is unique to the unit. As the lieutenant explains, this helps everyone to stay up to date,

> "[…] we all have departmental cell phones and we pass this on as we're in the field going. So, if you've got [three officers] out on surveillances and they see something, they take a picture of what they see and they put it in the group […]. We've got detectives who start looking at this guy and start researching the target location […]. […] we put it in here so that everybody has a sense of everything that's going on" (Lieutenant, Armed Robbery Task Force).

4.3.3. Failing to alert officers – "be-on-the-lookout" bulletins

Roll call, as described above, does rarely contain any information on things officers should look out for such as persons of interest or cars related to past incidents. The task of transmitting this information – operating on a level of knowledge of *crimes* – is taken up by an email system. BOLOs – "be-on-the-lookout" emails – sent by detectives to everyone in the department constitute an attempt to order information flow in the organization and make the information more accessible. The system replaces sending bulletins via FAX to the individual districts. BOLOs present a way for detectives to tap into the tacit knowledge and ongoing observations of front-line officers. Yet, BOLOs, like many of the technologies described in the following chapters, break down and cause fragmentation of approaches due to various workarounds. The system renders itself useless through information overload with a high number of daily emails, irretrievability of information where the relevant email needs to be found and information is hidden in pdf attachments, and irrelevance where BOLOs relate to incidents in other districts. Individual officers and districts try to counter these issues by returning to analogue print outs or derivative digital tools.

With all detectives sending emails the number of BOLOs platoon officers receive is predictably large. As a result, many of the officers are overwhelmed by the overall amount of emails received, including the number of irrelevant BOLOs relating to other districts. For instance, one platoon officer complains about receiving fifty BOLO emails a day and that some detectives would use those “emails [to] make you seem busy”. She deems the system so “overused that it has become useless”. Part of the issue of information overload is that many BOLOs contain information that is very unlikely to be relevant to officers in a particular district. A person wanted for a shoplift on the other side of the city, as one platoon officer explains, would be unlikely to travel into his district, and hence the BOLO would not be useful. Keeping BOLOs up-to-date and filtered by relevance seems to be a challenge given the lack of a system for detectives to add tags for filtering or retract outdated BOLOs. Especially outdated BOLOs present a problem outside of inefficiencies of police procedures if they cause unnecessary police encounters for citizens (this problematic is taken up again in the context of warrants in section 5.2). Furthermore, BOLO emails are sent out once but may be relevant for a longer period of time. However, it is near impossible for officers to memorize all of them. As a task force officer describes, “Once you check your email five days a week, you’re not going to remember Monday’s [BOLO]” (Task Force 5, District A). Even if they remember a relevant BOLO it can be difficult to find it again. For example, a detective in district B is unable to retrieve a BOLO about a gun that is relevant to a current case.

These issues cause districts and officers to implement their own workarounds, fragmenting practices of communication relating to cases. For example, district A uses print outs pinned to the back of the roll call room. This way officers see only those BOLOs relevant to them, the person charged with putting them up can take obsolete ones down, and they are available for repeated viewing. Several officers read through the pinned BOLOs before their briefing starts. Yet, while the push pin wall makes BOLOs more accessible, officers can hardly take the wall with them in the police car. The irretrievability of information is still an issue. For the BOLO to be of value, officers need to take note of it, remember it, and then be confident enough to act on their memory of the BOLO. For example, one officer is concerned that she would have seen the BOLO back in the station but would be unable to ensure the description in the BOLO matches the person she observes in the streets. However, this would be necessary to “act in good faith believe it’s them”. Consequentially, the use of BOLOs relies on lucky coincidence. This is not to say this would never work, as this example demonstrates:

> “I had just got done doing a report and I'm just like, I'm just going to check my emails really quick and it was just like pure coincidence that I had just checked the email and a minute or two later I see the guy just walking on by. Like, huh. [Laughing] So. […]. And I decided I'd stop them, and I ended up arresting him for the automobile burglary that he committed. So, they obviously, they do serve their purpose” (Platoon officer 7, district A).

To solve the push-pin walls lack of retrievability in the car, a task force officer in District A has found yet another workaround further fragmenting approaches. He helps himself by carrying print outs on his clipboard, as well as merging them into one big Word file which he would be able to open on a phone.

Despite all the problems with BOLOs, some detectives rely on them efficiently transporting information. One detective at headquarters even calls BOLOs “one of the advancements in the technology”. Some are probably aware of the issues as they affect them in similar ways (see the detective above who could not find a BOLO he remembered), but the convenience of just sending out an email together with the pretext of officers’ duty to read them makes them continue using it. Other detectives prefer to speak to officers in person. Communication, in person or in the form of BOLOs, between detectives and officers is important because it represents a way for detectives to tap into the tacit knowledge and everyday observations of frontline officers. A homicide detective describes how he would hope for more information after making officers personally aware of what he is looking for,

> “[…] let's say I have a murder in a certain area. I will kind of tag maybe the general assignment, the task force, and explain to them basically what I'm looking for, so they'll kind of be in that area, see if they see something. Let's see they see a car that kind of fits that description, they'll stop it, and they will give me a way more detailed FIC then maybe somebody who's just randomly stopped the car” (Homicide Detective 2).

FICs are field information cards filled out after persons and vehicle stops and containing information on observations the officer makes (these are addressed further in sections 5.3 and 6.1). The detective’s quote underlines the importance of communication between detectives and frontline officers, albeit this is hindered by a BOLO system that gives the illusion of effective communication in addition to gaps in hierarchy as described above.

4.3.4. Priorities in investigations – between crime counts and crime types

The way crimes are counted also influences how investigations are distributed among detectives and which cases are prioritised. Institutionally cases are split into bigger investigations carried out by detectives located at headquarters and day-to-day investigations pursued by district detectives. At headquarters these are further split up into different units focussing on crime types, such as homicide, sex crimes, or drug trafficking. In the districts, detectives work either on property or violent crimes. These crime types separating detectives are largely the same types that are used to count crime. Crime types compartmentalise investigations into investigation types and determine priorities as categories through which crime increases are monitored. Especially district detectives' priorities in investigations can be driven by day to day crime changes rather than the necessities of individual cases. This is described by a detective at headquarters,

> "Oftentimes, there might be situations where you would like to be able to take this further, but you just can't because there's another burglary […]. [The detectives] get more time to investigate […] but even they sometimes get to a point where you know, you may have this case and you're working it and you're getting somewhere but you know what, now you're tied up in the rotation again. So, now you're catching whatever this next thing is […]" (Major Case Narcotics Detective).

The district detectives' priorities would be set by crime trends,

> "Let's say there's been a rash of burglaries in a certain area, right? Well now that's the focus in that district, is clearing out these burglaries. But […] the drug deal that is going on a couple of streets over is kind of put on the back burner" (Major Case Narcotics Detective).

While in district B the caseload seems to decide if multiple detectives would work the same type of crime, District A detectives are regularly assigned cases of a singular type. This goes so far as to one detective only dealing with vehicle burglaries and thefts. This detective seems somewhat dissatisfied with his job as a lot of these cases are impossible to solve given the lack of evidence. Beyond the individual detective's job satisfaction, this type of assignment again renders the connections between cases invisible. This detective would not be able to explore connections to other types of cases. He might miss the relation between guns stolen from glove boxes and the shootings that follow, as it is observed by detectives in district B. Categorization for counting can, as discussed above, render connections that cross categories invisible. This is especially the case when these categorizations are institutionalised in job roles.

4.4. Supervision through data

The department has two mechanisms by which officers are held accountable through data. The first is compliance management that is part of the CompStat meetings. Here, officers from the compliance department review, for example, body worn camera footage and based on pre-defined score cards check whether officers comply with policies. Violations, such as failing to start a recording, are counted and published on the department's data visualization platform. This process centralises supervision and adds another level of supervision beyond the direct relationship between officers and their direct superiors. The second mechanism is a program called INSIGHT in which officers are compared against departmental averages for various performance categories such as the number of arrests or uses of force. These numbers are then used by direct supervisors for management purposes. In the first case the instructions for officers follow directly from the numbers. In the second, supervisors are less clear about what actions to take based on the numbers and some question the comparisons hardwired into the program. Although both arrangements could be described as centres of calculation and translation

(Callon, 1986; Law, 2003), only the first successfully translates into effects on the periphery in the form of compliance and reprimands.

While the crime statistics need to be translated into actions, the link is often significantly clearer for compliance data as it counts (in)actions. An officer takes too much time writing reports? Ask them to write the reports sooner. In contrast to the competition introduced by crime numbers the consequences of competing for compliance are clearly also more positive.

Compliance monitoring is an addition to the classical CompStat process made in the context of the consent decree. The idea is to go beyond holding officers accountable to just crime statistics in their area:

> “[…] it’s like a […] more enhanced CompStat I guess. So, what we wanted to look at was not just crime […]. […] You know, how well our office is performing on a bunch of different levels not just on being able to have effect on crime. You know, are we wrecking cars? Every time we wreck a car, it costs money. […] How do we measure use of force? […] How do we measure our response times? How do we measure public complaints? How do we measure satisfaction? A whole bunch of different things. So, that’s why we kind of try to dive into with our [data platform] a little bit. When before we only looked at crime” (Chief).

At headquarters, commanders report their statistics on compliance measures such as correctly uploaded and labelled body-worn video, time to fill reports, and use of force incidents. These presentations then give members of the internal investigations unit a chance to highlight reviewed cases that were handled well or that do not comply with policies. For example, the commander of the internal investigations unit highlights officers in one district not introducing themselves by name during traffic stops. In the districts, commanders check the compliance data and instruct lieutenants and sergeants to talk to their officers when they identify issues.

For example, in district B, two officers are singled out for their number of pending reports. The officers are then later talked to by their direct supervisors during a roll call. Where compliance may have been left to direct supervisors in the past, the data platform together with digital recording devices such as body worn cameras and field interview cards allow for a centralisation of supervision that adds to the supervision by direct supervisors.

The supervision of officers and detectives has always a technologically mediated element to it: the filling of forms and reports that are reviewed by superior officers (see section 5.3). Through these documents a centrally positioned supervisor can see what their subordinates are doing. For platoon sergeants, this system is supplemented with a live computer aided dispatch dashboard on which they can see which unit is responding to which call, how long they take to respond and how long it takes for them to handle the call. Apart from this direct monitoring of officers' actions, Insight is a data analysis tool that is available to supervisors to spot officers that may need interventions by highlighting those that deviate from the department average. The department's policy describes Insight as follows:

> "INSIGHT is [the department's] Human Resources and Personnel Management system and data warehouse which can be accessed by Department supervisors to receive and integrate member information in order to facilitate close and effective supervision of members as well as identify any patterns or series of incidents that may indicate at-risk behaviour".

Insight tracks information about, among others, arrests, uses of force, citizen complaints, civil lawsuits, and accidents – but also about awards received as well as commendations.

The program enjoys mixed uptake. A sergeant in district A would only pay attention to the email alerts she would receive from time to time when someone in her unit deviated from the department mean. Otherwise she would not have the time to look at Insight. A sergeant in district B, on the other hand, sees the program as a good way of checking officer' "productivity". However, for this supervisor, as for others, the counts need careful interpretation and the main supervision is carried out in person.

The main problems supervising officers identify with the system mirror in many ways the issues relating to crime counts identified in the previous sections. The numbers underlying INSIGHT fail to take qualitative differences into account equate officers in different roles and are at times erroneous. For instance, supervisors would need to carefully interpret outputs because expectations for officers within the same role could differ and the comparison to means would fail to take these qualitative differences into account:

> "[…] an average is technically looking at everyone and just kind of finding that middle point. But that doesn't mean that it's going to apply equally to everyone with that same title. There are some districts where people have to get into use of force situations more often, or certain watches, like the night watch […] versus the people who are working at 8 AM. And, so, if the same average is applied universally, it doesn't always work out that way" (Homicide Detective 3).

Here, the categorization necessary to make things countable creates a problem by equating those within the same category – a grouping that in some areas would be near impossible:

> "[…] we all do narcotics. But [this detective's] job is very special. I got a guy that's a K9 operator, alright? I got a guy that investigates strip clubs and stuff. So, although we are all part of the thing and we all go to do the enforcement part, we're all working together as a team, but we have very different jobs" (Major Case Narcotics Sergeant).

Apart from issues with categorization, the data used for scoring officers can be flawed. As a major case narcotics detective cautions,

> “[…] since it’s a database that the information still has to be put in by a person, it still has those same limitations of data being put in incorrectly, you know? It happens because people make mistakes. And some people are incompetent” (Major Case Narcotics Detective).

Similar to the knowledge of *crimes* maintained through direct communications, supervisors stress the importance of in-person interaction for supervision. For example,

> “[…] you still need to be there and have that human interaction because I’ll be able to see him on his days and see that he’s not himself. […] It’s one of those things where, you know, you can look at somebody that you see every day and you can tell whether something’s bothering him. Something’s wrong. Even if to somebody else they seem perfectly fine” (Major Case Narcotics Sergeant).

Finally, the more specialised the officer’s role, the more direct the supervision would be – rendering the technologically mediated supervision at a distance superfluous. As a homicide detective describes,

> “[…] our sergeants, our supervisors, actually go out on the scene with the people. So, they're not reading a report sitting on their desk that they don't have working knowledge of. […] Where, in a District, and a detective may go out and their supervisor's off. So, they really just reading what they say” (Homicide Detective 2).

4.5. Summary

Crime statistics as well as compliance numbers are produced in a complex process that involves negotiating access, integrating disparate systems, and cleaning data. A process that also, as the idiosyncrasies in different districts show, comes with a multitude of decisions on how to count, all of which affect the count and its use for different decision-making practices. Yet, through the social setting of the CompStat-style meetings, the statistics carry power: they set priorities in what crimes are addressed, they inform strategies on how to deal with repeat calls or domestic violence, they drive competition between districts, and commanders perceive of them as measures of performance.

Patterns in the crime data, spurious at times, have to be translated into strategies and actions. In the case of compliance this could be a straightforward instruction to an officer to keep up with writing their reports but it could also be borderline impossible when the statistics to be acted upon are based on misleading comparisons with a cohort of officers in distinctly different roles. In the realm of criminality, a gap between two epistemologies has to be covered: an epistemology of *crime* represented in crime rates and an epistemology of *crimes* represented in the commonly maintained tacit knowledge of locations and individuals related to incidents. The translation from the first, setting the priorities, to the second, finding reasons for the statistics, is achieved with accounts of details about individual crimes as well as maps as translation device. However, these translations are not always made or left to frontline officers without access to an overview of recent incidents. Spatial patterns are translated into patrol strategies supporting a territorial approach to policing that many officers discredit because of the strain it causes (and has caused in the past) to the community and the department's reputation.

The underlying segmentation of crime types necessary to make crimes countable risks obscuring links between crimes. This segmentation is institutionalised in the division of labour among detectives specialising in investigations of certain types of crime. Patterns across categories are easily missed while those within categories drive priorities. In this way, crime statistics as they are used in CompStat meetings undermine to some extent more targeted forms of policing focussing on serial perpetrators and networks of perpetrators active across different categories of crime. While crime numbers give room for subjective and instrumental interpretations, they, at the same time, shape subjectivity by confining it to the same categories that are the basis for their production.

Relating the findings in this chapter back to the concepts of ‘biopower’ and ‘centres of calculation/translation’ as introduced in the literature review, the contribution here is two-fold: First, it renders the knowledge created in these centres complex. Different priorities, or ‘orderings’ such as targeted investigation and police presence intersect with different ways of knowing in the form of *crime* and *crimes*. Perhaps the centre is too close to the action to solely rely on statistics and ‘biopower’. Second, the translations from the centre to the periphery by themselves interact with other knowledges and often become precarious or side-lined by other orderings. Similarly, the creation of representations as detailed at the start depends on constant work by the analysts and is still fragmented through parallel efforts. In the end, there is a plurality of orderings that ‘sort of’ work in creating somewhat unstable ‘pools of order’ (Law, 1994).

5. Use of technology during patrol and calls-for-service

In contrast to the previous chapter, this chapter looks towards the periphery, towards the officers patrolling the streets. On patrol or responding to calls-for-service, officers have two main sources of information: the dispatcher and other officers over the radio, and the department’s databases accessible to them through their on-board computer. Adding to the precarious control over where police officers patrol described previously, the first section demonstrates that even the central ordering principle of answering calls for service – the ‘reactivity theme’ of policing (Manning, 2008) – does not direct officers without friction. The second (and main) section investigates the extent to which the department’s databases inform officers’ decision-making – particularly during stops. Just as there is friction in delivering instructions to officers, there is friction in officers reporting information towards more central positions despite electronic forms designed to simplify the process. A continuing theme in this chapter are the breakdowns and workarounds officers find in their use of these technologies.

5.1. Dispatch and navigation – breakdowns and duplication of efforts

The main task for districts' platoon officers is to respond to calls-for-service. This section highlights the various technical breakdowns that occur in the communication of information relating to an incident and how officers arrive there. These breakdowns are due to a) the fixed nature of the technological solutions, that is free text boxes that are too small for their content and rigid, inadequate scripts for call operators, and b) the lack of technology for navigation. Where these technologies fail in their task, efforts are duplicated on other pathways such as radio communication, personal phones, or maps on the on-board computer. Yet, these workarounds cause further problems some of which officers perceive of as endangering their safety.

When a member of the public calls 911, this call is received at the department's call center. Here, an operator goes through an automated script of questions to collect all the relevant information concerning the incident. This information is directly entered into a computer and officers receive the information on their on-board computers regularly referred to as the "CAD" (computer aided dispatch). This happens as soon as the most fundamental information is gathered, that is location and type of incident codified in a radio code. Whenever there is a new call a sound cue alerts the officer and they can check the details of the call on their screen. When an officer takes the call another sound cue alerts the others that it has been taken up. Taking the call means telling the dispatcher, who is also located at the call center, over the radio. The call operator successively adds more information to the call as the script of questions progresses. This information is then updated live on the officers' screens. This is where the first instance of technology breakdown occurs: the box in which this text is displayed is fixed to roughly 2 by 10 cm. This makes it almost impossible for officers to read the information while driving towards an incident – particularly because all cars except one are operated by single officers. Not only do they have to scroll down within the box, they have to scroll down every time the dispatcher adds something to see the new information. Together with frequent connectivity issues of the on-board computers this means that some officers resort to asking the dispatcher for details over the radio instead. The radio steps in where the CAD fails, with the consequence of officers asking for further details taking away 'airtime' from other communications (the consequences of which are described further below).

Apart from being difficult to read, some officers are also discontent with the quality of the information relayed to them by the dispatchers. The call handlers follow a strict protocol which is automatically enforced by software that prompts them to ask specific questions in a pre-set order. To the officers, these questions would often not cover the information they would need about an incident. An older platoon officer says that in the past a former police officer had been taking calls and provided them with more relevant information. He highlights the experience necessary to ask relevant questions which contrast with the formal logic of the software. As a workaround, he would often ask the dispatcher to call back and ask further questions if possible. However, this is yet another way in which 'airtime' is taken up to support a struggling technological process.

Given their ubiquity, it may come as a surprise that police cars are not fitted with navigation systems. Consequentially, all interviewees describe how they sometimes struggle finding the location of an incident. Sometimes it would be the direction of a one-way street forcing the officer to drive around the block, sometimes they would just not be familiar with an area. As one of the officers describes:

> “[…] there’s these little, you know, quiet little neighborhoods that we never go into. […] the street might go this way one part. But you cross over the street and it goes this way […]. […] you’re trying to get up there in a hurry and […] these streets make no sense in this city. […] Your computer gets the cross streets. Those are fine and all but […] when all those streets start zig-zagging and going diagonal, then those cross streets aren’t really that beneficial anymore” (Platoon Officer 7, District A).

Similarly, street names can be confusing: “Once side is South and the other side is North. […] sometimes you hit the wrong address” (Task Force 4, District A). To avoid these issues officers help themselves by pulling out their personal mobile phones, open a street map on their screen, or ask the dispatcher, who can see the car’s GPS signal, for orientation. The first two solutions make driving difficult as they take the eye away from the street and, in case of the phone, the officer only has one hand to drive. Asking the dispatcher when lost, again takes up ‘airtime’.

With the radio duplicating efforts of the computer aided dispatch and standing in for the lack of a navigation system, the resulting increase in communications over radio would take up capacity officers would rather dedicate to more relevant communications. Officers are concerned that they may not be able to inform the dispatcher that they are taking action and in case something goes wrong no one would know where they are. A task force officer in district B describes this concern of needing to alert others of taking action:

> “People need to know where you are. Even if you’re doing something silly. Something like a little traffic stop can turn into a foot chase, can turn into a use of force, can turn into a deadly use of force. So, you want people to know where you are in case…” (Task Force 1, District B).

Another task force officer in district B expresses how sometimes a ‘crowded’ radio can frustrate relaying this information leading to the officer to have to weigh the risks of engagement,

> "I can't tell you how many times I'm like 'I can't get out' [because others speak over the radio]. You know what you say? Fuck it, I'm going anyway" (Task Force 5, District A).

The duplication of communication efforts on the radio because of breakdowns of the computer-aided dispatch system and a lack of navigation systems, brings radio communications to the limits of their information transmission capacity. As a result, officers fear information flow perceived essential to their own safety may be interrupted.

5.2. Databases during stops and calls-for-service – complicating suspicion formation and discretion

Whether on a call for service or stopping a vehicle or person, officers regularly search the police force's databases for persons, vehicles, and addresses. This section analyses in three parts the role databases play during stops and calls-for-service extending existing literature that has mostly focused on officers' direct observations and biases. It first explores how the database moderates officers' suspicion from the initial decision to stop a person or vehicle to the interaction with the stopped person. The second part interrogates the role previous police encounters recorded on the database play in officers' discretionary decision making on the consequences of a violation – e.g. whether to hand out a ticket or just a verbal warning. It highlights the consequences databases can have in amplifying deviancy, both during stops and in response to calls-for-service. Finally, the third section addresses the malfunctions of databases from incomplete or imprecise search results to breakdowns of information flow, their consequences for the interaction that unfolds, and the individual workarounds that officers find. The analysis is supplemented by quantitative appraisals of stop and search based on data published by the police department.

To initiate a stop, officers need to meet a threshold of reasonable suspicion. The department's policy defines this in the following terms: "Articulable facts that, within the totality of the circumstances, lead an officer to reasonably suspect that criminal activity has been or is about to be committed. The standard for reasonable suspicion is less than probable cause but must be more than a hunch or a subjective feeling". For violations of traffic laws the standard is increased to probable cause which the policy defines as: "The facts and circumstances known to the officer at the time that would justify a reasonable person in believing the suspect committed or was committing an offense". The policy further states, "The stop must be based on what the officer knew before prior to the stop. Information learned during a stop can lead to additional reasonable suspicion or probable cause that a crime has occurred, but it cannot provide the justification for the original stop". Officers must articulate the specifics of their probable cause and reasonable suspicion on field interview cards filled after each stop. These are checked by supervisors and the internal accountability section. It is within this reasoning on reasonable suspicion and probable cause that information from databases can have an influence. However, it is one source of information among many.

In a review of the literature on police stop and search practices, Johnson & Morgan (2013) identify four interrelated processes through which police officers develop suspicion: 1) officers would base their assessments on stereotypes relating to persons and vehicles. These would often be young men of low socio-economic status, in high crime neighborhoods, and from a minority ethnic group, or vehicles with tinted windows, certain bumper stickers, or vehicles in poor condition. 2) 'Known criminals' and locations such as drug houses are targeted more frequently. 3) Persons, vehicles, and behaviours that do not 'fit in' with the usual observations are observed more carefully. Often this suspicion is developed procedurally through longer observation and, during a stop, further questioning. 4) The authors also describe nonverbal cues, such as stutters, as contributing to officers' suspicion. Particularly the use of stereotypes would violate the police department's policy. However, Quinton (2011) finds for police in England and Wales that broad generalisations and stereotypes have the strongest influence on suspicion formation. With interpretations of situations being elastic, they could often be reinterpreted in a way that conceals the use of stereotypes.

While the subject of this section is the influence of police databases on officer decision making, any biases in who is stopped will necessarily be reflected in the databases. A look at the department's public dataset of police stops can help to develop an idea of these biases. As Figure 2 shows, Blacks make up a higher proportion of stops relative to their proportion in the city's population while the relation is reversed for Whites, Hispanics, and Asians. Blacks are 2.26 times more likely to be stopped than Whites (p = 0.000 in a Fisher exact test). However, this does not necessarily mean that skin colour is used as a signifier to form suspicion for stops. Not only may for example the driving population be different from the city's population (see McCabe et al., 2020), racism intersects with and is part of structural inequality which means, for example, that Blacks in the city are overwhelmingly more likely to be poor. Figure 3 demonstrates this with the city's distribution of household incomes by race. If probable cause is the policy threshold for a traffic stop, this means that those without the income to maintain their car are more likely to be stopped.

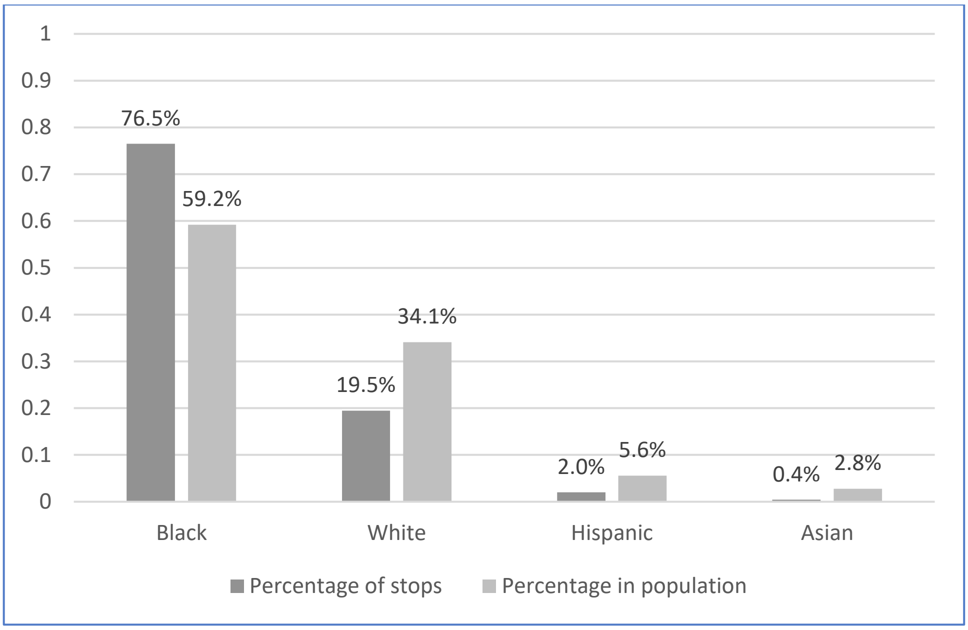


Figure 2 Share of stops by race for 2018 in the department's public dataset versus share of the population based on US Census data.

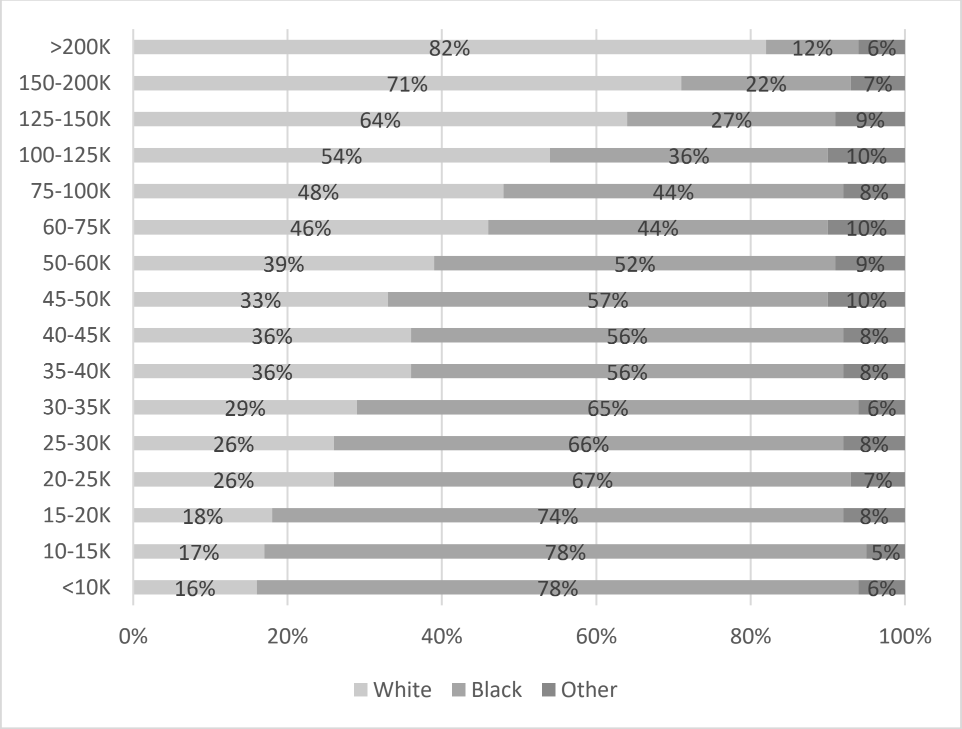


Figure 3 Household income by race based on US Census data.

Moreover, there seems to be no difference in the number of stops of Blacks during daylight and darkness. Following the logic of the ‘veil-of darkness test’ (Grogger and Ridgeway, 2006; Pierson et al., 2020), if vehicle stops were biased towards blacks, their share of stops would be lower during hours of darkness when police officers cannot determine skin colour as easily. As Figure 4 demonstrates, the rates remain very similar even if the light conditions change over the year (p = 0.404 for a proportions z-test, all times combined). This would suggest that, at least for vehicle stops, it is not immediately apparent that race would inform the decision to stop individuals, or to a degree small enough not to produce a significant finding.

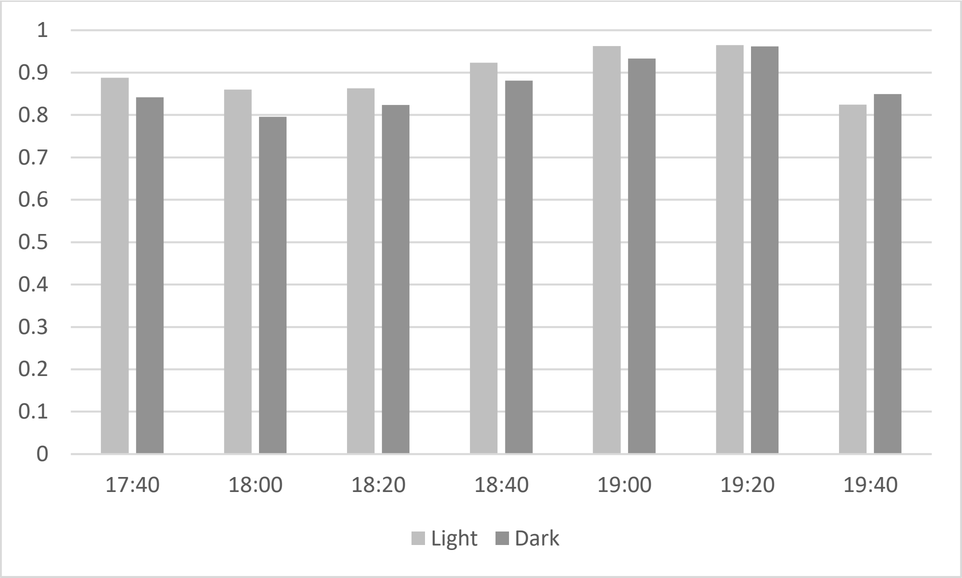


Figure 4 Percentage of vehicle stops involving Blacks out of all stops involving Blacks and Whites for periods of light and darkness. This makes use of the change of light conditions throughout the year. Light refers to hours till sunset and dark refers to hours after dusk. Hours of twilight are excluded. Based on 897 stops during 2018.

The question of racial biases in police stops is clearly complex and goes beyond the scope of this research, not to mention other possible biases. Just like the crime data discussed in chapter 4 cannot reflect the qualitative differences between crimes, stop and search data cannot tell anything about the qualitative differences between stops from simple things like the respect afforded by officers, the type of questioning, to the appropriateness of use of force. The police department has a long history of police brutality and misconduct, including police killings covered up, evidence destroyed, and paper trails changed. Up until the ‘90s the department’s officers were organised in cliques along racial lines. The Department of Justice’s investigation within the context of the consent decree found deep mistrust of police in the city’s minority communities. African-American residents reported discourtesy, harassment, and unwarranted stops, arrests, and use of force – particularly in the context of the ‘jump-out’ tactics described in section 4.3.1. Hispanics reported being regularly questioned on their immigration status. Yet, the consent decree forced the department to make major changes to strategy, training, policies, and accountability mechanisms – some of which are reflected in the policy quoted above. Many police officers had to leave the force and have been replaced by new recruits according to new hiring policies. The department has made progress as reported in regular reviews by the consent decree monitor. Yet, previous to this study, four years after entering the consent decree, 20% of stops still do not fully comply with the new policies. Infractions range from officers not properly introducing themselves, to the use of “boilerplate” language in the justification of stops, to unwarranted stops. In one briefing, as observed during this study, officers are ordered to “round up those shemales” referring offensively to the city’s transgender prostitutes – a group singled out in the Department of Justice’s investigation as one of the groups targeted by discriminatory police practice. In one interview a white officer is nostalgic about the past when he and his partner would put people up against the wall and search them. On the other hand, the DoJ’s investigations were based on officers being forthcoming about racial biases, and the senior officers in the armed robbery task force denounce the ‘jump-out’ strategy as a cause to mistrust in the communities. Without a much larger qualitative analysis of police stops, and as internal investigation officers were unavailable for interviews, it is impossible to speak to how much change has occurred and what the 20% of non-compliant stops are composed of. In the end, whether it is racism by the police, the policing of racist laws, or a structurally racist society, policing affects Blacks disproportionately. Given the history of racist policing in the city and the deviancy amplification of recorded infractions as discussed further below, it is perhaps fortunate that the databases discussed here were only created in the context of the consent decree.

Observations and ‘gut feelings’ described in the literature, such as someone being out of place or behaving strangely (or ‘gut feelings’ in the form of stereotypes), regularly form the initial motivation for a stop. As the policy quoted above stresses, this gut feeling still needs to be made explicit in the field interview card. When asked about the relationship between those observations and information from the database, a task force officer describes:

> “I mean, your observations and your gut feeling is going to come before you get to that anyway, before you get to running that name or anything like that, so your gut, I mean, for the most part you go with your gut” (Task Force 6, District A).

The aim of this section is to go beyond the human factors of discretion and add another factor to the list of influences on officers’ suspicion: databases. To get a better idea of how databases inform officers’ decision-making during different stages of these stops, the following analyses some situations from two ride-alongs with a task force officer. Although this is by no means a representative study of how officers build suspicion, the observations provide an insight into the ways in which the database comes into play during a traffic stop.

Table 1. Decision-making during patrol.

ID	Initial Observation	Direct Contact	Searching Databases	Action/Outcome	Analysis/Comment
	Vehicles				
1	• Coming from outside the city • One front light broken • Taking time to pull over	• Smell of (old) weed ○ Passengers explain that owner of the car and themselves smoke, but no weed in car ○ Officer does not believe them • "The passenger was very nervous". • As they seem cooperative, officer decides not to handcuff them but asks them to exit the car.	• Officer questions if car is brown as registered on database • Traffic attachments for the passenger: "Not worried about the traffic. There's something else going on". • Nothing to go on for the officer Keeps observing, maintains suspicion from passenger being nervous. Officer decides to search the car given perceived smell of cannabis	• Does not find anything in the car • "It's not against the law to be nervous. I, if a cop pulled me over, I mean, I might be nervous or anything like that if I've had a bad experience in the past. And I know, I've had a bad experience […]". • FIC	Initial suspicion translates into interpretation of data. I.e. officer is sceptical that the beige car would be classified as brown.
2	• Tinted windshield • Upon driving behind the car: Smell of Marihuana	• Driver is videotaping, seen as confrontational by officer • Father with son: "What makes it hard is 'cause he's there with his kid. I don't wanna put both of 'em in the back of the cop car […] or traumatize the kid". • Since driver is cooperative and with kid, officer asks them to exit car and puts him in handcuffs. Does not sit them in the back of the police car. • Officer searches the car and finds a small bag of Cannabis and a grinder, which he confiscates.	• "You can see he's had two misdemeanour arrests in the past, had a traffic arrest, no warrants, suspended driver's license". • "This is his old address. He's from the neighbourhood here […]". • No consequence	Confiscates Cannabis and grinder. "That's all it is. He gets a municipal summons and goes on his way". FIC, police record	Database search without extra suspicion since officer has already found something.
3	• No license plate	• Driver tells the officer that he had just gone to jail for driving without insurance and that the police had taken his license plate • Officer: "And I was like, 'they don't take you to jail for that man'."	• "So, he's been arrested for nine felonies, twelve misdemeanours, […] three traffic, […]. No warrants on file. […] failure to appear out of [different county], speeding". • Checks the passenger without result. • Clarifying date of arrest to search FIC database: "There you go, that's why he went to jail [, traffic arrest]. And the reason he didn't have a license plate, 'cause it was a fraudulent license plate. […] now I know this car isn't stolen […]".	Issues a warning as the passenger is on her way to work and they are unlikely to be able to afford the ticket. FIC	Use of database to figure out what had happened to the driver and if the car, since it had no license plate, was stolen.

4	• What first appears to be no license plate turns out to be a covered plate to avoid red light cameras • Illegal lane change	Retrieves passengers’ details.	“So, he doesn’t live that far. […] They might be heading to his house. She lives on [street name]. That is way over there. Give him a warning. They have a temp tag […]. […] it comes back to the same number. It’s still correct”.	Lets them go with a warning. FIC	Home address and license plate check satisfy officer that everything is ok.
5	• Expired license plate (hence, search of license plate gives no result)	Retrieves details.	• Runs the plate again with different year and finds the car. • Verifies address and insurance • Checking her name also gives no results.	“[…] she checks out. I’m just gonna give her just the warning of… ‘Cause I mean writing her a ticket for that is not…”. FIC	Database search confirms what officer saw at a distance.
6	• Tinted windshield and driver texting			No action as shift ends.	There were multiple situations like this.
7	• Illegal U-turn			“[…] that lady did that illegal U-turn? We would have felt it out, but I saw the kid […] in the back seat. So, I figured she probably just did that picking her kids up and being lazy. It wasn’t worth the stop”.	Time and paperwork for unlikely result.
8	Beat up car with ‘stuff’ in back window and on dashboard. “I like this car in front of us”. The officer searches the license plate. “This is an area known for drugs. People come over here and buy drugs […]”.		• “His address comes back to [a different city]”. • Search comes up with a warning that owner can carry a gun. • Some attachments from other areas. • “He doesn’t have any traffic attachments, like unpaid tickets or anything like that. So, he doesn’t really have a history of anything or hasn’t been on anyone’s radar too much […]”.	No action. “[…] you have to also remember […] if it’s worth it or not. Because then I could be tied up dealing with him and a call could come out or something else and I’ll be missing that or won’t be able to help somebody else […]”.	While the database confirms his suspicion that the car is from outside of [the city], the gun and lack of records make the stop seem not worth the effort.
9	“You see this car backed into a spot in the back of the [gas] station? So, let’s say someone was gonna rob the store, their getaway would be sitting like that […]. And look at it, he takes off when the police comes”.		Out of state license plate makes search impossible.	Drives a short bit behind the car and then turns around.	Cannot search for out-of-state license plates.
10	“[…] I got excited there for a second. I was like, is this a Mazda? And they had […] four, five kids in there?”.				Officers were looking for a dark Mazda that was

					involved in car burglaries committed by juveniles.
	People/Houses				
11	- Officer sees two persons in a house that is seemingly under renovation or abandoned; on coming closer one of them previously sitting outside quickly goes inside and shuts the door	- Officer gets out of the vehicle, knocks on the door, no one opens - Upon seeing what he believes to be a flashlight moving to the back of the house he walks around the house where he finds a screen pushed down. - He comes back to the front where the person who had closed the door comes out. - He handcuffs the person and questions him. - The person does not have any keys to the house and cannot prove their residence. - Gives only a nickname for the second person. - "[…] in his wallet, when I took his ID out, was […] a good amount of money in small bills, like 5s, 1s, 10s […], which is consistent of selling drugs".	- No outstanding warrants.	"I mean, we could sit here all night, go on to figure out who owns the residence, if he's supposed to be here, but then at the end of all that, all we would have is a trespassing. […] [The second person] probably had drugs on him, and 'he left and he stayed'- kind of thing". FIC	Knowledge of drug selling processes, suspicious behaviour (locking the door). Information will be preserved in FIC. Person has become of interest to the task force as they all talked about what happened.
	Suspicion				
12	"So, this is a good house right there. […] Did you see the people inside? […] they had a big security dog. We came by here once […], they were out there playing dice and they were smoking weed. So, we stopped the car and we went out to talk to them and they locked all the doors in that place".				Knowledge of history around places makes officer return to them.
13	"So these are like all abandoned [houses] and [drug dealers] know that they can hide, like that door is kicked open back there, they can hide stuff inside those abandoned houses and they can go get stuff out of it or they can hide drugs or guns in there, or hide out in there if they are trying to hide from the police or hide from somebody else, too."				Suspicion towards abandoned houses.
14	"So, this brick house right here, this two-storey one on the corner, supposed to be a lot of drugs".				Intelligence related to a place.
15	"[This area is] for our district, it's kind of like what you'd say the rough area. […] this is for us where all the trouble happens".				Does he patrol here because of this knowledge or to show me around?
16	"I know that guy in the pink shirt. So, it's like you look at him and see how he's bent over, and his shirt was tighter around his back? You can see he doesn't have any guns. That's what I was looking for. If you see like their shirt snag onto something or hand in a certain way, then I could articulate [it]".				Knowing a person and seeing if there is a reason for a stop.
17	"[…] a construction worker at night, isn't that weird? You see the guy with his lamp on his head? With that ladder right there? […] we'll see if something comes out, then I feel bad".				Person's behaviour out of the ordinary. But no action.
18	"So, you saw that guy, just peek out the street up there and then dip back down. In front of this white van right here, we're gonna make a turn. There's gonna be a guy standing wearing dark clothes. There you go, this is another area known for drugs and stuff like that. So, these guys out here, he saw us parked down there for a minute. He doesn't want us to see his face. [The person on the sidewalk is wearing a hoodie standing with their back towards the police car. The officer tries to make out their face in the mirror.] […] when he saw us moving, he went back 'round those on a phone. So, you never know, maybe telling somebody, 'Hey, the police are in the area'".				Suspected reason for a behaviour given the location.
19	"These people use like crack cocaine. That's an abandoned house that they sit inside and use drugs. […] So, the old people are probably the users. The young guy comes in and sells to the old people. […] So, I don't care about the old people. They are users, they have been using for years […]. The guy who is supplying them […], that's the bigger fish that you're looking for. You could come out all day every day and grab a homeless person or grab someone like that and find drugs on them and arrest them. It's not gonna fix the problem. You get the person they are getting the drugs from, that's the problem".				Strategy, knowledge, place

20	“So, the guy on the bike doesn't fit in. […] So, there are a bunch of old timers here and he leaves when the police come, right? […] he might be […] a middle-man, where he goes from house to corner to sell [drugs]. Or he might not be anything. He might just have been on the street corner when the police showed up. But that's why we have to investigate more, you know?”	Knowledge of drug selling processes, person that stands out

Table 1 gives an overview of all stops and moments of suspicion during the ride-alongs. The order of columns in the table reflects the order of a stop. Suspicion or a reason for a stop come from an initial observation, which is then followed by stopping the vehicle or person and a direct contact. In most cases, the officer starts searching the databases only after this contact. Based on observations and databases, the officer then decides how to proceed as listed in the "action/outcome" column. This last step is further discussed below in terms of the influence the database has on discretion. In the following examples from this table are denoted by their case numbers.

The task force stops that form the basis to this analysis are different from those that may be carried out by platoon officers, especially those tasked with traffic enforcement. Task force officers target an area and look for reasons to stop individuals or cars that are suspicious to them. They engage in a tactic of escalation: stops begin with an initial reason – such as a traffic infringement – and officers aim to discover more serious violations once the engagement begins. As a task force officer explains,

> "If let's say I was going through that car and I found a gun and the gun was stolen. Like that's how it builds up to doing more work. And it might stop gun violence or connect him to where that […] gun got stolen out of a car […]. […] Or that gun was used in a crime and they can match the ballistics […]" (Task Force 1, District B).

Detailed ethnographic engagement with officers makes it possible to differentiate five ideal typical stages during which database checks contribute to persons and traffic stops:

Before the stop occurs:

6) *Building suspicion*: During the phase of initial observation an officer may seek to substantiate their hunch by searching a vehicle registration while driving behind the

suspected car (case 8, although not successful) or to confirm their observation (case 5). This is impossible when the license plate is not searchable (out of state license plate in case 9), when it is a suspicious person, or when the on-board computer freezes (see below).

During the stop:

7) *Routine check*: An officer routinely checks for outstanding warrants or attachments, as well as car insurance and license. This search is unrelated to the reason for the stop. Officers also check for mismatches between the vehicle information in the database and the actual vehicle. Although likely a rare practice, one officer also mentions searching social media in some cases to inform their suspicion (see also section 6.6).
8) *Verification*: Searching the database further can confirm the stopped person's claims (e.g. validity of a temporary license plate, case 4) or help make sense of a person's story (case 3).

After the stop:

9) *Record suspicion*: When an officer does not have sufficient grounds for holding a person but maintains their suspicion, they can record this in the field interview card (case 11). This way the suspicion can carry over into future encounters with other officers.
10) *Record*: Even if the stop does not lead to a police report, officers are required to fill a field interview card (FIC) for every stop. This information can then be searched on subsequent stops and used in future investigations.

The following further interrogates these moments of suspicion.

Databases contribute ‘facts’ to the officers’ reasoning on suspicion. As such they can moderate suspicion: On the one hand, suspicion can be increased when the information given by the stopped individual mismatches with the database or the database indicates a criminal record. In case 1, for example, the officer increases his suspicion when, at first, he perceives a mismatch between the car’s colour and the colour that is registered on the database. The database provides a ground truth against which observations are compared. Furthermore, the results of a name search include the criminal history of a person. Multiple officers say that they would be more alert if the individual had a criminal history. For one platoon officer this was a question of both staying safe and being more inquisitive:

> “[…] it allows you to, you know, just keep a better eye on that person. Not let your guard down knowing that if there is something going on, you know, they've been arrested for all these felonies before and you know, last thing they want to do is […] go to prison and you might be the one that puts him in prison the rest of their life”(Platoon Officer, District A).

Knowledge of a person’s criminal history would not only influence officers’ scepticism, suspicion and precaution and thereby structure subsequent actions, it can also have implications on what actions officers would be allowed to take. As another platoon officer mentions, having a felony charge on the record would mean she would check for a concealed weapon which, given the sentence, the person would not be allowed to carry.

On the other hand, suspicion can be decreased when there is no record on the database, or the database matches with an observation or the story given by the stopped person. For example, in case 3 the driver claims to have gone to jail for driving without insurance. The officer is suspicious because this is impossible. The database helps clarify that the person had gone to jail for a different offense and the license plate had been confiscated because it had been fraudulent. The database helps the officer to reinterpret a suspicious excuse into a misunderstanding. Table 2 contains a summary of all the different factors that contributed to in- or decreases in suspicion during observed stops (with the addition of criminal history as mentioned in interviews). Given the small number of observed stops this is unlikely to be exhaustive. However, it demonstrates the multitude of other factors that influence suspicion that are also reflected in the literature, many of which are observations the officer makes.

	Reasons for Suspicion	Reasons to Lift Suspicion
Behaviour	Avoiding police contact or identification (leaving, shutting door, wearing hoodie)	Being cooperative
	Nervousness	
	Taking time to pull over	
	Talking among each other while officer out of earshot	
	Parked like a getaway car	
	Unlikely story or justification	
Context	Out of place/time: construction worker at night	
	Young person among old drug users	
Objects	Beat up car	

	Substantial amount of money in small denominations	
	Smell of Cannabis	
Place	Being/entering from out of town	
	Area known for drugs	
	“rough” area	
	Abandoned House	
Intelligence	Known house	
	Known person	
	Person or car of interest (BOLO)	
Database	[Criminal history]	
	(Perceived) mismatch (car colour)	
	Being from outside the area	Being from the area
		Lack of warrants and criminal history
		Explanation for story

Table 2. Factors contributing to suspicion formation during stops.

Once a stop is initiated, the database becomes influential. However, it only modulates already existing suspicion – however biased that may be. The database has little influence on who is stopped and who is not, even if it can provide the excuse for a stop. This is because at least the initial suspicion stems from the officer's observation or, in case of the platoon, a police contact that is already in progress. This may become different in the future when police equipped with license plate readers or facial recognition cameras may be prompted by technological systems to interfere[22]. As is apparent from Table 1, not every car the officer had reason to stop was actually stopped, yet an automated system would potentially highlight all those cars that an officer usually would not stop. This is unless the officer can actively deploy the reader to quickly check cars that invoke some sort of suspicion. In this case readers would extend the possible pretences under which cars could be stopped.

The database's influence is perhaps the greatest where it prompts immediate action or biases discretion. The first happens when the database alerts the officer to outstanding warrants. These function like a repository of orders that can be carried out by any officer once they become relevant. The database makes these orders available across time and to anyone with access to the database. Biasing discretion, on the other hand, is not as direct. Here, instead of limiting discretion, information on the database complicates the decision-making on what consequence a violation has. Does a broken taillight warrant a ticket or is a warning enough? These discretionary decisions are the focus of the second part of this section. While most of the analysis is based on stops, the database has a similar role when officers respond to calls-for-service.

[22] From the police officer's perspective, this is the major change that automated detection systems will bring about. They turn the officer more into a 'marionette' that enacts stored instructions, such as warrants and suspicions. Counterintuitively, rather than making everyone suspicious, they eradicate or at least partially supersede suspicion as motivating a stop. However, this does not imply that members of the public might not feel under suspicion, nonetheless.

At first glance, it seems rather obvious: if someone already has a record of traffic violations on the database, the officer is less likely to let them get away with a warning. As a platoon officer explains,

> "I say for example, I do a traffic stop out there. Traffic violation, I run your plate. If I come in contact with you, I'll run your name. Check you. See if you have warrants. Any traffic violations or history of driving and that may result in a ticket or not getting a ticket. That's one example like that" (Platoon Officer 7, District A).

However, the decision of handing out a warning versus a ticket is not as straightforward (and techno-deterministic) as the step from recorded warnings to ticket makes it seem. Rather officers are challenging the database and the law. As the following discussion between two officers with an age gap between them demonstrates, the decision when someone should receive a ticket is far from clear and officers make judgements on the fairness and expected effectiveness of the penalty seeking not to further disenfranchise those they encounter[23]:

> Young Officer: "I feel like it helps us because you might have a person who has a vehicle that they've failed to register, maybe don't have insurance, which we see pretty much all the time, it helps in the sense of because you could, this person could have been stopped three times in one month and got three verbal warnings for the same thing, but now they're still driving after they got three verbal warnings for the same thing, so now you're just neglecting to do what you have to do to be legal. So, at point then I think it's time to issue a ticket, you've been stopped three times this month already and got three verbal warnings, well now it's time to give you a [ticket]".

[23] Here, police officers act similarly to the many workers Dodson (2009) describes as the 'moral underground'.

> […]
>
> Older Officer: “See, I don’t think hardship has a time, when you’re on hard times and you’re in the city, you’re a female, you’ve got three kids and you’re working at Walmart, OK, your resources are going to always go to shelter, clothing, food and necessities and you’re going to let what you get away with and it’s a hard thing to do when you know you’re going to cost someone a month’s pay in fines because for the last six months XYZ officers have stopped you and […] told you this, but the problem is you just don’t have it. So, you’re making decisions on hardships and you create hardships on people that really do not deserve hardships. I know you shouldn’t be driving, I know that could be catastrophic too, if you don’t have insurance and you hit my family, I understand that”.
>
> The discussion continued a little longer. After the interview, the older officer takes me by the side to tell me that the younger officers were not able to make these decisions yet. They would be relying too much on the systems and would not see the bigger picture.

Motivated in the same way as the older officer above, the task force officer during the ride alongs decides not to write tickets where they would worsen the situation the stopped individuals are already in. For example, a woman that has no car seat for her kids:

> “None of the kids wore a seatbelt or had a car seat in that car. […] We could turn around, we could stop that car, we could write her a bunch of tickets, […]. It would cost her, but we don’t have car seats to give her. Well, she can’t afford it. So, what’s gonna happen if she can’t afford car seats for her kids? You think she’s gonna be able to afford to pay the ticket and then get car seats […]? […] I’ve been stupid poor before I had the

> job. And I know that getting a ticket […] sucks more on top of like already not having a car seat”.

Similarly, the officer decides not to give a ticket to a driver without a license plate who is driving his wife to work at Walmart (as the officer observes from her clothes):

> “I’m not gonna write him a ticket. I could have towed his vehicle. You know what I mean? But that means she’s not gonna go to work. They’re not gonna have a means of transportation. ‘Cause you can see, since January, February, March of 2017, he hasn’t gone to court for one traffic ticket, what do you think he’s gonna do if I tow his car and write him up? […] you’ve got to pick your battles” (Task Force 1, District B).

The database makes it harder not to act as it will give the history of how often other officers have done so before. However, as the older officer argues the concern that someone had been only given a warning for too many times may still be overridden by ethical considerations around the consequences a ticket may have for the individual. While someone may have been stopped before and accordingly have an entry in the database, this does not mean that their circumstances have changed. The database is not depriving the officers of discretion but rather shifting the basis on which discretion operates by supplying a history of police contact. Here, the field information cards designed to track stops and hold officers accountable develop an affordance that complicates discretion because of their function creep into stops.

Beyond the circumstances of the individual case, recorded warnings may be contributing to more tickets being issued. Linking to the previous discussion of targeted policing strategies versus territorial policing (see section 4.3), this could have consequences for acceptance of police and police legitimacy. Access to records and compulsory recording of all stops (as mandated by the consent decree) may push the balance ever so slightly from compassion to enforcement – thereby commencing a process of deviancy amplification (Young, 1977). Where records on the database are subject to biases in stop decisions, these biases are amplified through this mechanism. Future research is needed to establish the extent of this effect. It also raises the questions of which information officers should have access to during stops and for how long information regarding stops should be available on the systems.

Whereas the record of prior warnings on the database biases the consequence of an observed infraction from warning to ticket, the database's effect is perhaps even more problematic where it biases the assignment of guilt. Decisions from the past can influence decisions in the present through the database, potentially distracting from the individual circumstances of the incident. This is of particular importance to calls-for-service responses. One platoon officer describes how they would base their assessment of who would be at fault in a domestic incident on records of previous altercations:

> "[…] typically, in those situations, they've called before. You might not be familiar with what's going on between that couple, but we have like, the reports that we type, we can search people through that database as well. So, you can look at their history and just see that, alright this person normally is the aggressor and we've got a situation where it's like, this could go either way. They both have marks on them, you're not sure where the-- you know, who really started it, but then you look and you see you go four reports saying you know, the female just has been, you know, just the one that has always been, you know, starting the whatever physical engagement, then you can be like, well, based on the history, I'm not going to take you to jail today. It looks like you're-- we determined you're the aggressor so you're going to jail today" (Platoon Officer 7, District A).

Databases inform officers' decision making through the 'facts' they provide, whether these facts would influence suspicion, prescribe an action, or inform discretion. Yet, this important information is not always available: information is outdated or plain wrong and the technology stops working from time to time. These breakdowns are subject of the last part of this section. As one example, name checks can be performed in multiple systems and would often return differing results. The national database would often return search results that are nowhere near the searched for name. The department's own database, on the other hand, would return only exact matches leaving no room for variation in spelling. Sometimes this means that officers miss important information, as this platoon officer details:

> "Sometimes you'll run a person's driver's license number. You'll get, you know, A, B. You run somebody's full name, you get A, B and C. Like sometimes you'll miss a warrant. Sometimes you've already let this person go and then it's almost like everything catches up and it's like, Oh, crap. That person was wanted for like, you know, whatever it may be" (Platoon Officer 7, District A).

While these issues mean that checking records can be tedious for officers and they have to check carefully that the results actually relate to the person of interest, errors in the system for outstanding warrants have consequences on how the situation develops. Served warrants would sometimes still be in the system escalating the situation. According to a task force officer:

> "So, now you're looking at someone that's wanted, say for armed robbery, but he just got out, but they never took it out the system. So, I'm not going to be as cordial to you, so to say, if you're really a bad dude, you see." (Task Force 5, District A).

On the one hand, officers are clear that no system would ever be perfect, and a database would always contain errors:

> "I mean, there's so much going in and so much coming out, there's a large volume of stuff, of paperwork and entry, data entry that's just human error, people make mistakes" (Task Force 6, District A).

On the other hand, verifying warrants with the National Crime Information Center (NCIC) takes between 30 and 45 minutes – time that someone is held without a reason if the warrant turns out to have been served already. Many officers feel that this is an unnecessarily long process. A task force officer blames systemic problems for this issue:

> "Standing in the rain or, you know, being held for-- because we can't verify something. Now, I know there's always room for error and I understand that, but it's when something is consistent, there's a problem, there's a breakdown […]" (Task Force 5, District A).
>
> The verification of warrants is not the only system that malfunctions, the on-board computers themselves regularly break down cutting officers off from their databases and adding time to stops when officers wait for the system to reboot. Officers question the legality of holding persons for a prolonged amount of time in these circumstances. For example, one officer asks, "OK, and 20, 30 minutes pass, now have you illegally detained someone, just trying to ID them on reasonable suspicion?" (Task Force 5, District A).

Like the breakdowns of radio communication discussed in the previous section, officers are also concerned about how these system breakdowns affect their own safety. A slow system steals the officers' attention and, in the officers' view, gives the stopped person time to think about their actions. As one of the task force officer outlines:

> "It turns into a use of force situation because now they've gotten to know you, they get to see your personality, they get to read you a little bit, see if they think they can wiggle out of the problem, run, do whatever. So, that's a big concern for a lot of officers from what I hear and from what I know" (Task Force 5, District A).

And later:

> “But everything does equate to officer safety, no matter what because you take your eyes off of what you’re doing […] and you’re having all these problems, you’re getting frustrated then you lose sight of your peripheral, […] and it’s just they say 99.9% of the time nothing, zero, zero, but that one fraction of that one percent, it’s done, and I refuse to be that one fraction of that one percent” (Task Force 5, District A).

Yet, the system’s lag and fragility not only present an obstacle to the officers’ work, some also employ it towards their advantage. One sergeant instructs their platoon officers to place the suspect in the car while waiting for the NCIC to verify a warrant. This would give them the opportunity for a pat down mandated by department policy. However, this pat down would usually not be allowed as a person could only be padded down if the officer suspects a weapon or can articulate a danger to themselves. Accordingly, a task force officer in a different district feels that such a strategy would probably get challenged in court.

Officers find multiple workarounds to help themselves when the systems are down. Platoon officers in district A ask state troopers in the adjacent district for assistance as their systems run more reliably. Other officers would use their radio to gain the necessary information but sometimes with little success:

> “Sometimes it's bad, sometimes it will be down. I remember probably the longest I've seen this system down was almost a week. And it's really hard to do your job because you can still contact NCIC and try to get them to run names, like, over the radio for you but they're usually-- they're less than willing to like, try to assist you, I mean. So, to try to do that, you know, it's also coming with, you know, like a lot of push back, you know”? (Platoon officer, District A)

To prevent everything grinding to a halt when the system goes down, one task force officer uses their mobile phone to take a picture of a person’s charge history to ensure they have it for writing the Field Information Card (see below) afterwards. Again, frequent malfunctions create a fragmentation of technological practices.

5.3. Forms, reports, and tickets – (un)intended consequences of digitization

Every incident comes with several forms to fill afterwards. From tickets that are given out to drivers, to field information cards (FICs), to electronic police reports (EPRs), to trip sheets recording an officer's attendance at an incident. Some of these forms are digital while others are filled by hand. Electronic reporting carries many advantages: it allows for speedy exchange and signing off, mistakes can easily be corrected, information can be copied and pasted, and fields can be auto-filled. Electronic forms can also be more insisting than paper forms: when a field is not filled the computer can deny the form to be sent. Yet, this is where electronic forms develop their own affordances and unintended consequences. Like other technologies described in this chapter, electronic forms sometimes do not work or work poorly. In contrast to the mission creep of FICs used to inform suspicion as described in the previous section, in a double twist electronic forms may also be acting towards the goal of their design without acting as designed: Introduced as an accountability measure to monitor compliance with department policies, forms regulate police action possibly more because they are cumbersome than because superior officers read them. Furthermore, because they are an accountability measure, officers revert to paper forms – an even more cumbersome method – where they do not trust the electronic mechanism.

To begin with the advantages, electronic forms can be sent off immediately and if necessary be reviewed. This replaces intricate paper-based processes in multiple realms. One example are traffic tickets:

> “[…] it used to be, write the ticket, get the carbon copy, give them the copy and you would have to drop off a copy of the signed copy here. It would physically have to be brought down to traffic court. So now, it’s all on the computer so there’s no person picking up tickets every day to bring down to the traffic court and potentially losing tickets on the way to traffic court” (Platoon officer 7, district A).

While bringing traffic tickets to the court may be tedious, it does not directly impact on other tasks. But the same convenience applies to warrants, as this detective describes,

> “It used to be where you sit there, and you type out a warrant, and then you call the judge, and then you're going to drive to the judge's house, or the judge might be somewhere else, and you meet him somewhere else […]. Whereas now […], you can have an answer from the judge within five minutes” (Domestic Violence Detective).

Here, the digitalisation of warrants speeds up the process from filing a warrant to its execution which impacts the speed with which officers can act.

Not only can digital forms travel quicker, they are also fundamentally different from paper forms in offering reversibility. This means officers can, for example, amend police reports when their superior officer requests changes. More fundamentally, they can correct simple input errors. Multiple officers tell of the frustration of starting all over with each mistake made on paper. A female platoon officer remembers how she broke out into tears when she took down the wrong vehicle identification number twice in a row, having to restart the form every time. Furthermore, digital forms allow for duplication or ‘copy-paste’. A male platoon officer recounts having to fill paper reports for every single charge of 25 outstanding charges in an arrest, filling the same fields with the same information over and over. Last but not least, the computer can auto-populate fields such as date and time. This is why a platoon sergeant insists on her officers using the digital system. It would reduce the number of tickets rejected due to wrong dates and times.

Like many of the department's technologies, forms would not always work as intended. As in other cases, the system would break down from time to time making it inaccessible. In one roll call multiple officers complain that the software for issuing tickets has stopped working properly after an update. To fix the issue they need to take the car in for repairs. In another roll call officers are asked to do more traffic stops but the relevant fines are not on the system yet so they cannot issue the tickets as requested. While in theory offering reversibility, 'copy-paste', and auto-fill, those features do not always work as expected. For example, information does not transition between field-interview card and electronic police report database. Hence, officers still need to fill the same information multiple times. The same is true for reversibility. In a roll call briefing the sergeant tells the platoon officers not to do affidavits on the digital platform for tickets because they would not be able to redact them if they wanted to turn them into a summons[24].

Many of the reports officers must fill have been introduced in the wake of the department's consent decree to monitor officers' compliance with the law and department policies. Hence, officers must fill forms, for example, for every stop they carry out. While the forms are designed for monitoring, perhaps as unintended consequence, the amount of forms to fill and the cumbersome input provide a regulatory effect on the amount of stops officers would carry out. Paperwork makes it difficult to pursue a 'jump-out-work'-strategy as described in section 4.2.3. It takes simply too much effort to fill all the forms that ensue from a stop, which makes officers

[24] Affidavits are sworn statements by complainants or law enforcement officers filed with a municipal court concerning misdemeanour offenses covered by city ordinances. Summons are written notifications issued by officers for minor offenses in lieu of custodial arrest and require the recipient to appear in court.

consider whether a stop would be ‘worth it’ as one task force officer puts it. Future research could address the extent of this relation between time needed for paperwork and number of stops across different police departments.

As an example of the hassle that forms can provide, this is a task force officer struggling with the stubbornness of a field information card form insisting on certain fields to be filled after a traffic stop for an expired vehicle registration:

> “So, then it comes down 'did I pat 'em down'? No, I did not pat 'em down. Did they consent to search? No. [inaudible] form completed? No. Was the subject searched? No. Body cavity search. I didn't; we can't do a body... I'm not a doctor. […] if I click no on a pat down, no I didn't touch the person, I gave her a warning. So, nothing else should pop up. But every time. Evidence ceased? No. And I gave her a verbal warning. […] It goes back to the main pages for vehicle. I missed something. Oh. Required to exit the vehicle. So, some of this stuff, the consent decree came up with. And that's their way of thinking” (Task Force 1, District B).

“Their way of thinking” refers to the ‘higher-ups’ or the ‘civilians’ that developed the forms and are seen as being detached from the practical work. However, it is the form’s insistence that is making the process frustrating rather than the number of categories its authors have come up with. After all, many of the fields would be skipped if the form were on paper. However, it also demonstrates how the form’s authors can (or could) exert more power over its use by deploying the affordances of electronic forms.

Given their use for compliance monitoring and the associated disciplinary measures, filling and filing forms correctly is of importance to the officers. Accordingly, when systems break down and forms fail to be transmitted officers can lose trust in the system and revert to alternative reporting methods. This leads to a multitude of different approaches between officers. As an example, officers are using different ways of recording their work on so-called trip sheets. Trip sheets record every incident attended and every stop carried out. Officers report these via radio and their sergeant later compares this sheet against their own record. Some officers fill a pdf version on their computer, and others carry clip boards with a paper version. Curiously, no one seems to be using the online system for trip sheets. A story of an officer who was disciplined because of a trip sheet that had been lost during the upload process is making the rounds in the department. The head of analysis explains that the servers had unexpectedly not been able to deal with the load of the self-updating trip sheet system. However, the officer had been disciplined for multiple previous incidents. But given the resistance and technical difficulties the analyst had given up on it: "I'm not gonna die on a hill for that one. That battle is lost" (Head of Analysis). Where systems do not fulfil their purpose, individual workarounds come into existence, fragmenting practice.

5.4. Summary

This chapter explored the technologies routinely employed by officers on patrol or responding to calls-for-service. The theme of technology breakdowns forms the core of the section on dispatch and navigation, cuts across the other two sections, and indeed continues in the following chapter. Wherever technologies fail (or lack altogether as in the case of navigation), officers find their own workarounds leading to a fragmentation of technological practices and often a duplication of efforts across multiple technologies. Sometimes, as in the case of increased radio traffic, this leads to problems elsewhere. The issue is amplified where power structures increase the dependence on the technologies' functioning, such as the accountability mechanisms attached to trip sheets described in the previous section. Simultaneously, digitalization can be enabling where it makes officers' work easier as in the case of quick information transfer and reversibility afforded by digital forms. The affordances of technologies can also have (un)intended consequences as seen in the possible regulatory effect cumbersome forms have on officers' willingness to carry out stops.

Finally, the section on databases during stops and calls-for-service grappled with the role of databases in officers' formation of suspicion and discretionary decision-making. Databases do not take away freedoms of decision-making but rather complicate the process. During the formation of suspicion, they add information to the usual factors of stereotypes, known persons and locations, incongruency, and nonverbal cues (see Johnson and Morgan, 2013) and, at times, provide a more legitimate reason for a stop. They moderate suspicion depending on whether information on the database matches with officers' observations. Information from the database often structures subsequent action, for example when the database reveals previous convictions prompting a more cautious approach by the officer. In their discretionary decision-making on penalties officers regularly weigh the fairness and effectivity of measures taking the stopped individual's circumstances into account. The recorded outcomes of previous stops complicate this process and possibly push the scales slightly towards enforcement where many previous encounters are on the database. This may have consequences for the public's perception of police legitimacy. The influence of records is particularly problematic where they affect the assignment of guilt, that is someone becomes more likely to be guilty because they have been deemed so in the past. Here, databases lead to deviancy amplification and possibly create a feedback loop.

6. Investigations and surveillance – seeing more and differently

This chapter analyses the role of various technologies during investigations and for surveillance purposes. The technologies discussed here create, each in their own ways, new visibilities, whether those are visibilities of new information as in the case of social media revealing individuals connections and details on how they spend their lives, or the visibilities created by a network of surveillance cameras and license plate recognition cameras. These new visibilities fundamentally transform the spatio-temporal conditions under which investigations and targeted surveillance are possible. Many of these visibilities rely on the technologies' ability to serve as 'epistemic time machines' (Waterton, 2010) rendering the past available to the present. As such they are of huge importance as constant, proactive evidence gatherers for investigations. Most of the technologies described here are relatively successful in becoming 'points of obligatory passage' (Callon, 1986, 1999) for investigations. That is, to successfully build a case that stands in court, detectives have to go through these technologies. Consequentially, the technologies' affordances will sometimes impose their own constraints and timelines onto officers' work – 'ordering' investigations (Law, 1994).

As with the technologies described in the previous chapters, technological practice is fragmented. Sometimes this is because officers have to find their own workarounds to breakdowns, other times it is because officers find their own ways of best making use of what the technologies can offer and the practices vary between different units of the organisation. Finally, with new capabilities come new concerns for their abuse - especially where these new capabilities are as far-reaching as those described in some of the sections below. This chapter particularly discusses officers' justifications of the use of license plate readers and social media in the context of how they are employed.

The chapter discusses seven technologies: the first section complements the previous chapter by looking at how detectives employ databases to connect to the knowledge created by frontline officers filing reports on a daily basis and how they critically evaluate this information. The next section discusses network charts which are created for violent crimes based on the department's database. It contrasts the producer's aim of making information accessible with detectives’ misinterpretations of the networks. Third, introduced to ensure accountability, body-worn cameras take on the role of digital witness making officers’ experiences available to detectives and replacing witness statements. The fourth section scrutinises how video surveillance transforms conditions of spatiality, temporality, and visibility in investigations and targeted policing operations. License plate readers, addressed in the fifth section, provide a contrast between the successful automation of surveilling car movements with the organisational factors that prevent mounted readers from being employed. The sixth section interrogates the grey areas that come with the new extensive insights afforded by social media, as well as the practicalities of employing social media for police work. Finally, the section on phone data highlights the work and sometimes struggle that comes with the task of filtering through troves of data.

6.1. Databases for investigation – connecting knowledges to the present

What regularly forms the end of engagement for officers is the starting point for detectives. Not only will detectives receive the initial electronic police report from the responding officer and start their investigation there, adding supplemental reports in the process; reports also often become part of the investigation as detectives just as officers will search databases for clues. In this way, information recorded in the past for compliance can transform into a clue in a future, unrelated case. Databases connect local knowledges produced in different sections of the organisation and render them available for future use. Digitizing the reporting system means that they become searchable and filterable. With paper, as used before, the trail gets easily lost: “[…] you write it on a piece of paper, you put it in a box on the front desk. And it never got documented” (Homicide Detective 2). This section analyses the value of information held on databases to detectives and the trust they place in it. It also highlights some of the technological hiccups detectives experience when searching these databases.

The database of police reports connects detectives to the local knowledge that officers have who daily patrol their beats. This is especially valuable for major case detectives located at headquarters who would not have the regular direct engagement with a locality. For example, the information can help them make sense of tips they receive from locals:

> “[…] we'll get tips from people in the neighbourhood, ‘Oh, we heard that the person with the nickname of “this” is the one who's responsible for this murder’. And if you don't have someone in that district who knows all the nicknames of all these people, then you don't really have any way to look for that until now, with the field interview card database and things like that. […] if anyone ever pulled them over and they said, ‘My name's this, but my actual name is this.' […] If that officer records it, we can search by that field. So, we can make identifications or potential identifications from that as well, which is really helpful” (Homicide Detective 3).

Information is recorded on every stop. Even if the officer did not find anything but the initial infraction the car or person was stopped for, the recorded information can become essential for a future case. As a homicide detective describes,

> “[Field interview cards contain] information that we never would have had before. […] If you pulled over somebody it was like, OK, you wrote them a ticket and let it go. […] I had an investigation where it was a shooting that happened. It was a black Honda Accord. They said the person had a donut on the tyre. And I went back, so randomly I looked at FIC for a black Honda Accord, and there'd be like five or six of them that pulled up. And I'm going through them, and lo and behold, one of them had a donut tyre. It was pulled over two days later with the guys that wound up being my shooters. So, it's useful. If that technology wasn't around, I would've never even known about that” (Homicide Detective 2).

In contrast to searching databases to establish suspicion, as discussed in section 5.2 on police stops, detectives use the database to identify suspects for a crime that has already happened.

While the first use could be problematic where it is used to conceal illegitimate reasons for stops, the detective's use of databases appears less problematic. Differential access to databases, for example regarding records of minor offenses and inconsequential traffic stops, could address this difference in uses.

Department records are by far not the only data source detectives consult. They use a long list of tools to conduct background checks on individuals (registered names, addresses, and phone numbers), vehicles (license plate searches, collisions, repairs, towed vehicles), registered guns, alerts for credit cards, pawned items, and more. All these data points can add valuable clues to an investigation. However, detectives stress that records on their own would not suffice: "[…] you have to still do boots on the ground, because this database is just a starting point. We have to verify. Some of the information is old" (Homicide Detective 2). Generally, detectives see these data sources as aiding their investigation and supplementing 'good old detective work'.

While often useful to detectives, the problem of retrieving files that existed with paper forms is not completely solved with digitalization. When searching databases, detectives often come up against the same issues that platoon and task force officers face as described before. For example, detectives are also unable to search or filter BOLOS. To filter electronic police reports detectives in District B help themselves by copying them into Excel. Searches would not always retrieve the expected results. A detective in district B, for instance, tries to find reports mentioning a specific gun. He starts the search looking for "Taurus" and "9mm" yielding some results. Yet, "Taurus" and "9" does not return any reports. So, he tries multiple combinations of search terms to try and find a relevant report. Clearly, even in a digitized format, finding relevant information can present a challenge.

6.2. Network charts – mistranslation of meanings

Perhaps because information retrieval can pose a challenge as described in the previous section, the department has another way of consolidating and delivering information particular to investigations of serious crimes such as shootings and homicides, as well as conspiracy investigations. An analyst runs a script to extract names from electronic police reports and field interview cards. Based on co-occurrence these are then added to a network chart which is sent to the investigating detective. The chart is interactive and links to the underlying files. This chart comes together with a report written by the analyst who reads through all the files that the script uncovers. As further analysed below, the chart curiously makes little use of its network properties. Even more so, detectives read unwarranted meaning into the connections and, consequentially, warn of the legal consequences of including these charts in an investigation. The analyst's formal definition of a connection (being named together), collides with detectives' operational definition (conspiration). This highlights the multivalence of charts, their need for interpretation, and the potentials for mistranslation. Not adding information beyond what would be in the files, other detectives find the charts of little use.

The network graph includes all names that are mentioned in reports related to an individual under investigation. This could be mentions as co-offenders, co-victims, passengers of a stopped car or even witnesses mentioned on file. Graphs would rarely contain more than 15 individuals. The analyst would not go beyond first-degree connections (i.e., only direct contacts with the person of interest, not contacts of contacts) unless one connection was related to a criminal group. Network nodes would be colour coded depending on the type of report or field card they refer to – unless there are obvious groups such as family members or cliques.

Social networks, or in most cases here ego networks, are a way to visualize a matrix of connections between listed nodes. The pattern of connections distinguishes a network graph markedly from a list of individuals related to the central (ego) node. Yet, the analyst judges the network's structure uninformative: "The structure often does not say anything" (Analyst 1). She argues that the visualisations would be more about efficient display of information rather than analysis. The graph should only render all the relevant files more accessible to the detective. However, this underdetermination of the graph's connections leads to misunderstandings, which the armed robbery task force's lieutenant fears to impact legal proceedings. Not only the detectives, but also prosecutors and defence attorneys could misinterpret the connections as proven links. As he describes,

> "[In the network] the analyst basically laid out the fact that because a gun was connected on these crimes and it was found in possession of this guy, that this guy committed all these crimes, it's very dangerous to say that, you cannot say that, […]. […]. You cannot say that because Brian was arrested with a gun that was used in the murder of him, him and him, that he murdered him, him and him, right, because I could take a gun and murder somebody as easily as he can. […] the analysts have to be up to date on law enforcement enough to know that they can't say certain things, because in this country we have, you know, a precedent, it's called Brady material, anything that we gather in the course of an investigation is Brady material and the defence is entitled to all of it […]. […] when [the case] gets to court, it's all going away because if you don't turn that over, you lose the case. […]. But right here, there's this analyst that works in the police department said that the gun that Brian had killed him, him and him, and therefore it must have killed him, him and him, and, Christine, my client, Christine killed nobody" (Lieutenant, Armed Robbery Task Force).

Perhaps because of these complaints the analyst started sending the network charts with a disclaimer that it should only be used as a starting point for investigations. She also stresses that the graphs would not be court ready.

As the network charts mostly provide another way to access files detectives can search for by themselves, some detectives are sceptical about their usefulness. While speaking positively about them and hoping for the analyst to work within his unit, the armed robbery task force's lieutenant concedes, "When we get [the social network analysis], that does sometimes assist us, but to be honest with you a lot of times we know about it already because the analysis comes from cases that we've made […]" (Lieutenant, Armed Robbery Task Force). A detective in district A cannot recall any case where the tool would have been useful: "[…] in my day-to-day investigations, I find it not very useful. […] I haven't had one case that it was useful" (Detective 3, District A).

6.3. Body-worn cameras – from accountability tool to memory aid and evidence collector

Body worn cameras were introduced as a measure of accountability. However, the cameras are another example of mission creep. While possibly serving accountability, the main use officers and detectives describe is retrospective in reviewing footage as a memory aid or as evidence. This applies both to criminal cases, as well as investigations into complaints against officers. The ongoing collection of digital evidence transforms cases that otherwise hinge only on accounts of witnesses. This section provides an overview of these functions before pointing to the technological hiccups that exist with body worn cameras where the design tries to take control out of the officers' hands presumably to increase accountability. Because of their retrospective use, the cameras are grouped here with other technologies used in investigations.

On every call and for every interaction, officers turn on both their dashboard camera and the body-worn video camera. Afterwards, the footage is automatically uploaded to an online platform footage where officers then label the video with the incident's identification code. On the platform, senior officers can review the footage and the compliance team samples some videos for checks. This is where the cameras function as a tool for compliance. A district lieutenant makes clear that the cameras are about the officers' behaviour. His officers could not just go out "motherfuckin'" people anymore. Similarly, lead officers in the armed robbery task force credit body worn cameras as one of the factors in ending 'jump out work'. Despite this (optimistically, within the spirit of cultural change), the cameras seem to be generally well-received with officers displaying a 'nothing-to-hide' attitude as reflected in this statement:

> "So, I don't mind them. I didn't come on this job to violate people's rights or […] do any wrong to people. So, to me, you know, it's not a problem having […] every interaction I have recorded, you know?" (Platoon officer 7, district A).

This is not to say that officers would not miraculously 'loose' the camera, or it would 'fall off', or 'somehow' not record. However, to what degree officers would avoid scrutiny in these ways is beyond the scope of this study.

Perhaps one of the reasons for officers' acceptance of body worn cameras is that they discovered their use. After all, not only those who ensure accountability would be able to re-watch the footage but also the officers and detectives themselves. Rather than being a measure of accountability, officers refer to mainly two functions of body worn cameras: providing an evidential record and protecting them from complaints[25]. Officers and detectives refer to the evidentiary use of camera footage in three different situations: 1) searchable by officer, date, time,

[25] This finding is congruent with research by Koen and Willis (2019).

location, item number of the incident, and category, camera footage can make responding officers' experiences available to detectives. They provide more detailed information than a police report written after the incident could contain. For example, a homicide detective describes how the footage can sometimes provide crucial additional evidence for closing a case:

> "There was a murder that happened, and right when the officers arrived on the scene, a lady walked up to one of the officers. And the officer didn't realize how important this was, because she was kind of scrambling around, trying to secure the scene. Somebody basically told them, 'Hey, I saw the guys. I think they went to a warehouse around the corner, but I'm not sure.' That's all she said. And come to find out, there is a warehouse around the corner, and right after the murder, they drove right into it. And I was able to find that person's body camera because they didn't get any of the person's information or anything, and I was able to see who the person was. And, later on, I was able to find the person, because it was actually a neighbour, someone who stayed in the neighbourhood. So, I was kind of able to go around and kind of find that person. So, that's something that if that wasn't around, that information would've just been lost" (Homicide Detective 2).

2) More than clues for an investigation, the footage can become critical evidence. For example, in district B's CompStat meeting, officers discuss recorded footage as an option to pursue a case in which the victim does not want to press charges anymore. This use of video footage raises questions regarding the role of the victim where prosecution can continue against their will. On the other hand, it may prevent the victim from having to testify and relive a traumatic experience as further described in the context of social media data as evidence below (section 6.6). 3) The video can help officers recall more details from a situation they attended themselves. One officer, for example, uses the camera footage to write her reports and quote from the recordings rather than relying solely on her memory. Other officers say that it helps them to revisit a case before testifying in court, which would often be a long time after the incident.

Just as footage could serve as evidence in a criminal case, it can contribute to investigations into complaints against officers. Officers and detectives highlight the cameras' use in exonerating officers. The following statement by a platoon officer seems to represent this widely held view: "And also too it's for protection from frivolous complaints, because we get a lot of those" (Platoon Officer 7, District A). While judges would usually believe officers under oath, they would still expect video evidence. In both uses, the cameras serve as a form of 'objective' memory that serves as evidence supporting the officer's view. It would be interesting to know how the cameras came to be seen as tools for exoneration rather than investigation into compliance. Perhaps the evidentiary use and cases where officers were acquitted highlighted the cameras' practical use. This quote from a Homicide Detectives supports this perspective: "At first, I'm not going to lie, I did not like body cams. But now, I understand why they're useful" (Homicide Detective 2).

Although mostly working fine, even the cameras would have their technical problems. In the newest vehicles, all cameras turn on whenever the car's sensors notice police lights. The new feature of automated recording led to a recording deluge – an increase in non-event videos to be tediously labelled by officers:

> Officer 6: "[…] if their lights are activated, any officer that comes in within 20 feet of my vehicle with that camera will automatically activate it"
>
> Officer 5: "Even if they're not on scene".
>
> Officer 6: "You know, if you activate the lights, it automatically turns on all your cameras, in-car, our two body cameras, so sometimes you got to turn the lights on just for traffic control or to get through. Who's going to label an accidental video or non-event video—" (Task Force, District A).

Since labelling videos on the in-car computer was somewhat cumbersome, officers use – against policy – their phones.

6.4. Video surveillance – transforming spatio-temporality and visibility

This section addresses two separate uses of video footage: detectives use camera footage retrospectively in their investigations, while task force officers use live-CCTV feeds for pro-active operations. Cameras and the associated recording devices are limited in terms of where they are, what can be seen, whether they record anything at night, for how long they extend into the past, and the types of video formats they save their files in. All these limitations affect the spatio-temporality of their use and what is visible to who. This first part of this section reviews the politics that underly access to cameras determining the spatiality of camera availability. It analyses how the reliance on video footage for investigations shapes the timeline of investigations – including a failed attempt to streamline the discovery of cameras and an outlook into how artificial intelligence is about to speed up video review. The second part analyses the use of cameras in pro-active operations in which task force officers aim to record an offense on video. This strategy, mostly aimed at drug crimes, transforms fundamentally what would otherwise be a stop and search strategy targeted at known individuals or stereotypical suspects: officers wait for an offense to happen within range of the cameras, they see from a different perspective, they are seen differently, and they can instantly review footage allowing for new observations given a committed offense. Again, video changes conditions of spatio-temporality and visibility.

Video footage plays an important role in investigations and surveillance. Especially detectives investigating crimes that happen in public would rely on video footage to solve their cases, and, according to a task force officer in district A, juries would often expect video evidence as an effect of TV shows like CSI. The property crimes detective sergeant makes this reliance very clear: “We all know with property crimes, unless we got a camera, [often] we ain’t got fingerprints, it’s extremely difficult to solve” (Detective Sergeant, District A).

The department is correspondingly keen on expanding its capabilities. In addition to its own recent roll out of 300 cameras spread across the city, complete with blue lights on them, the department together with the city aims to increase the number of cameras by incentivising private installations as well as attempting to legislate for mandatory cameras on alcohol serving premises. Private owners are offered to link their cameras to the department’s network for a fee of $25 per camera. In exchange, they are promised increased security. For example, a burglary alarm could create an automatic alert at the ‘Real-Time Crime Center’ (RTCC) that provides terminals for officers to review and monitor video footage and is managed by Homeland Security. The city’s drafted ordinance to mandate cameras outside of alcohol serving premises promises to add about 1500 cameras to the network. However, some opposition has formed, as one commander explains: “[…] people don’t want to be seen with somebody else’s lady” (Commander, Major Case Narcotics). Not everyone wants to live in the vicinity of a police camera, even more so when it is equipped with a blinking blue light. Hence, it is not difficult to find newspaper reports of protests against the introduction of video cameras and complaints about the lack of civil engagement in the process. The placement of video cameras is clearly a political process. Given the influence camera placement has on whether and how crimes are possible to investigate, the political and economic factors in camera placement, and consequences for the community such as chilling effects[26] need further attention but are outside the scope of this research.

[26] See e.g. Murray and Fussey (2019).

The use of video footage sets conditions on the timelines of investigations. Acquisition, handling, and review of video force priorities on detectives and take up a considerable amount of time. As the detective sergeant above states, property crime detectives rely on video evidence. Accordingly, a detective in District A describes his job as going out to find video from the scene. He would spend considerable time driving to the locations of incidents, locating cameras, and soliciting the footage from owners. The immediate collection of video footage would be important, as detectives in District B explain, because many cameras would quickly overwrite footage. Here, the technology forces prioritisation.

Because detectives are often unsuccessful in finding cameras, the department tried to streamline the process through an online map of cameras. This map includes all cameras owned by the police and private cameras integrated in the network. However, as a detective in district A explains, not only does this not include all cameras, the direction cameras are facing would be unclear form the map so that detectives would have to check the location anyway. This renders the tool useless to detectives.

Once a camera is located, the handling of the video itself can pose challenges taking time away from the investigation. Detectives encounter camera owners that do not know the passwords to their cameras, video codecs are difficult to obtain and playback can be limited to real-time view, the video quality itself could turn out to be inadequate, and detectives have trouble sharing video files due to size restrictions in emails. To bypass this last issue detectives in District B set up a Google Drive account to which camera owners could upload the video. Here, the technical difficulties lead to a workaround that could be problematic in terms of data safety.

Finally, reviewing the footage, especially when it is impossible to speed up the playback, takes significant time. While on one evening detectives in district B kill this time eating chicken wings in front of their screens, a new technology that is so far only available in the Real-Time Crime Center aims to shorten the process significantly. BriefCam Analytics uses object recognition technology to speed up hour long video footage into minute long sequences by overlaying multiple events. That is, all the parts of the footage in which nothing happens are cut and the remaining ones are overlaid. Cars that drove past in a 10-minute space now follow each other within the same frame. Because it is based on object recognition, it can also filter footage by object. It produces, for example, a short video sequence or a list of photos of all men walking through the frame or of all red cars driving in a certain direction across a junction. The resulting video presents a fascinating view: “It’s so cool […]. I’m looking for a guy in a red shirt between this time and this time and all you just see is people in red shirts. Like, it’s crazy” (Major Case Narcotics Detective). Yet, perhaps this kind of software is also creating a new kind of insecurity: what if the software misses something? How does the software compare with detectives who may easily miss a crucial moment when watching sped up video?

The use of video footage in investigations requires time and prioritisation of tasks. It is limited to locations where cameras are installed but allows a view into the past and is therefore crucial for many investigations. Another area where video is transforming police work is pro-active policing. Video has played a role in the department in covert surveillance for some time. Now, this is extended by using live monitoring of the recently installed cameras’ video feeds. At the forefront of this, task force officers in District A check locations they know to be likely locations for drug deals. This approach is markedly different from stop-and-search strategies described above in section 5.2. Instead of looking for a minor infraction to uncover a different offense, officers seek to record the offense itself, that is a drug transaction. Consequentially dealers could be charged for the transaction rather than just simple possession of drugs and the associated higher sentence could help in reaching a plea deal. However, while this strategy may seem less invasive than widespread stop and search, it not only comes with the invasion of cameras installed all over the city, it is also concentrated on those areas predetermined by the location of cameras. Furthermore, it can lead to questions of legality where officers misjudge an observation as probable cause.

Beyond these consequences, the use of video cameras in pro-active policing has direct impacts on the police actions themselves. The cameras change conditions of spatiality (limited to where cameras are), visibility (for and of the officer), and temporality (longer duration of observations, delayed sense-making). Based on an observation of an operation of District A's task force in the RTCC, the following compares these changes to a patrol strategy and to physical covert surveillance (for example, sitting in an unmarked car).

1) Spatiality: With the cameras being in fixed locations, the camera strategy is obviously fixed to the cameras' locations. This means that officers are waiting for something to happen in a space. This is similar to covert surveillance where officers may pick a spot to watch, just that the choice of locations is more limited for cameras. This tempo-spatiality is very different from patrols where officers' observations cannot acquire the same duration, but they can encounter suspicious behaviour anywhere. The effect of duration is analysed further below. All three strategies contain a bias towards drug transactions in public spaces. With the camera strategy this bias is focussed on areas where cameras have been installed (Norris and Armstrong, 1999).
2) Visibility of the officer: On patrol, an officer looks for suspicious behaviour while driving past a group of people. This suspicious behaviour would often be a reaction to the officer's presence. This visibility effect does not exist in the same way for the officer in the RTCC (or for covert surveillance). However, in the observed operation the officers' initial strategy is to combine a visible, police-owned camera and a less

visible private camera at a construction site. In past instances the dealers had moved around the corner and out of sight of the police camera but still being in view of the second camera. Similar to covert operations, officers are keen not to be detected[27]. Hence, they try to arrest dealers and users at a distance of the cameras – a precaution one of the officers thinks may not be necessary: "It's a big camera, with lights, with flashing lights, and they just continue to do it" (Task Force 7, District A).

3) Visibility for the officer: The camera influences how the officer perceives the situation. The camera is tiltable, panable and zoomable. However, all motions are delayed, resulting in step by step movements. Sometimes the officer zooms in too far, losing the person they are following. In the observed operation, the camera's fixed position means that the officer is unable to identify a person sitting behind a pole until the person finally moves.

4) Yet, while limiting the view in terms of positioning, the camera also enhances the view in terms of how far it can see. The exchange the officer observes, for instance, happens at a distance at which she would have been unable to see details in person. Furthermore, seeing from above allows the officer to spot what suspected buyers have in their hand when they would check themselves, palm upwards, after a purchase. The high vantage point also puts the officer at the RTCC in a position to direct the officers 'on the ground' to stop individuals moving away from the suspected drug deal – in the observed case describing the clothing and naming the street they turn into. The camera operator can coordinate multiple police officers stopping multiple suspects. All these aspects are unique to operations using installed surveillance cameras.

[27] See also Fussey and Sandhu (Fussey and Sandhu, 2020) and Loftus et al. (2016).

5) Temporality: The camera does not change who is deemed suspicious: persons known to the officer as drug dealers or users, and those who ‘look like’ drug users, as well as those ‘hanging’ at a corner. The officer would follow these with the camera, looking for transactions. However, the observation’s duration would allow for a transformation from initially unsuspicious to suspicious. The person next to a car with a tool filled trailer turns from what would have appeared to any passing police patrol as someone working in the area into a drug dealer as soon as he is approached by a drug user known to the officer. “We were just thinking he is a working man cutting the grass” (Task Force 7, District A). Furthermore, known persons which often could not be stopped for lack of reasonable suspicion could now be observed until they give cause for suspicion.
6) While this aspect of duration is available to officers conducting covert surveillance as well, officers in the RTCC can also immediately review the recorded video feed further changing the operation’s temporality. The officer can skip to any moment in the footage previously recorded and back to the live feed, without affecting the recording. With the recording being instantly available, it would be easier to argue a probable cause for search. Usually, during a persons stop this would be impossible and they could only perform a pat down during which it would be difficult to locate drugs. The recording also allows for delayed sense-making: With the stopped person having turned from a local worker into a drug dealer, the officer goes back in the footage and tries to identify where they had hidden their drugs – going back further than the moment of her initial suspicion. She is also able to slow the footage to identify fast hand movements. She then directs the other officers to check any places or pockets she identifies as possible stashes. As a task force officer in District B explains, this connection between the drug dealer and their stash is almost impossible to make

> otherwise: “[…] they know that if they don’t have it on ‘em, let’s say they have it in a bush next to ‘em or in the mailbox or something not on their person, it’d be hard to prove in court possession of that” (Task Force 1, District B).

6.5. License plate readers -successes and frictions in the deployment of automated surveillance

License plate readers are cameras that, as their name indicates, can read the license plates of cars. All plates are recorded in a database with a picture and a timestamp. If a database matches with a list of “hot” plates of sought for cars, an alert is created and sent out via email. The department employs two types of readers: stationary readers that are installed at strategically chosen intersections and record all the plates passing by, and mobile readers mounted to patrol cars used primarily to recover stolen cars. Stationary readers focus on movement while mounted readers focus on detection. Especially the stationary readers are often central to investigations. They provide a record of the past that is available at a distance. This section first examines the considerations that went into the placement and therefore the spatiality of fixed license plate readers. It then considers the use of these fixed readers in detective and task force investigations before addressing the mounted readers’ incompatibility with organisational requirements. As with other technologies presented here, license plate readers would not always be reliable. Officers need to be vigilant for regular false reads. Finally, license plate readers record everyone’s movements and, hence, pose a threat to people’s privacy. Consequentially, officers feel a need to justify their use highlighting their usefulness in targeted employment for serious crimes. Presently, the system’s extent is mostly limited by technical and budgetary constraints. Officers only need to have completed training and record a justification for every search.

The locations of license plate readers split the city into multiple zones for which the readers register every incoming vehicle on major in-routes. The positioning reflects a combination of technically mediated knowledge in the form of hotspot maps for shootings and situated knowledge of major routes in the city. The commander who set up the system still has two prints of yearly heatmaps of shootings provided by a “GIS guy” from Homeland Security hanging on the wall. He explains that the pattern of shootings was helpful in dividing the city because it would be relatively stable over time. Similar to the maps described in section 4.2.3, these maps provide an important interface between the statistical knowledge and the commander’s situated knowledge of the city. On their basis, he identified travel routes, intersections and choke points demarking hotspot areas. He had put stickers all over the map denoting the location of cameras and the direction they were pointing in. As he puts it, “[The person setting up the system] gotta be somebody who has a feeling for the geography. […] I grew up in this city, [so I know] you gotta take this street to get out” (Commander, Major Case Narcotics). Additionally, some of the readers are placed to be in the same location as existing surveillance cameras allowing for the reader to take a picture of the back of the car while the camera covers the front – and with it potentially the driver.

The process of placing license plate readers (and sensors more generally) is imbued with contingency. A different commander might have chosen a different crime, seen different choke points or based the placement on traffic flows instead of crime. Was it just that shootings were stable or is there an implicit assumption that shooters travel between areas, that they signify area-based conflict? What other implicit assumptions flow into the placement of sensors? And perhaps most importantly what consequences does one chosen placement have compared to another? Which crimes become easier to investigate, who is more likely to become a suspect?

These questions go beyond the scope of this study but, especially given the increased dissemination of sensing technologies, will need to be addressed in future research.

Investigations focus on any movements between the zones created in this manner. In its simplest form this could mean checking a car's presence in an area during a time of interest in the past. For example, this could be checking the alibi of a suspect in a homicide investigation. Here, the license plate readers operate as a record of past movements – a record that otherwise would not be available or relies on witness statements. This record can also be searched to reveal a pattern. The Armed Robbery Task Force, for instance, uses the readers to draw connections between crimes. As the sergeant describes,

> "We get a suspect that's using a red Honda and we know that car is stolen and we have four armed robberies with that and then all of a sudden we hit another armed robbery, we may look at their cameras and see if a plate tripped anywhere around there and if it does, it gives you another say, 'Hey, he's probably the suspect in that one, too'" (Sergeant, Armed Robbery Task Force).

Beyond checking if a suspect's car was in the vicinity of other crimes, the officers from the Armed Robbery Task Force also use the records from license plate readers to track the movement of stolen cars in the city, identifying areas of interest for covert surveillance.

All the above uses start out with a number plate that officers have a (legitimate) interest in – a suspect's car or stolen cars. In theory, the technology can also work the other way around by cross-checking all cars in the vicinity of likely related incidents. In this manner, the database created from license plate reads can create a list of possible suspects that were present in the vicinity of multiple incidents. This kind of filtering is a new capability. However, none of the interviewees describes such a use; perhaps because the system does not include enough cameras yet to demarcate areas small enough for any meaningful filtering, or because the department's policy requires searches to be justified and based on specific license plates.

Finally, officers can set up alerts for 'hot plates'. This is used when investigations are interested in present movements of a person. For example, detectives in Major Narcotics have set up alerts for cars related to drug trafficking to notify them when they enter the city. Similarly, detectives searching for a 'fugitive' would add license plates of persons that might be in contact with a wanted person. More generally, these alerts are of use where investigations are interested in the movement of a car and a related person. What would have in the past required extensive physical surveillance is now possible at a distance and employing little resources.

'Hot plates' are also central to the use of mounted readers. Rather than alerting an officer to a car's movement, officers use the readers to detect cars of interest. These could be, for example, stolen cars. Alerts generated through this system can be interpreted as pre-recorded prompts for officer action. The process by which an officer becomes suspicious of a car before checking the plate in a database as described in section 5.2 is skipped. In theory, this could mean that patrol officers focus their efforts on vehicles of interest rather than looking for suspicious behaviour thereby eliminating some of the biases that come with the latter. Discovering a stolen car could also entail an investigation into the driver by stopping the car or, in case of a parked car, waiting for the driver to return. However, in practice, the way readers are deployed prevents these uses of the mounted license plate readers. Each district has one police car equipped with a reader. When this car breaks down the reader cannot be used, which happens frequently as this officer states,

> "The one car we had in the district with the license plate reader, it was down for a while. That's an issue we have. Our cars are always going down. And

> this one, specifically has had a lot of issues. So, you know, we haven't been able to utilise it as much" (Platoon Officer 7, District A).

Furthermore, the readers are mounted on platoon officers' cars who have little time to patrol outside of answering calls for service. And if despite these issues platoon officers get to employ the readers, they have either difficulty stopping the car:

> "[…] with our policy, I mean, if it's actually moving, chances are if you try to pull it over, you're very limited of what you could do except watch it drive away" (Platoon Officer 7, District A)[28].

Or, if the car is parked, they do not have the time to investigate further and just repossess the car:

> "You really don't have time to sit there and sit on a car. You know, just recover and go on to the next call" (Platoon Officer 7, District A).

Consequentially, the readers get little use. Asked by the commander if they made use of the readers, the detective sergeant for property crimes in District A replies with an evasive 'sometimes'. In district B the platoon sergeant and lieutenant do not even know who uses the car equipped with the mounted reader. They contact the officer they think should have the car. But the officer informs them that he stopped using it months ago as he does not know how to operate it.

Not only does the readers' placement on platoon cars collide with other uses of those cars, it also interferes with other investigative uses. For example, members of the Armed Robbery Task Force are unable to employ the districts' cars carrying readers:

[28] The department's no-chase policy introduced by the consent decree is one of the changes least welcomed by officers.

> “I’ve requested on big cases, big investigations, where we can’t quite find the vehicle although we’re hearing or receiving information a vehicle goes certain places, to have them deploy those cars in a certain area to help us, but we’ve run into a roadblock because each individual District, we have eight of them here, each District has one car and they are basically dispatched out on a daily basis, based on the command of that District […]” (Sergeant, Armed Robbery Task Force).

Mounted license plate readers conflict with the call-for-service function of policing that is firmly attached to the same cars. This, in some cases literal, misplacement results in low utilization of the readers[29].

License plate readers do not always work reliably. Officers and detectives stress the need for verifying that the plate read by the reader is correct. For example,

> “[…] you may get a license plate where somebody’s one number off or the numbers are inverted. And then you look it up, and you say, I’m looking for a red Cadillac, and the license plate might come back to a blue Chevy. So, you have to verify” (Homicide Detective 2).

Reads could be off by one number or the numbers could be inverted. Sometimes it is the correct number but from a different state. And sometimes the reader would read something else than a license plate. White cooler boxes branded “Yeti” and carried on flatbed trucks, as a commander explains, would reflect the light in a similar fashion to license plates resulting in a lot of “Yeti” entries on the database. Verification is not much of an issue for detectives, whereas officers may have to react quickly. By policy they must verify the output. However, in another

[29] This issue is not unique to the studied police department (Lum et al., 2019). Koper and Lum (2019) argue, “Our sense is that many agencies deploy their LPRs with no particular strategy. LPR technology is often treated as a resource that has to be divided equally among administrative units (e.g., districts or divisions) within the agency, rather than allocated based on needs assessment. Assignment of LPRs to officers might similarly be made with no particular strategy nor any guidance for the officers”(Koper and Lum, 2019: 529).

department a misreads has led to someone being wrongfully stopped and held at gunpoint (Farivar, 2014).

Not only can license plate readers produce potentially dangerous misreads, they are also a threat to privacy as they record everyone's license plates. With this, patterns of behaviour, such as doctors or lawyers visited, or an affair, can become visible (see ACLU, 2013; Merola and Lum, 2012). Aware of the criticisms around the technology officers defend its use as targeted and based on existing suspicion, as well as highlighting its usefulness for investigations. For example, this is the Sergeant of the Armed Robbery Task Force:

> "And I know there's a concern that police are taking just everybody's stuff and they're fishing it but it's not like that, it's used for us, it's used in specific crimes with specific perpetrators or specific suspects to help direct us to identify and catch them and help us collect the evidence" (Sergeant, Armed Robbery Task Force).

Similarly, the commander who planned the readers' placement stresses the "historical" use as evidence in cases with existing suspicion. He further points to their main use in investigations of violent crimes. According to him, the technology had proved so useful that the department had stopped tracking the number of murders, shootings, car thefts, and other crimes solved with the help of license plate readers because they became too many to track. Finally, the commander argues that there is no reasonable expectation of privacy for license plates: "[…] everything that you can see with your naked eye, […] we're not invading your privacy" (Commander, Major Case Narcotics).

However, despite this apparent focus on certain crime types, the department's policy does not put any limits on the use of the readers apart from them being used for public safety purposes. Generally, the system's limitations are mostly due to the way it is implemented: a) mounted readers' placement on platoon cars entails limited use as described above, b) budgetary limitations determines the limited number of available cameras, and c) the system's storage capacity limits data retention to six months. The commander illustrates this limit with an example: In one location, three cameras cover six lanes coming down from the interstate highway. "You couldn't even imagine. [There are] 20,000 cars in an hour [that] drop off the interstate" (Commander, Major Case Narcotics).

6.6. Social media – fast-paced insights and new grey areas

This section first analyses officers' use of social media for intelligence and evidence gathering looking at publicly visible information, creating fake accounts, and asking third parties to provide access, as well as applying for warrants. It details the importance this type of information has in establishing profiles, networks, and locations of suspects as well as evidence gathering on illicit activities carried out on social media. It then addresses the practicalities in terms of time pressures and skills needed before discussing officers' justifications for the easy, at times problematic, access to information on social media.

There are two main ways in which task force officers and detectives employ social media: a) they use social media to gather intelligence about individuals' activities, their personal networks, and the locations they are in. Some of this information is collected from public profiles, some by asking third persons for access, and some through fake accounts. b) They use data obtained from social media companies through warrants as evidence. This happens often after gathering intelligence or when officers cannot access information otherwise. Note that while practically these two approaches go hand in hand, logically the first circumvents the second – and along with it all the safeguards of applying for a warrant. This issue is addressed further below.

The most prominent example for intelligence gathering through social media is the strategy of the Armed Robbery Task Force. It is central to their targeted strategy (see also section 4.3.2). As the lieutenant describes, they use social media to identify suspects' locations:

> "[…] the robbers would get on social media too and […] they're talking from a location, so we're able to look at the background and say, […] '[…] I know exactly where that house is'. So, we go out there, we find the house. So, now we know an area where they're hanging […]" (Lieutenant, Armed Robbery Task Force).

These locations can then be physically surveilled.

Another officer also outlines social media's use in exploring a suspect's personal network and thereby widening the pool of suspects:

> "[…] a lot of guys go by nicknames, so it's kind of easy for us to find. The names that they go by in the street is their Instagram nickname, so we just type that in and then, sure enough, they'll pop up and then we'll kind of have an idea of who he hangs out with […]. So, you're pretty much into the gang now without really working that hard […]" (Officer 1, Armed Robbery Task Force).

Information that would have needed intensive physical surveillance efforts in the past is now available to officers within a few clicks – without any hurdles. On the one hand it enables a strategy that avoids the constant harassment of citizens with stop and search, on the other, persons become suspects by association potentially exposing them to more severe interferences with their lives.

This issue is exacerbated where officers use social media for ad-hoc intelligence to inform their suspicion during stops. While likely not widespread practice, such a use is laid out by a task force officer,

> “I might have a suspicion so let’s say I look you up on social media and […] then one of the guys in the picture might be somebody on this wall [of BOLOs]. Someone DIU [District Investigatory Unit, i.e. district detectives] are looking for. So, now I know that y’all are affiliated or y’all are a rap clique. And so, then I start looking up your rap videos. I start looking up on YouTube and now I see y’all have guns and drugs in this video. […] So, now we start putting together a picture of who these players are and also what kind of activity they might be into” (Task Force 3, District A).

Here, the stop becomes a ‘fishing expedition’ where whatever (biased) observation leads to a search for actionable information. This highlights the need for regulation of police access to social media.

Not all intelligence gathering on social media brings up only networks, locations, and some idea of the ‘character’ of those targeted, it could also uncover crimes that are committed *via* social media. This is where intelligence gathering bleeds into the evidentiary use of social media. Whether naked pictures posted without consent, or chats of drug and gun deals, some of the examples given by detectives and task force officers would not be solvable without this. An example of such an operation is given by the Armed Robbery Task Force’s lieutenant:

> “[…] when they get cars, when they get guns, they take those and eventually they sell them off to guys who go out and commit robberies or shootings or murders and they do that on social media. You know, we had one kid, he was sixteen years old, we had him on seventeen gun transactions on Instagram […]. […] he actually went on Instagram one day, we found the location of where he was, […]. […] it was all done on social media and that’s the only reason we were able to make that one particular case, that particular day […]” (Lieutenant, Armed Robbery Task Force).

In the case of child sexual abuse, evidence collected from social media helps detecting and evidencing crime. As a child abuse detective explains,

> "[…] we get up on social media, when we want to […] corroborate different information in child abuse cases, because again children don't report. And then sometimes we'll try to look, did the child tell anybody? And sometimes we'll get that information from their social media pages" (Child Sexual Abuse Detective).

Both examples underline the importance social media can have for investigations as a space where crimes are committed and recorded. Whereas the gun sale may have been investigated with a lead starting in the physical world followed up with a warrant for data from social media, the child abuse case raises the question of if and how detectives should seek to detect crimes on social media where perhaps there is no prior information that could be used for a warrant. The police department has decided not to undertake any blanket monitoring of social media as long as there is no caselaw (see further below).

Part of why social media proves so useful for officers is because of criminals posting information relating to their crimes – a fact that multiple interviewees find surprising. Their explanations include lack of awareness, bragging, and, perhaps most convincingly, a new form of street credibility. The word-of-mouth street credibility of the 90s, claims the Armed Robbery Task Force's lieutenant, is todays' visibility on social media. His sergeant illustrates,

> "He is constantly on Instagram and every time he's on Instagram, he has a mini AK47 with him and it's on Instagram. Now, unfortunately, he's not a convicted felon, but we also know he's a mid-level heroin dealer and he is constantly posting on here, 'You all come and get me if you want but I know you're scared.' And in this section of the city […] nobody will go near him or mess with him and he's a suspect in multiple homicides, but no one wants to come forward and testify against him because they're terrified of him. And, like he said, he's all over social media and anybody can see him, and they know that he's got an AK47 with him at all times" (Sergeant, Armed Robbery Task Force).

Again, does this use of visibility on behalf of criminals justify police searching for these cases given their effect on feelings of security in the wider community? Or should the investigation begin somewhere else giving access to social media through a warrant only when other evidence is available? The position of police officers on the conditions of access is analysed further below.

Gathering information from social media influences the timing of intelligence gathering and investigations. In intelligence gathering, staying up to date presents a challenge that requires time and commitment from the officers that is tendentially only available to those in special units or major case detectives. As the Armed Robbery Task Force's lieutenant describes,

> "[…] you've got to be on social media every day, because the one day you're not up on the social media is the day they decide to go shoot somebody and they're telling you right there on social media, you know. So, there's a lot of… you really have to buy into it completely and it's a lifestyle" (Lieutenant, Armed Robbery Task Force).

Not only does monitoring social media require constant attention, once an officer finds something and wants to preserve it as evidence, they are presented with a short time window to complete a warrant. Particularly Snapchat is mentioned multiple times.

> "I think Snapchat is probably the most difficult one, because everything erases right after one day. So, once you find a Snapchat, you have to hurry up, get a perseverating letter, then send it, get the warrant, and try to get it within a small timeframe. So, I think that's probably the hardest one. […] With Snapchat, it's gone. It's just crazy" (Homicide Detective 2).

Even if it is not the social media company deleting data by default, the user could destroy evidence if officers are not fast enough. As a detective specialised in investigating sex crimes explains,

> "Instagram, Facebook, Twitter. If they delete these things, we can't see what the content is after the fact. They'll have a record for us to say, 'At this time, something was posted, and then at this time it was deleted'. But they can't give us what that actual content was after it's been deleted" (Sex Crimes Detective).

Apart from highlighting the prioritisation necessary to obtain warrants, the resentment displayed by both detectives above at evidence having been deleted reveals an underlying expectation of accessibility of records. A similar sentiment is present when detectives speak about social media companies returning warrants. For example, this detective complains,

> "They return warrants if there's a tiny mistake like a missing period in the IP address and you have to start the whole process again" (Detective Sergeant, District A).

He continues pointing to the power differential between detectives and those big companies,

> "What am I going to do? They're bigger than us, more powerful than the government and have an army of attorneys" (Detective Sergeant, District A).

The option to delete, standard deletion cycles, and social media companies' scrutiny of warrants seem to provide more hurdles to data access than any oversight mechanisms within the justice system. Because of these hurdles, officers need to be quick in applying for a warrant but then may need to wait for a comparatively long time to receive the evidence – which coincidentally creates another incentive to access social media through other channels.

The extent to which social media is used in intelligence gathering and investigations varies between units, and dissimilarly from many of the other technologies described previously, by age. This leads to knowledge gaps within the organisation and consequentially divergent use of social media across the organisation. Younger officers seem to be more comfortable with using social media. For example, a task force sergeant highlights this shift from physical surveillance to social media surveillance by age group,

> "Young officers will jump on social media and dig around, while my bread and butter was physical surveillance. I could stake out a house for 10 hours, no problem, I'd be the guy in the tree, in the bush, in a car" (Task Force Sergeant, District A).

Similarly, the Armed Robbery Task Force's lieutenant credits younger officers with introducing social media to their strategy:

> "[…] I give credit to a lot of the younger guys because I don't know Instagram. I don't think [the sergeant] does, […] but the younger guys know the social media better than us ancient guys, right?" (Lieutenant, Armed Robbery Task Force).

With the increased use of social media comes expert knowledge in writing relevant warrants and obtaining court orders, something "[…] that a lot of the guys in the unit become proficient at doing […]" (Lieutenant, Armed Robbery Task Force). Some of this knowledge in the Armed Robbery Task Force has been developed in a close working relationship with the assistant district attorney.

This knowledge gap between the special task force and other units also becomes clear in how much officers do or do not struggle with the data they receive from social media companies. A homicide detective describes the painstaking process of piecing together information from these reports:

> "You would think you're sending a search warrant to a social media platform; they'd send it to you in a format that looks something like the user format for that? But, no, it comes in like a very plain text kind of format. And it's hard to sort through; you have to read every line just to find what you're looking

> for. And even then, if there's a message that's sent, it won't show you if there's a photograph attached. It will give you this long string of letters and numbers that you then have to go into another folder and match those exactly to find the photo and bring it. So, it's just, there's a lot of steps to get what you're looking for" (Homicide Detective 3).

A member of the Armed Robbery Task Force on the other hand knows where to look:

> "Sometimes it will be a 12,000-page report from Instagram, but the thing is that we've learned that they're using the inboxes and direct messages to conduct criminal transactions. They'll sell guns; they'll trade stolen cars; all through their inboxes. So, that's where we get a lot of these, a lot of the evidence from is there" (Officer 2, Armed Robbery Task Force).

Here, the lack of knowledge and training causes somewhat of an information overload for some officers possibly resulting in delays of investigations.

The discussion above raised concerns around police uses of social media and the manner in which officers can access it. On the one hand, officers can easily go on 'fishing expeditions' on social media trying to come up with reasons for suspicion against a person. On the other hand, some criminal activities take place online and it would be difficult for officers to know where to look before they start looking. And then there are varying shades of grey between these poles. Legally, as a task force lieutenant explains, police have a lot of leeway in monitoring social media, including the creation of fake accounts:

> "[…] in the United States, we have precedent from our highest courts that basically say if we as law enforcement create a fake Instagram account and we send a friend request to Daniel and Daniel accepts that friend request, everything that he posts from now on, we can utilise, we can do legally. With that being said, so we do that, we have multiple guys, multiple detectives and multiple accounts and they're watching guys all the time […]" (Lieutenant, Armed Robbery Task Force).

Circumventing applying for a warrant by befriending a person of interest with a fake account or asking a third person is described as a “creative” strategy by major case narcotics detectives:

> Detective 1: “[…] I can fully understand those rules, […] and those checks and balances […] to combat police overreach but it does make you have to be more creative”.
>
> Detective 2: “Creative. Yes. You got to invite the devil in” (Major Case Narcotics Detectives).

While these detectives accept the dubiousness of some of these methods as necessary, another detective sees officers’ easy access as potentially more problematic:

> “[…] when you identify somebody, you can pretty much, for lack of a better term, stalk them. And then when you do it from a law enforcement perspective, it could become problematic” (Homicide Detective 2).

Similar to the justifications for the use of license plate readers (section 6.5), the justification for the use of social media is apart from the use cases described above its targeted application. As officers of the Armed Robbery Task Force argue,

> Officer 1: “Typically, people we target. If we develop a suspect in a crime or a string of crimes, we will look into him and try to find his specific social media page and then that’s… we don’t, we’re not just on social media looking for someone saying they’re doing something, it’s very target specific”.
>
> Sergeant: “Based on evidence, based on a suspect, on a crime, or a group of guys that we have been… we might look at two or three guys involved in a crime, we get into them and then we realise that there’s a lot of crime being committed in here and that it may grow slightly too. We’re not like kind of just searching, waiting for somebody to do something, there’s too much work just following the evidence to lead us to the guys rather than just openly searching, you know” (Armed Robbery Task Force).

However, if the action were always targeted like the officers insist, having a formal process to provide safeguards and oversight to social media searches would be completely feasible. Instead, as mentioned before, officers rely on publicly visible information, fake accounts, and third persons to access much the same data they would receive through warrants. This is where a defence claiming the information is publicly accessible anyway becomes questionable. The chief of police, for instance, argues, "People put stuff out there. It's not like we're doing anything deceptive to get it. When people put things out on a public domain, it's on a public domain" (Chief). However, fake accounts and third persons are deceptive and do provide access to private information.

Finally, the department does not employ blanket social media monitoring – for now. As the chief argues,

> "[…] I'm kind of trying to stay away from all that right now. […] let the mess get sorted out. […] There's no use to having a sense of something that's really controversial when we're not quite ready" (Chief).

Homicide detectives have however encountered software used for this purpose in the neighbouring department's fusion center and with the FBI. The tool alerts to the occurrence of predefined keywords across multiple platforms. They had used it in the past during special events. These tools raise new questions, especially when combined with AI, of how individuals should come under scrutiny of police.

6.7. Phone data – data overload, filtering, and curation

There are two types of phone data detectives and task force officers analyse: phone records from the network provider and data called 'phone dumps' directly downloaded from a phone. Both types of data provide officers with rich sets of data detailing communications, contacts, locations, and diverse media files. This section focusses on the disparate practices associated with phone data and the resulting data overload for some. It also considers the consequences this amount of data has for compiling court cases.

Data from phones can be acquired with a warrant given the officer articulates a reason why there might be data associated to criminal activities on a phone. A task force officer gives the example of a drug dealer,

> “So, I can write an arrest, […] I believe you are selling drugs […]. And I also have to say that, you know what, commonly used for […] distribution of drugs, they have contacts in their cell phone […]. So, I can take your cell phone as evidence. As part of that case, and I can rip that cell phone, they cellebrite it, they plug that in, and it takes all the data off the cell phone and puts it into like a PDF file. And I mean it’s thousands and thousands of pages. […] But I can look at everything you’ve had in your cell phone. Get information, contacts and location and stuff” (Task Force 1, District B).

A person’s mobile phone contains a lot of detailed information on a person’s life: contacts, call records, messages, location data, and more. The second type of phone data – phone records – contain similar information on contacts and meta-data on communications, as well as details on locations visited. However, by contrast, it does not include any information on the content exchanged in messages. A homicide detective describes this information,

> “The phone records will tell us which cell phone tower their cell phone pinged off of at a specific date and time. And, so, that won't give us their exact location, but it will give us a general area where they were at the time. And then also the people that they communicated with, the different phone numbers. So, it's a lot of data to comb through, in terms of latitude and longitude, and correlating that with the time that they placed a call” (Homicide Detective 3).

Again, phone records contain a lot of information. The sheer amount of information presents a challenge to officers. Some detectives tell of their struggle analysing the data while others are surprised anyone would find it difficult. The challenge, as it presents itself to some, is the amount of information in always changing formats. As a detective describes,

> "[…] say I call Verizon, and I ask them specifically for the phone records between this phone, the victim's phone, and then this phone, the offender's phone, just those two numbers. I just need their numbers, all contacts, text messages, any electronic communication, photographs, digital photographs, whatever the case is from. Let's say, July 10th to July 20th. They will send me their dump from the whole month of July, both of them, whose phones they called. I get everybody's number. It's overload" (Sex Crimes Detective).

Not only would they receive more information than needed, the information would also be structured differently from carrier to carrier. For those struggling with the analysis, this impacts on the timeframes of their investigations:

> "[…] once these phone records and everything come back, you look like you're in a rat's nest. Everything's just stacked up around you, and you're trying to just keep order on everything, each individual-- 'OK, this goes with this case, this goes with this case, this goes with this case.' And we have time frames. With domestic violence, if they're arrested, we're supposed to have 10 days to follow up. And if they're not arrested, we have 14 to start making contact with the victim and get some type of supplemental report" (Sex Crimes Detective).

While some detectives are overwhelmed with the amount of data, others are not – a reflection of disparate data practices. The sex crimes detective quoted above reads the files line by line (as do others):

> "It's a lot of coffee. […] every once in a while I'll have a cigarette and take a break […]. And a highlighter's my best friend" (Sex Crimes Detective).

Other detectives, however, are surprised because the digital files would be easily filterable. As a homicide detective describes,

> “For me, it doesn't bother me, because I know what I'm looking for. A lot of times they send things in Excel, so I'm pretty good with just finding the specific cells that I'm looking for. And then I'll take those and put them in something more readable, and then just plug the coordinates in Google Maps and figure out exactly where I'm looking at. I just kind of make my own spreadsheet, to have it be a more readable format. But I can see, it's so much data when you first get it, that if you don't know what you're looking for it could be very overwhelming” (Homicide Detective 3).

In absence of a software solution (mostly probably due to cost, as one detective speculates), some units try to solve the issue organisationally. The Major Case Narcotics detectives have one detective tasked with analysing data for everyone in the unit. However, multiple detectives insist that the person analysing the data would need to know what they are looking for and therefore it could often be only analysed by the detectives themselves. Local detectives recount how they had been overwhelmed with data in a past case and had asked for assistance form two interns at the district attorney’s office. Being unfamiliar with the people, their slang, and the area the interns missed a lot of information. One of the detectives stresses, “Nothing can beat local intimate knowledge. This is institutional knowledge that you can’t package” (Detective Sergeant, District A). This highlights the need for software to render information accessible to officers as those to who it may be accessible despite its presentation may not be in a position to understand it.

The amount of data, as well as individual detectives’ struggle with it also become issues in taking cases to court. For those having difficulties wrapping their heads around the information, this can result in feeling unqualified to testify based on their findings[30]. For instance, this is how one detective feels,

> "[…] when I'm getting to court, I'm trying to explain this, but I actually, technically, really haven't been trained to evaluate this kind of stuff" (Homicide Detective 2).

Beyond the capability to explain the data, the data itself could pose a challenge. Some detectives are concerned that it can endanger their narrative in court. As a child sexual abuse detective explains,

> "I just want to know the conversation between these two people […]. […] Because I'm not interested in the kid's pictures. Yeah, she might have taken pictures of herself in the bathroom, but the defence will use that to discredit the child […]. I'm not interested in that. She's doing what teenagers do. […] But […] you give it to me; I have to disclose it" (Child Sexual Abuse Detective).

Consequentially, some detectives prefer to employ screenshots as evidence rather than whole phone dumps. This allows them to both avoid the information overload and curate the data sent to court.

6.8. Summary

On their own, many of the technologies discussed here have brought significant changes to the character of police investigations. But it is only in placing them side by side as in this chapter that the extent of this transformation of investigations by digital tools begins to become visible. Moreover, in contrast to uniform, technologically determined practices, examples like some

[30] Lack of technical proficiency can have serious consequences. For example, Denmark had to free 32 inmates over flawed geolocations from phones used as evidence in court (Henley, 2019).

detectives analysing phone records as printouts with a highlighter versus others filtering Excel sheets illustrate the diversity of digital practices. One common denominator of the technologies discussed in this chapter is that the records they provide render the past ever more accessible to investigations. This includes recording infrastructure set up or integrated by the police, such as CCTV, license plate readers, and body worn cameras, but also police tapping into recordings not necessarily made for law enforcement purposes, such as phone records and social media data. These records that are increasingly taken for granted and relied upon could however be described as 'selective memories': databases only cover police interactions as does video from body worn cameras, license plate readers record movements in and out of large parts of the city, and CCTV is restricted to camera locations. The spatio-temporality of police activities and infrastructures conditions the new visibilities afforded by these technologies and thereby shapes the possibilities of future investigations. Particularly social media not only becomes a new 'location' for criminal actors and acts, but also provides investigators with a wealth of new information including individual's social networks, whereabouts, and activities.

This chapter further interrogated the temporal affordances of technologies in day-to-day investigatory practice. The fast pace of social media updates and the speed at which some platforms delete records requires task force officers to remain engaged with the medium during proactive investigations. Similarly, the speed at which video recordings overwrite informs the urgency of detectives retrieving CCTV footage. CCTV also shapes the temporality of investigatory practice where officers can instantly review footage to re-evaluate their observations, or where BriefCam condenses the otherwise time-consuming search of retrieved video.

Many of the capabilities described in this chapter raise legal and ethical concerns in their facilitation of unprecedented access to private lives. A common justification given by officers is that the use of these technologies is targeted and effective. Much of the information like social media profiles and license plate would be public information visible to anyone – an argument that is based on the ‘plain view’ test for reasonable expectation of privacy established in *Katz vs United States*[31]. The constitutionality of license plate readers remains still unclear (see Díaz and Levinson-Waldman, 2020; Lynch, 2020). Especially in case of the investigatory use of social media, lines become blurry quickly. Using fake profiles or asking third persons enables officers to access information for which they would otherwise need a warrant. More guidance, for example in the form of departmental policy, could be necessary in this area. Another question for criminal justice procedure arises from detectives, with best intentions, seeking to curate evidence by collecting it only in limited ways (such as screen shots instead of phone dumps). Against the background of an unprecedented amount of potential evidence to be collected, the question here is how much evidence is necessary for the legal process and who decides where the limits should be. More positively, the example of slow updates on license plate reader hits also demonstrates how technology can contribute to enforcing departmental policy, in this case the prohibition of car chases.

Finally, continuing themes from previous chapters are the breakdown of technologies and the fragmentation of technological practice: license plate readers not only record false reads, those mounted on patrol cars are also rarely used because the vehicles are driven by platoon officers responding to calls-for-service; some information on databases is irretrievable because of a poor search function; social network maps get misinterpreted; detectives struggle with the wealth of video formats and resign to sharing video files on Google Drive because they have no other means of exchanging them; and some detectives wrestle with the data overload in phone records while others find filtering the data trivial. These observations not only highlight

[31] See also *California vs Ciaraolo*, and for an indication of possible limitations *Kyllo vs United States*.

the multiplicity of technological practice but also its constant evolvement brought about by practitioners finding workarounds to problems or new uses for tools available to them.

Interlude – (in)coherence of order and technological affordances

This section revisits some of the key insight provided by the US case study to lay the groundwork for the analysis in the following case. As set out in the introduction to the US case study, a multiplicity of 'orderings' (Law, 1994) prevails in the police department. With responding to calls for service, investigations, proactive policing (or intelligence gathering), patrol (with unclear purposes between deterrence, chance encounters and demonstrating presence), and compliance and accountability, there are at least five organisational priorities that criss-cross through the previous chapters and that are not always clearly distinguishable. From afar, some of these configurations resemble 'centres of calculation/translation' (Callon, 1986; Latour, 1987; Law, 2003) - particularly the CompStat meetings that collect and aggregate information on crime to allocate resources for patrol, investigations, and proactive policing. Considering Law's (1994, 2003) argument that the stability of orderings stems from their material heterogeneity, the department's data dashboard could even be read as the materiality supporting such an ordering. Yet, there is no such central order controlling both representations (surveillance) and translations (domination) to the findings of the US case study. Instead, there is social complexity – 'mess' (Law, 1994) – with a multitude of locations in which representations are formed and decisions about how to organise action are taken, supported (and at times failed) by a multitude of technologies. Representations laboriously assembled by the department's analysts (section 4.11 and 5.3) are sidestepped in parallel systems (section 5.3), turning them into weak 'obligatory points of passage' (Law and Callon, 1992). Once assembled, the processing of these representations is also hardly straight-forward, with crime statistics and accounts of crimes needing to be aligned with a variety of priorities and strategic options (section

4.2)._While the crime statistics would allow for a form of ‘biopower’ (Foucault, 2009), for example by patrolling areas with abnormal crime counts to deter further crimes, the mixture of a logic of ‘aggregation and reaction’ and one of ‘attributing causes’ reflects an empirical entanglement of different forms of governmentality (see section 2.2). Even more so, once an action is determined based on the centrally available knowledge, the translation of this into effects on the periphery rarely works. Rather every step is precarious and often adds new interpretations and priorities. Examples of this are the various strategic priorities in section 4.3 including the failure of roll calls to pass down instructions for patrol, and even the smaller hiccups in relating details for calls-for-service described in section 5.1.

The analysis of the UK case study described in the next part of the thesis also rubs off against (and sits awkwardly with) the conceptual framework of ‘centres of calculation/translation’. Here, the data visualisation platform multiplies analysis and interpretation by tasking the periphery with it, while simultaneously shaping this analysis in institutionalising a focus on individual risk and ‘problem-solving plans’ (particularly chapter 8). Becoming an ‘obligatory passage point’ (Callon, 1999) as the centre of discussions on resource allocation and subsequent recording of activities, the platform also turns into a vehicle for managerial surveillance.

The coming chapters further continue the second main focus of the previous analysis: the technological practice of police officers. Chapters 5 and 6 have highlighted the diversity of this practice and how it is often shaped by breakdowns and workarounds. On the one hand, technologies like video surveillance, license plate readers, or social media have become ‘obligatory passage points’ (Callon, 1999) for detectives if they want to solve cases – just as they are often collocated with passage points like major street junctions or an access point to online communities. As such, technologies change the spatio-temporality of police work (chapter 6). On the other hand, this relation is not deterministic. For example, section 5.2 demonstrates how databases do not replace, but rather complicate officer discretion during vehicle and persons stops. This relation of ‘affordances’ (Hutchby, 2016) that technologies have in police work is foregrounded again in the coming chapter 8 which analyses the co-construction of risk between officers and the automated individual risk scores produced by the data dashboard in the UK police force.

Data Part 2. Demand-driven policing in the UK: How risk scores and data visualization shape policing. Preface to the UK case study

As a result of austerity measures implemented by David Cameron’s Conservative government following the financial crisis of 2008, police forces in the UK have suffered from budget cuts and increasing demand associated with reduced provisions of social services (see e.g. BBC News, 2017; Dodd, 2019; National Audit Office, 2018). One of the interviewees describes the situation as following,

> “So, kind of the reason of that, and this would apply to any UK police force, is we're... demand has increased, complexity of demand has increased on all UK police forces. At the same time budget cuts have come in. We've taken like 60 to 70 million pounds out of the organisation since 2010, like 20 to 30 percent reduction in our budget line. When our actual demand has probably increased by 20 to 30 percent in that time period” (Business Intelligence Manager).

Under these conditions, the UK force studied here introduced a new data visualisation platform (DataVis) to better allocate its resources. In this, the goal associated with this platform is very similar to many predictive policing applications. However, the platform has a significantly larger range of functionalities from identifying businesses that call unusually often and areas where ‘anti-social behaviour’ requires ‘problem-solving plans’, to risk scores for prioritizing offenders and victims, to a large number of performance management features. Prevention is not only the goal for analysis pointed outwards of the organisation, but also for the analysis of workloads and the prediction of burnouts.

DataVis[32] is a data visualization platform that combines multiple, previously separated, databases and provides officers with various dashboards called ‘apps’ that supply them with preconfigured views of aggregated data. These may be related to information about crime and suspects like maps of recent crimes, crime trends in an area, risk ratings, times when certain crime types occurred, or peaks of demand; or performance information like number of outstanding reports, time frames of victim contact, or number and variety of cases worked by a team. The underlying database architecture is relational and allows officers to click through different levels of aggregation from force level to a specific patrol beat or individual case files. They are provided with multiple options to filter the data according to their needs. DataVis provides a “self-service environment” in which officers can do a lot of the data analysis that was previously provided centrally. Even more so, it provides them with data analysis that previously would not have been available due to constrained resources for human analysts.

The software comprises of around 30 ‘apps’ for different tasks. To give an idea of the types of tasks encompassed, the following are some of the more central functions: The Crime Intelligence App comes with a number of different ‘views’, that is a collection of diagrams, lists, and maps. It visualises crime trends as number of incidents compared against fortnightly averages, puts offences on maps, lists linked individuals, and associated modus operandi. It allows filtering, for example, for burglaries in a certain area, over a certain time range, with a certain modus operandi. It can be a starting point for identifying crime series. It also shows forensic recoveries made at crime scenes allowing officers to identify promising cases. It links in intelligence reports and a special Anti-Social Behaviour View enables officers to link ASBs to other possibly linked crimes. Furthermore, it allows officers to identify frequent callers and address possible,

[32] Pseudonym.

underlying issues. An Offender Management App gives a risk score to, at the time, 218386 offenders on the system. It outputs a list of wanted individuals, recent prison releases and intelligence gaps on individuals. The counterpart is a Vulnerability App that gives risk scores to victims. DataVis also includes a Supervisor App, and, as a counterpart, a MyWork App that display workloads, demand scores for officers, open tasks and cases linked to each officer.

The following two chapters analyse the simultaneous standardisation of practice and pluralisation of decision-making afforded by the software. The first chapter interrogates how patterns in the data rendered visible by DataVis and particularly individualised risk scores are interpreted and translated into actions. It contributes an empirical perspective on the co-construction of risk between officer and software as a counterpoint to common techno-deterministic perspectives on predictive policing. The second chapter investigates the effects the software has organisationally in institutionalising a 'threat-harm-risk'-approach through the risk cores, redistributing knowledge, and re-ordering performance management. It thinks through the ways the software assumes power. Particularly in comparison with the previous chapter this highlights the difference in affordances that police information systems can have, which only become visible through detailed empirical engagement.

The analysis here is based on conversations with seven interviewees in six different roles. These are the Business Intelligence Manager with the main responsibility for DataVis' continued development, a Tasking Coordinator using DataVis to allocate resources centrally, a Chief Inspector and a Neighbourhood Sergeant covering neighbourhood policing (engagement with the community in a specific area focussed on proactive prevention), a Detective Chief Inspector, and two Offender Managers.

7. DataVis in practice

This section focusses on risk scores and crime patterns as ways in which DataVis represents the ‘outside world’, that is criminals and crimes. The goal is to show the process of co-construction of risks between officers and software. In a far more complex way than the often-assumed techno-determinism, officers add their own priorities and practical considerations to how they use and interpret information displayed in DataVis. The first sub-section deals with the prominent feature of individual risk scores and their interpretation and enactment, while the second sub-section describes the identification of crime patterns as starting points for investigations and ‘problem-solving plans’.

7.1. Risk scores

While risk scores are clearly not the only use of DataVis, they form an integral part of the strategy for reducing demand. The logic of this approach is rooted in a criminological discourse on ‘chronic offenders’ and ‘career offenders’. Beginning with Wolfgang et al.’s (1972) cohort study on offending in Philadelphia, criminologists have pointed towards a small share of frequent offenders causing a large proportion of crimes (see e.g. Blumstein et al., 1986; Cohen, 1983; DeLisi, 2005; Falk et al., 2014; Piquero et al., 2003; Weiner and Wolfgang, 1989). This insight has propelled programs of selective incapacitation, for example through ‘three strike’-laws that seek incarceration for repeat offenses (Visher, 2016; Weitekamp and Herberger, 1995). Critics have questioned the effectiveness and appropriateness of individual-focussed policies based on selective incapacitation (Blumstein and Moitra, 1980; Gottfredson and Hirschi, 1986; Kovandzic et al., 2004; Stolzenberg and D’Alessio, 1997; Visher, 2016; Weitekamp and Herberger, 1995). Parallel arguments were made a little later in the ‘dangerousness’ debate among UK criminologists (Bottoms, 1977; Bottoms and Brownsword, 1982;

Conrad, 1982; Floud, 1982). In the 1990s and early 2000s, the legal framework for actuarial risk management procedures for offenders comprising of restrictions, conditions, sanctions, and enforcements organised through agency cooperation between police and social services began to take shape in Britain (Kemshall, 2010; Kemshall and Wood, 2008; Wiliams and Nash, 2014). This approach integrates actuarial risk assessments of reoffending with assessments of ‘harm’. More recently, Sherman et al. (2016) distilled these norms into the ‘Cambridge Crime Harm Index’ which in turn Liggins et al. (2019) use to attribute the majority of harm to the ‘felonious few’. The risk scoring discussed here builds on similar assumptions combining offending patterns with a numerical index of ‘harm’. A statement of one of the offender managers reflects the ‘chronic offenders’ discourse:

> “So, the concept is really simple. When it comes to sort of burglary, car theft, used to be shoplifting. If you take the top 20% of the offenders, […] they will commit, roughly, 80% of the crime. So, if you go after that 20% […], then, hopefully, you're taking your biggest bite of the cake. You're really having the most opportunity to influence and reduce that 80% of crime” (Offender Manager 2).

However, as the Business Intelligence Manager insists, the focus is not supposed to be on incapacitation,

> “[…] we’re not in the business [of] just locking [people up] […] ‘cause we’re gonna [be] doing that forever and a day with some of these individuals and it’s just non-sensical, and quite frankly, […] we can’t afford it. So, we need to be reducing demand […]” (Business Intelligence Manager).

The ways in which officers interpret risk scores and try to act on them to reduce this demand will be the subject of the next two sections.

The Business Intelligence Manager, in charge of DataVis's development, explains how previous offending and harm scores are combined,

> "[…] this is breaking down those offenders into risk categories. So, high, medium, standard risk. […] basically we have a daily model that scores about two million people[33] in our database every day. So, we have a likelihood of offending model that is very similar really to the OGRS, the probation services', OGRS risk modelling[34]. […] And then, what we do, we, for that ten years' worth of offending, we link it to this concept of harm. So, for every Home Office crime classification we've given it a harm value. […] So, what we do, we have the likelihood of them offending and then the aggregated harm. We kind of put those two together to determine the risk" (Business Intelligence Manager).

The risk scores are then additionally qualified by whether individuals have been 'escalating' in their offending:

> "[…] if […] harm has been front-loaded around the more recent [events], then we have a trigger that actually we're saying that they're escalating. You know, so this person has gone from shoplifting, kind of low-level volume crime, actually now we're seeing […] serious violence and threats and all the rest […]" (Business Intelligence Manager).

The risk scores, while including an element of prediction, clearly entangle 'objective' prediction with normative priorities encoded in the 'harm' score. What is apparent here – particularly in the visual separation of columns for harm score, reoffending risk, and the combined score on DataVis –, is that opposed to ideals of mechanically preventing objective predictions of the

[33] It is unclear where this number comes from as it contrasts with 214000 offenders he mentions later, as well as 218386 offenders mentioned by the Tasking Coordinator. It may include victims for which a harm score is calculated but who would not appear in the list of offenders.

[34] See Howard et al. (2009).

future, the risk scores aim at the standardization of normative priorities. The evolving and vague language of risk and harm in laws and statutory guidance[35] is translated into simple numbers. Whereas calls for transparency in the literature and public discourse regularly aim at unmasking the ‘objective’ veneer of the data analysis, here transparency is required to enable public debate on these explicitly encoded weightings of normative judgements.

Furthermore, anyone who has been linked to a case as a subject over the last ten years is included in the risk ratings. The Business Intelligence Manager makes clear that individuals would not need to have been convicted as “[…] obviously the proportion that gets through to conviction is quite small” (Business Intelligence Manager). This raises questions of due process and who the final arbiter of guilt should be in the criminal justice system.

Although the scores are targeted at standardising practice across the organisation, the risk scores at first created new uncertainty by highlighting all those individuals that could require attention but were previously unknown to officers. In this sense, the logic of risk scores follows what the literature review in chapter 2.2 identifies as ‘algorithmic discovery’ (albeit the configuration that DataVis entails does not quite match with that of a ‘centre of calculation’ as detailed in chapter 8). As the Business Intelligence Manager recounts, risk scores were accepted only with the introduction of DataVis because it would enable officers to quickly review relevant case files:

> “[…] when we first started doing predictive risk modelling outputs, before we had, before you could interact with it, it was just seen as, ‘Oh great, there's loads of risk lists flying around the constabulary, which I've got to research every single one of them’. Which they can do really quickly now, but they

[35] For example, see Baker (2010) on the linguistic confusion caused by the differentiation of ‘harm’ and ‘serious harm’.

> couldn't back then. […] the organization was quite uncomfortable with seeing all the risk" (Business Intelligence Manager).

Now, instead of arguments of effectivity and objectivity discussed in the literature on predictive policing, the standardization of risk assessments and its application to all files without the possibility of missing a case are the arguments for the adoption of automated risk scores. As the Business Intelligence Manager describes,

> "[…] when you start running predictive risk models you've got a really powerful torch and you can see it and it's kind of like, 'Ooooooh myyyyy goooooood', like quite scary, but you will need to embrace it because you can make better resourcing decisions. Appreciating that you can't do it all, but you'd rather be able to see it, to make the decision, rather than have that lighter, […] where an officer said this person is high risk. Well, hang on, what about all these other people we've got a shed-load of data and information and intelligence on? You know, we shouldn't just be seeing risk through a referral mechanism" (Business Intelligence Manager).

The notion of risk employed by the Business Intelligence Manager and other interviewees seems to point to three separate ideas of risk: First, there is the question of probability of reoffending, which does not seem to be the main logic operating here as it forms only part of the final score which includes also recency and harm. Second, the disquiet caused by risk made visible described in the above quote resonates with Mary Douglas' (1992) theorisation of risk as the moderns' logic of apportioning blame which then structures action towards avoiding this blame. Here, the visibility of risk renders blame attributable to the police where they fail to prevent it. On an individual basis, some interviewees fear that the risk scores introduce a new professional risk in being held accountable to acting on the scores. However, as section 7.1.2 demonstrates, the risk scores are far from the only priority for officers who consider other non-quantified 'risks' such as perceived public disorder. Which leads to the third and possibly main meaning of risk: Rather than identifying cases that pose the highest reputational or legal risk to the organisation, the risk scores are *one* of the prioritisations of police work. Functioning as priority scores they are believed to reduce crime by focussing police interventions on those causing most of the crime. Thus, risk is less related to dealing with future consequences of present action, as in the thesis of the 'risk society' (Beck, 1992; Giddens, 1991), but rather with prioritising action to bring about a different future.

The following sections will look at how the officers using DataVis interpret the risk scores and how they act or do not act in response to them.

7.1.1. Interpreting risk scores and deciding to act

> "What [the Business Intelligence Manager] has said all along is that DataVis is an aid. We shouldn't hold our eggs in that basket, you've got to have professional judgement as well. You've got to have someone looking at that individual, saying, 'Right, this is what he's suspected of, this is what he's convicted of'" (Offender Manager 2).

The goal of this section is to address the new choices officers face when they are presented with risk scores, to understand what the risk scores mean to officers, and how exactly they interact with the professional judgement mentioned by the Offender Manager.

Oftentimes critiques of predictive policing paint a techno-deterministic picture in which the software decides, and the officer blindly follows – something which under section 49 of the Data Protection Act 2018 would be illegal in the UK[36]. What will become clear in this section,

[36] Section 49 contains the right not to be subject to automated decision-making; it states, "(1) A [data] controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law. (2) A decision is a "significant decision" for the purpose of this section if, in relation to a data subject, it (a)produces an adverse legal effect concerning the data subject, or (b)significantly affects the data subject".

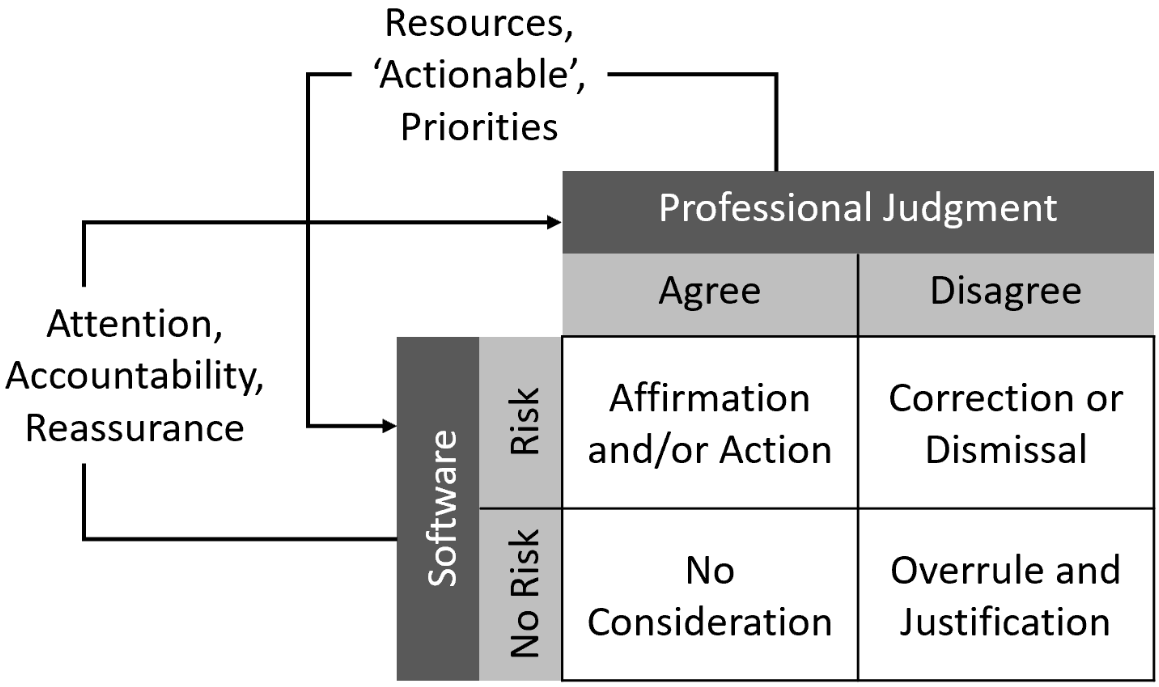


Figure 5. Schematic of the co-construction of risk.

is that the relation is more complex than that. The perceived risk is co-constructed in the interaction between officer and software. This is not to say that the software is not ascribed values of science and fact. Indeed, the Tasking Coordinator asserts that DataVis would give a better assessment of current issues and risky offenders than officers' "knee-jerk"-assessments in the past and the Chief Inspector refers to it as "putting a little bit of science into that". However, all interviewees stress the importance of professional judgement. In fact, the Chief Inspector reels back his claim a little later in the interview: "You always have to bear in mind that however good an algorithm is, it's not absolute science. It is a guess. That's all it is" (Chief Inspector).

Professional judgement plays not only a role in assessing if an offender that is flagged by DataVis poses a risk, it also encompasses practical considerations around resources, risk scores being 'actionable', and other strategic priorities. DataVis is helping to "put people on the radar" (Tasking Coordinator). However, once on the radar officers have to decide what to do with those individuals that are brought to their attention (section 7.1.2 will further elaborate on the decision making around which actions to take). While the decision risk/no risk may appear binary at first, the professional judgment in which DataVis is embedded constitutes a more complex process (see Figure 5). In this process the officer decides to filter the risk list according to their priorities. This may, for example, be offenders within their catchment area. The software then suggests a list of risky individuals, some of which would possibly not have gained the officer's attention otherwise. Unless the software reaffirms the names of offenders known to the officer, the officer would then check the individual's record to decide if the individual warrants further attention. This means on the one hand scrutinizing the offender's file, and on the other hand, tracing the algorithm's reasoning of harm and recency. If the officer finds an error in the score, the score is ignored or the error rectified. Beyond this, officers weigh the scores against their own mental 'lists' of risky offenders that reflect different strategic priorities. While the officer is selective about the risks presented by the software, the software provides reassurance not to miss risks given the high demand on officers, and draws attention to an evaluation of offenders through harm and recency of offending (section 8.2 will address the power relations that emerge from this in more detail). The following addresses this process along the outcomes displayed in the cross-table of Figure 5: correction or dismissal, affirmation and/or action, overruling, and no consideration. It then considers limiting factors that inform the prioritisation of individual's deemed risky because or despite the software's risk rating.

First, the necessity of professional judgement becomes quite clear in cases where officers are confronted with an unknown offender at the top of the list whose rating is 'erroneous' because of issues with the underlying data. The software functions quite unlike the ominous 'black box' in that it allows officers to trace errors. The Chief Inspector describes such a case:

> "[..] we had one person that featured on the most wanted list a few weeks ago. It was a female and she was, I think, second highest score; no one knew

> her. When they looked back on why she was on the second highest score, she’d been arrested as part of a murder inquiry, but that was over 20 people arrested to probe that murder inquiry. We charged a person; it was a different person. Whatever her involvement was, probably fairly minimal, and they were not charged, but that has raised their risk score. That's always the danger if you just use data alone, you have to apply human intelligence, and you have to question, ‘Well if I'm not aware of it, what is there in the background?’ At least, the system does enable us to look at that background very quickly through all the records, […] and then we've removed them from that list” (Chief Inspector).

Spotting and amending errors require an understanding of the factors that go into the risk scores. One of the offender managers, who is very aware of how the scores in DataVis are dependent on the data held in the force’s record management system, points out that the difference between being a suspect in a case or solely being mentioned was just a tick in a box. But being recorded as a suspect, wanted, or charged would count towards the score. Officers also have a sensitivity to the underlying data being flawed. As the Chief Inspector, points out, mistakes in filling forms – that is, entering data into the system – are difficult to avoid:

> “So many systems are so complex. You have to do this box. You have to do this box. You have to do that. When you are tired, or when your adrenaline is flowing, you don’t think about all these things. That’s where we have the problems” (Chief Inspector).

In consequence, officers check where the scores come from and amend errors if necessary. Paradoxically, the effort to reduce uncertainty through automated risk monitoring creates new uncertainty in its reliance on ‘good’ data. Data quality gains in importance as errors that previously would have inconsequentially collected dust on a paper file in the archive now cause unexpected risk scores. Consequently, the police force has formally added data quality to its risk register.

Second, the software's risk ratings could be in accordance with the officer's professional judgment, in which case the offender is either already known to the officer or they come as a surprise. In the first instance the risk ratings reaffirm officers' assessments, in the second they may require a readjustment of priorities. The Chief Inspector gives an example of such a change in course of action:

> "I don't think DataVis has necessarily shocked me. In one or two occasions where someone's brought something to my attention. I can think of one instance. I had a domestic incident: […] It was the sort of thing where a neighbour phoned saying, 'This has happened. I'm really, really concerned'. […] Officers had gone out and said it was two brothers. […] Somehow, randomly, that incident had come up on DataVis and it had a really high risk score, and someone had the common sense to look at why. They brought it back to me and said, 'I'm a bit concerned about this job'. I looked at it and, actually, when we saw the history of the young kid that made the threat, he was a person that could go and grab a knife and stab his brother. That information was there. You could understand how officers wouldn't have picked it up at the time, but that really surprised me. […] We put in place much more rigorous safeguards as a result of that. […]" (Chief Inspector).

Despite such 'surprises', most of the times the individuals at the top of the risk rankings would already be known to the officers. That is why DataVis has "not shocked" the Chief Inspector in the quotation above. But even if the majority of risk ratings is not surprising, these ratings fulfil a number of functions: They a) ensure officers do not miss an escalating risk, b) reassure them in their own assessments, and c), because officers at higher levels of the organisation have access to the same information, hold them accountable to knowing the top offenders in their area. Section 8.2.1returns to the issue of accountability. The following quote from the Neighbourhood Sergeant illustrate these three functions:

> “there was one person, the top offender I think it was, who came up to me, I had no idea who they were, but it made us make the inquiries to go, ‘Actually, who's this person?’ Actually, it was just for one thing from about just under 12 months ago that was an attempted murder, but it puts them right to the top of the list. But it made you question, why don't we know them? Should we know them? It could have easily been someone that we just missed.
>
> Similar occasions really, you get to see, it brings together emerging patterns quite easily, without you having to always be on top of everything. What you find, so [name] sat next to us now, she'll know the stuff. She'll know the stuff before we raise it, frankly. But that to some extent is exactly what you want it to reinforce the fact that the guys know exactly what they're doing.
>
> That's what this does really, so if a question comes down to us about what's DataVis showing this person's causing us issues. I would bet my house on the fact that all the beat managers here would know all about it, know what's going on, the vast majority of them. And would already be doing something with it. But if that wasn't the case then you'd need to have to be worried about what they were doing” (Neighbourhood Sergeant).

Third, officers were very aware of types of cases and strategic priorities that would and could not be picked up by the software’s risk rating. In cases like these their professional judgement would overrule the algorithm and they would keep track of these offenders themselves. For example, risks of offenders from outside of the force’s geographical boundaries would be underestimated due to missing records, or cases that escalated quickly but without historical precedent would escape the ratings. As the Detective Chief Inspector explains,

> “Where you've got a bucket, which is empty because you've not offended before and you haven't got that history of risk, to go high-risk is harder to spot sometimes. I think sometimes ... The example there would be a lady who started receiving things through the post, and that escalated to be notices around that she was gonna be killed, animals left. There was an incident

> where she was then stabbed. That wasn't quite so clear on DataVis because, one, it was fast-moving, but secondly, there was no precursor […]" (Detective Chief Inspector).

In consequence, officers would have to keep track of these cases themselves and rely on their professional judgement.

> "It certainly doesn't replace professional judgment because sometimes risk is based on your history. Sometimes there are circumstances where some person doesn't particularly got a history, but for whatever changes, mental health or [other] changes, they're very risky. Sometimes the analytics doesn't pick that up because they haven't done anything yet. It doesn't score as a high-risk. Your professional judgment and understanding the job and reading the victim is still really important" (Detective Chief Inspector).

Even more interestingly, risk scores sometimes do not reflect the same priorities officers deem important. The Chief Inspector, for example, believes a paedophile would pose a risk regardless of the amount of information the police would hold on them and hence regardless of the risk rating. For the Neighbourhood Sergeant community priorities are as important as the high-risk offenders that DataVis highlights:

> "We also have people that we know are high risk in the centre. But the way it might be reported, and the way stuff's done, they're not necessarily DataVis priorities, but they are community priorities, especially the street community people here. We got lots of people who are involved in drugs, sort of low-level offending, regular low-level offending. They don't hit the marks in the same way necessarily. Some do, some don't. […] You got to have that […] professional judgment […]. There's no substitute for the people, and you really see that when you've got good beat managers and good PCSOs that they can tell you immediately, not just say it's wrong, but why the data doesn't collect it" (Neighbourhood Sergeant).

It is clear from this statement, that attending to these other priorities also means having to justify this decision against the risk scores.

Fourth, offenders outside of those rated risky by the software and those added through professional judgement in the cases described above receive no further consideration. “The idea is with DataVis, that we’d never miss [anything]. Nothing would slip through the net with what you know and what they know” (Neighbourhood Sergeant). After all, DataVis was designed to help officers manage their high demand and the related limits in resources. One of the offender managers highlights this function,

> “What DataVis is really good for is that we, as our team, we can't keep an eye on everyone arrested for burglary or robbery all the time. It's just not possible. We're not here 24/7. […] So, what DataVis is really good for is bringing up people that we might not have seen before. Might think, ‘Haven't seen that thing before. That's a high score. They're escalating. They've got a previous for burglary. Let's take a closer look through it’" (Offender Manager 2).

So far, this section has portrayed the decision between risky and not risky in a somewhat binary way. However, priorities, as in including individuals the software does not rank high, and resource limits, as in ignoring those that are not in the ranking or of another priority, indicate a more complex process of co-construction of risk. The list of risky offenders is not a static object that officers can either agree or disagree with. On the contrary, risk ratings change over time and officers have multiple options to filter the lists according to their priorities. As a result, the decision of which risk scores to choose and which risk scores to act on is dependent on other considerations of resources and priorities that inform the officer’s professional judgement.

Against the background of limited resources, the risk scores present officers with new choices of who to focus on. The following quote from the Chief Inspector exemplifies the dilemma of this decision as well as the flexibility in creating a relevant list of offenders to begin with,

> “[…] we don't have capacity. Our highest risk offenders will produce thousands. If I narrow it down to my area, I could still have several hundred. So, then I might want to look at category of risk, I'll just look at my high risk. Well, then I can exclude those in custody. But do I exclude the ones that are being shown as [being in offender management]? One hopes that they are doing the right thing, so maybe I'll exclude those. Then I still have 30, 40. Well, with everything else I know people have got going on, I could say you're right one per beat manager, but that beat manager is stacked up, that beat manager's away, so I've got to take those off. It's a very arbitrary list and if I did that today, I can guarantee you next week or in two weeks’ time, when my next task meeting is, there will be a couple of different names in there. So, do I stop doing these because working with them is going to be three, six months? Do I now bring in other people, but then that's adding to my list, and I've just said capacity is an issue? Or do I take one point in time and say, ‘No, we're going to do these, screw anything else, we'll just focus on that.’ There's no policy, there’s no procedure, it's done on gut, gut instinct, it's done on a sense of knowing what people are committed with, and just trying really to manage maybe the top one or two. If I can do that, well, I'm doing one or two more than I was doing, not because I'm not doing anything. If I've got capacity to do more, I will try but as I'm sure everyone has said, ‘constant balancing act’. […]" (Chief Inspector).

Not only do officers have to decide who of those ranking high to focus on, but, as is clear from the quote above, they also decide who not to focus on anymore when someone else has become more important. “Occasionally, we have to say, ‘no, sorry. I know they’ve offended but I’m taking them off because we need to focus our time on the more harmful’” (Offender Manager 2).

Strategic priorities can not only prompt attention to offenders outside of the risk ratings provided by the software, as described above, they can also inform the way the software's risk ratings are produced in the first place. The Chief Inspector is filtering the list by area and offenders being out of custody, the Business Intelligence Manager mentions filtering by age when focussing on minors, and filtering by type of offence. The Offender Manager also suggests filtering those that are escalating in their risk versus those that have a high risk score that is fairly static. Filtering is a key component of the co-construction of risk. In contrast to a techno-deterministic view, the software makes the officer consider new risks as much as the officer makes the software reflect their own priorities.

Beyond deciding what the 'actual' risk is, the Neighbourhood Sergeant points to another dimension that informs the tasking decisions: do officers know what to do about a risk. Even further: do they judge it to be the right moment to do something. These professional judgements, which will be addressed in more depth in the following section on what steps officers take based on the risk ratings, shift the decision to a set of considerations that are outside the software's scope.

The co-construction of risk allows for a tension between risk ratings being merely about awareness and the accountability that comes with this awareness. The awareness perspective makes sense given the limitations of resources, the arbitrariness of picking the top offenders of differently filtered lists, the open question of when police attention should stop or be reallocated, and, finally, the complexity of what actions would be appropriate for 'managing' an offender. Consequentially, the Neighbourhood Sergeant sees a high risk rating as "[…] a standpoint for you to have to pay some attention and find out what's going on" (Neighbourhood Sergeant), and the Chief Inspector welcomes the added awareness even when no action is taken:

> "Even if we assess [the score] and say, 'Okay, we can see where it's gone up, but it's all because of historical stuff and, actually, there isn't anything happening. They have that high score, fine at least we looked at it and made that decision'" (Chief Inspector).

The police force made the strategic decision not to have procedures that would dictate who to focus on based on the risk scores. As the Business Intelligence Manager explains,

> "[…] we didn't want to go down the route of saying, 'right, everyone who comes in the top twenty needs to do something […]. […] this is a tool, you know. So, actually, 'I didn't do anything with this one because I was dealing with this one as a high-risk referral that came in'. […]. […] on the whole it's not that regimented. Because I think, we'd get into problems if we did. And I think, […] it would almost take away that judgement element to it […]" (Business Intelligence Manager).

Yet, the Tasking Coordinator argues that DataVis helps in creating accountability for those that ignore the ratings of high-risk offenders. In a complementary way, the Chief Inspector fears

> "[…] the time when we go to something, the information is on DataVis saying this is a really high risk, we've got to do something. We're not aware of it. And someone turns around and says, 'It was there. Why didn't you do it'? and someone is then held to account" (Chief Inspector).

Especially the public would have not much understanding for limits in capacity and capability that could have undermined the necessary actions.

The individual responsibility of deciding who poses a risk is diffused through local tasking meetings that review the top risk offenders and locations. In these meetings other priorities that are not picked up by DataVis can be discussed and prioritised. Section 8.2 will return to this issue of governance.

7.1.2. Actions from risk scores

“Take the carrot or we’ll beat you with the stick” (Offender Manager 2). What the Offender Manager describes are the two basic options officers have in dealing with offenders: enforcement or assistance in areas like housing, drug rehabilitation, or finance. As mentioned above the decision of acting on a high risk score is partly informed by the officer’s assessments of how and when best to interact with the individual. This assessment seems to differ with an officer’s role: for the DCI and for Central Tasking enforcement seems to be the focus, for the offender managers it is more assistance, while the neighbourhood policing officers bridge the gap between both poles. A fourth use of risk scores exists in providing ad-hoc intelligence during emergency-call handling. The following will outline these four different approaches to risk scores.

The Detective Chief Inspector stresses the reactive use of DataVis in prioritizing who to arrest and which crimes to investigate.

> “[…] so just say it’s a GBH [grievous bodily harm] outside in the street. Basically, with DataVis, we should be able to see actually the offender is high-risk. So, the review should be, okay, I’m the Sergeant, I recognize that the offender is high-risk for these reasons, I’m prioritizing this investigation. […] I can see the victim is of high risk, so I’m gonna safeguard the victim. We can’t deal with everything as a priority. We can’t. It’s too much work. DataVis must be part of that prioritization along with that professional judgement. […]” (Detective Chief Inspector)[37].

As the Chief Inspector puts it: “[…] who is it we need to go out and arrest that will have the biggest impact?” (Chief Inspector). Similarly, the Tasking Coordinator points out how DataVis

[37] DataVis includes offender risk scores as well as risk scores for victimization.

would be used to identify the top twenty offenders with outstanding warrants or offenses on the record management system to task operational support teams with arrests to make. Not only would DataVis help in prioritizing these, it would also help in filtering out those who were in custody already as DataVis drew on data from multiple data bases. At the time of the interview, 14 of the cases with outstanding warrants according to the system were also recorded as being already in custody. In the past, officers would have still been knocking on doors looking for these persons.

Prioritizing by risk scores, the Business Intelligence Manager explains, changes the focus from solely looking at the severity of a crime to taking the offender into account. Now, a shoplift that is committed by a high-risk offender would receive more attention. "[…] it's all about the person, not necessarily the offense in terms of that perspective" (Business Intelligence Manager). DataVis institutionalises a prioritisation of enforcement around the dangerousness of an offender including the value judgments encoded in the risk score.

A second use of risk scores is the prioritization for offender management. The Business Intelligence Manager is quite keen on stressing that "enforcement is what we do", he laughs, "but it's not in a vacuum. Where we need to do the doors in or all the rest of it, we will do, but ultimately we're wanting to reduce demand" (Business Intelligence Manager). And in another part of the interview: "'cause ultimately, we'd be doing that forever and a day. This is about getting upstream and resolving and, like, managing offenders, rather than just targeting them" (Business Intelligence Manager). While the Business Intelligence Manager suggests that demand is reduced through management programs by solving underlying issues and thus preventing any reoffending, the two offender managers, more realistically, highlight the success of merely extending the period of not offending.

> Offender Manager 2: “Somebody that's so entrenched in crime, it's unlikely that you're gonna stop them offending forever and turn their lives around. […] But the best thing for us to do, is if we can extend that period of not offending to three months, six months, 18 months, then we've prevented all that harm and unpleasantness to all the members of society. Which is, for us, what it's really about”.
>
> Offender Manager 1: “Yeah, for someone who's committed a hundred burglaries of... to have six weeks crime free, that is 150 less victims in the area that you're working in, which is an incredible success”.

Extending the period of no offending for a few months would not only prevent some of the harms caused but also reduce the amount of resources invested in attending and investigating crimes.

There are multiple “management programs” that provide the organisational structures for providing offenders with assistance. Based on public reports, there are two main management strands: MAPPA and IOM. MAPPA stands for Multi Agency Public Protection Arrangements and deals with registered sex offenders, violent offenders sentenced to 12 months or more, and those that ‘pose a serious risk of harm’. The arrangements exist for every police force in the UK and are led by police, probation and prison services with Social Services, Health Services, Youth Offending Teams, Jobcentre Plus and Local Housing and Education Authorities under duty to comply. Representatives of these agencies meet, at different intervals depending on the risk, to discuss and share information about an offender[38]. As of March 2018, the force has more than 2500 MAPPA eligible offenders in its area. However, the majority of these would be managed under ordinary arrangements. The second strand is IOM, which stands for

[38] Previous research suggests that there is resistance to this form of cooperation and information sharing among participating agencies resulting in police and probation services being the main participants (see e.g. Nash and Walker, 2009; Reeves, 2013).

Integrated Offender Management. Integrated Offender Management is like MAPPA in that it brings together police, probation, prison, and recovery agencies. It targets serious acquisitive crime. Within IOM sit IRiS and IMPACT. IRiS focuses on ‘domestic abuse, domestic extremism, sexual offending, criminal groups, and serious organised crime. While IRiS focuses on ‘the most serious and high-risk individuals’, IMPACT targets those at high risk of reoffending but with a lower harm risk, such as acquisitive crimes. It comes with nine pathways along which offenders are offered support: drugs, alcohol, accommodation, children and families, finance, benefit and debt, mental and physical health, attitudes, thinking and behaviour, education, training and employment, and for women: domestic abuse and sex work. Finally, the force has a version of the Troubled Families program which supports families in cooperation with local councils. Problems that are addressed are crime or ‘anti-social behaviour’, irregular school attendance, children at risk, individuals at risk of financial exclusion, domestic abuse, and various health problems.

The purpose of the meetings as described by the offender managers is to gather information on where the offender is in their life. Are they using methadone, what was the result of their latest drug test, do they have access to housing, or have they split with their partner? The agencies would meet on a bi-weekly basis to discuss offenders and possible ways of keeping them on the ‘pathways’ by providing opportunities like educational training or voluntary work. However, if the offender managers judge the individual not be following the right path, for example having relapsed into drugs or being linked to a new series of burglaries, they arrange for surveillance teams or capture units to eventually re-arrest them. The carrot is hanging very close to the stick:

> “[we] say to them, ‘Alright, if you reduce your offending, we will help you. We'll help you with your drug or alcohol abuse, we'll help with your housing,

> we'll help you with issues with your family, with finance. All these different pathways, we will help you. If you don't take my help, then you go to number one on the list, or you go up the list, and we will prioritize arresting you and locking you up'" (Offender Manager 2).

The decision making around who is kept in a management program, who does not require the same attention anymore, and who should be prioritized for arrest instead, is again dependent on professional judgement of the offender's progress. These judgements are translated into risk categories of red, amber, and green, which are then used to decide, for example, the frequency of meetings concerning an offender. DataVis helps in making these judgements by making information on an offenders progress along the 'pathways' easily accessible.

Offender managers may decide that the management program is not working when an offender does not accept any help. As one of the offender managers explains:

> "They say this is what I do. I'm happy doing this. When I get caught, I'll go to prison, I'm not going to change my life. It gives me what I want, it ticks all my boxes, go away. So, they go. And they go constantly through that. They go to court; they go to prison. They come out of prison after a very short stint because it might be hundreds of shop thefts. We cannot really change them unless they're ready to be changed so we have to put all our efforts into the right people. The ones that we can help to change" (Offender Manager 1).

What is clear from this statement is that the decision to prioritize arrest when there is no engagement also speaks to the limited resources for managing offenders and the resulting need to prioritize those that are more promising to be successful. This is similarly true for the second way in which offenders may leave the management program: engaging with the support and not offending for a while.

> “If we look at them and we say, ‘all right, for the last three months they've been engaging, they're in employment, no signs of drug use’, we'll probably take them off, because it's important that we keep it fresh, keep bringing those on that really need our scrutiny at that time. Be it positive scrutiny or negative” (Offender Manager 2).

Instead of being due to a decreased, computed risk score, this is the result of professional judgement of the offender’s progress.

The neighbourhood policing function somewhat bridges the gap between the prioritization for enforcement and the prioritization for support. The Neighbourhood Sergeant describes both activities, the prioritization for arrests as well as close cooperation with ‘safeguarding partners’, private rental teams, housing association and street community meetings with a group of agencies. However, his focus are powers instated by the Anti-Social Behaviour, Crime and Policing Act 2014. These powers, an iteration of the Crime and Disorder Act 1998, set limits to individual behaviours and, therefore, are neither supportive nor immediately punitive. He gives an example of their usage:

> “[…] one of our guys who's wreaking havoc in the centre […]. The work went in to getting some form of control over his behaviour and it was only a couple of weeks ago, [a second officer] managed to get a CBO [Criminal Behaviour Order] on him. The new form of ASBO [Anti-Social Behaviour Order]. So that excludes him from the main areas [where he has been] offending. Putting conditions on, really controlling his movements and what he can do, because he was that problematic, he needed that element of control. […] it’s generally orders, injunctions, CBOs, we got community protection notices and warnings that they dish out here like confetti at times, but anything that will just give us a little extra control over their behaviour. […]. So, when somebody is raised as a problem, we look at how to put the work in to stop them being a problem going forward. […] I think [second officer]’s vision is to see him locked up” (Neighbourhood Sergeant).

There are three things to note about this: First, without going into all the details of the legislation, five of the seven powers instated in the 2014 Act are supposed to restrict an individual's actions and prevent so-called anti-social behaviour[39]:

- Civil Injunction:
    - Issued by a County or High Court on conviction for any criminal offence,
    - can include prohibitions and positive requirements,
    - penalty for over 18s is unlimited fine or up to two years in prison for civil contempt of court.
- Criminal Behaviour Order (CBO):
    - Issued by a Criminal Court,
    - can include prohibitions and positive requirements,
    - penalty for over 18s is a fine and/or up to five years in prison,
    - breaching the order constitutes a criminal offence.
- Dispersal Power:
    - Issued by a police officer in uniform or a Police Community Support Officer (PCSO),
    - requires individual to leave an area for up to 48 hours,
    - penalty is a fine and/or up to three months in prison,
    - breaching the order is a criminal offence.
- Community Protection Notice:
    - Issued by police officers, PCSOs and others,
    - can include prohibitions and positive requirements relating to issues like graffiti, rubbish, or noise,
    - penalty is a fine,
    - breaching the notice is a criminal offence.
- Public Spaces Protection Order:
    - Issued by councils after consultation with the police and other agencies,
    - can include restrictions or requirements, or target behaviours of certain groups at certain times,

[39] More detail can be found in the legislation and the statutory guidance (see Home Office, 2017).

  - can also restrict access to public spaces,
  - penalty is a fine,
  - breaching the order is a criminal offence.

While the Neighbourhood Sergeant is unspecific about what the controls on behaviour and movement are, the Crown Prosecution Service's guide to the relevant case law can paint a clearer picture (see Levy and Hall, 2019). Cases that have been approved by the courts institute restrictions on individuals such as prohibiting begging in a specified area, wearing clothing with an attached hood, carrying spray cans in public, being drunk in a public place, associating with or contacting specified individuals, entering a specified area, being in possession of drug paraphernalia, carrying a mobile phone not registered under their own name, entering a list of car parks, congregating with a group of a certain size, carry a knife, being somewhere else than a specified place during a specified time. These are just some of the examples that have been tested in court. What becomes quite clear is that these restrictions can be far reaching.

This leads to the second point to note about the quote above: The Neighbourhood Sergeant is relatively sure that the individual will breach the criminal behaviour order eventually and end up back in prison. The orders lower the evidential threshold and increase the likelihood of arrest for actions that would otherwise be legal. The Sergeant notes that community protection notices and warnings are "dished out like confetti". This suggests that they are used frequently and are easy to obtain. Particularly in a context of resource deprived social services due to the same austerity conditions that motivate the use of risk scores, the use of ASBOs/CBOs as a fast route to re-incarceration confirms some of the fears from when ASBOs were first introduced by Blair's government; namely, ASBOs circumventing prosecution under criminal law through the use of civil law and eroding principles of due process, proportionality, and protections of young people (see e.g. Burney, 2008; Crawford, 2009; Squires, 2008).

There is another application of risk scores which the Chief Inspector mentions, that is ad-hoc intelligence when interacting with an individual. The Chief Inspector describes the use of mobile access to DataVis and its integration into emergency call handling:

> “Yes. They got mobile access, so if they're out and about and they're stopping someone on the street, what is the history of this person? Or going to go to a domestic. Someone sent us some risk factors, what are they? What is this person threat or risk score? Very quickly see there's a warning for weapons, violence. […] I think it does a lot more dynamic risk assessments. Intel cell, headquarters, 24/7 linked in with prompts, so when a job comes in, there immediately at, who is this person” (Chief Inspector)?

Unfortunately, given the functions of officers interviewed here, the interviews do not provide more information on how this ad-hoc information may change officer decision-making. However, as the discussion for the US department suggests, the information held on police databases is a) not neutral and contains errors, and b) becomes part of officers’ discretionary decision-making.

In summary, detectives and tasking unit employ the risk scores to prioritize investigations and arrests, offender managers use them to decide who to prioritize for support as long as this seems fruitful, and in addition to arrest and support, neighbourhood policing prioritizes individuals according to their score for setting limits to their behaviours, and ultimately conditions for their arrest. Given that the different options come with different legal thresholds that have to be met, as well as more general considerations on what measures may support or sufficiently restrict an offender, police officers have to make professional judgements not only on the risk someone poses, as described in the previous section, but also on what actions are appropriate.

Even more so, the offender managers and the Neighbourhood Sergeant describe the timing of effective support as something that can only come from professional judgement.

> “I think there's a lot of support that can be provided, there's a lot that’s available, and it can be really effective, as long as the person is ready. […]. I was in the town centre, probably about three or four weeks back, we saw somebody trying to fill up their housing sheets in the doorway where they were sleeping. It was quite problematic for them, but they were trying, which for us would be an indicator that this person might be at that point where we can do something with them. But then, the next day they might not be. A day after they might be again, you don’t know, but that person, at the moment is still out and about, still doing what they were doing, still causing problems. But there must be something there that is a button that we could press. We just need to try the different things to get them there. I believe in the stuff. I think this is as much about timing as it is about what's available” (Neighbourhood Sergeant).

7.2. Patterns: starting investigations and addressing demand

When it comes to data about what is happening outside of the organisation, risk scores are not the only view DataVis provides. Interviewees mention two more functions of DataVis: filtering available data to generate starting points for investigations and filtering the data to identify major sources of demand to then develop what the officers call ‘problem-solving plans’. Being able to identify starting points for investigations without the assistance of a specialised crime analyst speaks to what officers call the ‘self-service environment’ that DataVis creates. The structural consequences of this are discussed in the next section. Creating ‘problem-solving plans’ from identified sources of demand has consequences for the visibility of workloads within the organisation which will also be addressed in the following section. This section considers the decision making that patterns surfaced through DataVis enable.

DataVis visualises crime trends and locations for officers and provides a whole range of ways to filter crime data to what is of interest to the officer. If officers become aware of a recent crime series in their area, through looking at crime maps or otherwise, they can try and overlay these patterns with other information. For example, the Tasking Coordinator, the Detective Chief Inspector, and one of the offender managers suggest looking at recent prison releases and comparing past areas of activity with the newly occurring crimes. Cases can be filtered further by modus operandi or type of stolen good. One of the offender managers provides an example of this analysis:

> “So, for example, these are all in the last seven days. You might look at this map, and you might think, ‘Well, there is the [motorway]. Is it somebody traveling along the [motorway]? Do we want to start looking at automatic number plate recognition cameras to see is there a common vehicle traveling at the times of these burglaries?’ You might want to see who lives in the area, so you can overlay that map now. You could choose some impact offenders and see where's their home address in relation to those burglaries” (Offender Manager 2).

This analysis does not have to happen within only one type of crime. Based on their knowledge of the individuals involved, the Tasking Coordinator suggests that officers could try and link anti-social behaviours to other crimes like criminal damage. He also demonstrates the ‘Forensic Recovery’ app that displays which crime scenes have been attended and how many forensic recoveries had been made from them. This could help in identifying promising cases for further investigation. All these tools provide basic analytical capabilities to officers across the force.

While one could argue that officers are able to make more informed decisions given the data analysis they have at their fingertips, there may also be some concern that this is replacing local knowledges, especially given the resource constraints that make building local knowledge increasingly difficult. The software’s availability in conjunction with resource constraints somewhat changes the information that goes into professional judgements from local knowledge to patterns in the data. Accordingly, the offender managers see the simplicity of analysing data as a double-edged sword as they fear this to make officers lazy in keeping up with what happens within their remit:

> Offender Manager 2: “What's really important with policing, and I think we've lost it a little bit, I'll be honest, is having local officers in their areas knowing their offenders, knowing the crime times. I showed you those burglaries on the map, a few years ago we had a burglary team, we had somebody that would look at those every day. If we had those burglaries in [this town], he would be able to tell you who was likely to do it. Not from any computer program, but he would look, how did they get in? Was it through the cat flap? What time of day was it? Did they use a car to do the burglary? Did they take a car from the burglary? All of those things. You simply cannot replace human judgment and memory and ability with inanimate control. […]”.
>
> Offender Manager 1: “And I think that's the same for all our agencies as well. We do use that sort of knowledge where people have got a really in-depth understanding and they can almost, you say, feel it in your bones, you know which direction to go. And this makes you lazy to a degree”.

The same patterns used to start criminal investigations can also be used to inform decision making with the goal to reduce demand. The Business Intelligence Manager discusses identifying sources of demand this way,

> “So, these are like the top 20 locations in the force for where calls come in. So, we can visualize them. With these top 20 locations we see how many hours we've […] spent at the scene managing that incident and then add a dramatic costing to that 'cause we know how much a police hour costs” (Business Intelligence Manager).

Officers could include or exclude different types of locations like hospitals, children’s homes, mental health facilities, or retailers. Filtering common locations like hospitals, the Neighbourhood Sergeant explains, could reveal drug addresses or other locations providing another starting point for further investigation. Once a location is identified as causing a lot of demand, officers are asked to create a ‘problem-solving plan’ to reduce this demand. In the case of a retailer, this could mean identifying a duty manager that is more likely to call and having a conversation with them, as the Business Intelligence Manager suggests. Or, as the Tasking Coordinator says, checking if the retailer is employing enough security staff.

A location of high demand is not always associated to a particular premise, it can also be a larger area. The Chief Inspector gives the example of a whole neighbourhood:

> “[This neighbourhood] is an area of social deprivation. It's the highest demand area in the force, things like crime, domestic assaults, domestic abuse for antisocial behaviour. We've historically had lots of problems with children from the ages of eight, nine upwards, where they are just running feral in one of the main areas out there […]. They will press the emergency stop button on buses, which then cues the bus they need an engineer to come […]. They will set fires. They will run into shops and deflect stuff, and run out again, down to a level of kicking footballs in the car park to vex people out. […] Each damage has an incident, but that's just a single thing. What we're looking at is the whole wide picture, so we bring in and associate those instances to a problem-solving plan. […] we're dealing with partner agencies, we've done a lot of work to engage with young people with some of the youth providers, bringing in outside services with the skills” (Chief Inspector).

While this sort of area is less likely to be identified through DataVis – the Chief Inspector refers to there having ‘historically’ been problems –, DataVis is used to register problem-solving plans and, hence, renders the associated workloads visible. This internal visibility of work has organisational consequences discussed in the next chapter.

Analogous to the individual risk scores, patterns that initially cause concern can turn out to be irrelevant. According to the Neighbourhood Sergeant, violence against the person hotspots, while taken very seriously, can be anything from a cluster of low-level public order offences to murder. He is very clear that one would need to understand the detail and context of the information at hand. For example, he would be more concerned about violent offences in public rather than an ongoing private conflict:

> "[senior officers] were concerned about the violence against the person hotspot. 'cause it was flashed up on one of our systems. But it was in a house, between two individuals, but in a house. The two people known to each other. This was being raised to a public meeting as potentially a high-risk issue. Actually, when you looked at it, there was only a couple of incidents. It was just like mad people shouting and screaming coming home drunk. It wasn't actually of any relevance to the wider public. The rest were very behind closed doors. People knowing each other's' issues, so you need to be careful how you use the information, and where you put it as well. It's a very different picture" (Neighbourhood Sergeant).

There is a sense of dissatisfaction with the issue being raised solely based on a high level DataVis score in the Neighbourhood Sergeant's statement above. In that case an issue had been raised without looking further into the data as the Neighbourhood Sergeant would have expected. The following chapter will explore these tensions between different interpretations of the data further.

8. Reshaping the organisation

While the previous chapter explored professional judgement and agency in the context of DataVis's data visualisations regarding what happens outside of the organisation, this chapter turns the gaze inwards, towards the effects that DataVis's introduction has within the police force. In a first step this means looking at how DataVis changes the distribution and use of knowledge within the organisation. The second part of this chapter then focusses on how DataVis institutionalises processes by turning them into a thing, as well as sources of its legitimacy, and the mobilisation of facts as argumentative devices.

8.1. Redistribution of knowledge and pluralisation of decision-making

The introduction of DataVis to the force changes the structure of how information is exchanged, aggregated, and analysed. Whereas before central analysts would look at crime patterns and prepare briefing documents for tasking meetings, now a lot of this analysis has been automated so that the officers themselves can access and analyse the data. As outlined in the previous chapters on the use of DataVis, DataVis's main feature is that it provides a way for officers to access the data at different levels of aggregation (force-wide, within a city or for a specific patrol beat, individual case files) and filtered to specific interests (types of crimes, types of locations, date ranges, etc.). Even more so, it allows officers to seamlessly move between these different aspects of the data. DataVis makes all the steps of the aggregation traceable, which the manual process of writing reports on crime trends or patterns would not allow for. The re-distribution of analysis and decision making from central positions to individual officers using the software leads on the one hand to a changed role for crime analysts, on the other, it means changes in scale: in the amount of different perspectives from which the data is analysed, the amount of data itself that can be analysed, as well as the speed with which it can be checked. It also means that the interpretation of the data happens where officers have knowledge of the instances that are reflected in the data. DataVis automates a lot of the higher-level report writing that aggregates files at different levels. But the increased accessibility of files also means the creation of another type of work: 'data work'. Errors that create skewed risk scores as explored in the previous chapter have to be corrected. This chapter explores these aspects in more detail.

Interviewees referred to the structure of DataVis in terms of “self-service” and “democratising insight”. The Chief Inspector describes how it makes data insights instantly available:

> “Prior to [DataVis] if we wanted any sort of information about crime […] patterns, we'd have to ask an analyst. An analyst would then spend a week or two getting it, they would then send us a picture, which is already a week or two old. We were always chasing our tail; we were always responding after the event. What we quickly identified through DataVis, from its initial use was, okay, this is a great way of, we call it democratizing information. Putting the information in the hands of the people that need it. At a very simple level I can look at my area. I can see instantly what crimes have been reported pretty much up to the minute. In what areas I can map them, I can look at type of offenses, I can look at type of victims I can look at offenders. All that stuff typically has historically been done by analysts, and it'd take a long time, and we'd have to employ resource to do, suddenly we've got it now” (Chief Inspector).

Not only, has DataVis’s introduction sped up the process of aggregating data and identifying patterns, but, as the quote suggests, analysts are a costly resource that previously was not available to everyone.

> “There are still analysts, but to be honest, they’re such a prized resource and there’s not many of them. […]. You’re not gonna get an analyst for all those jobs. There just isn’t enough. You’ll get an analyst probably for every […] big threat-harm-risk job. […] I hate the term self-serve, but that’s what we’re doing” (Detective Chief Inspector).

‘Self-serve’ essentially means that officers take over some of the tasks that analysts held before, now aided by the software. It also means that the analysts’ role is redefined and potentially their number decreased. One of the offender managers brings ‘self-serve’ in context with budget cuts and the Business Intelligence Manager mentions that the analysts’ intelligence function was currently under review and that the technology should allow analysts to take more specialised cases, such as the high threat-harm-risk jobs the Detective Chief Inspector refers to.

"When I do the rounds talking to a police officer, I say everyone's an analyst. You know, it's all of our jobs to interpret the information around us" (Business Intelligence Manager). 'Everyone's an analyst' has two advantages according to the Business Intelligence Manager who stresses this repeatedly throughout the interview: First, it scales.

> "[Other forces] think it should all be just analysts and performance analysts using those tools. So, it doesn't scale out. That performance analyst who's at the centre can only do so much" (Business Intelligence Manager).

Instead the data is interpreted where it is needed. As the Business Intelligence Manager points out,

> "[…] the real killer bit was creating a self-service environment. So not building tools for the privileged few or specialist roles or analysts. Building tools for the people out there who are making the decisions and deploying resources or actually dealing with that risk […]" (Business Intelligence Manager).

Scale also means being able to deal with the amounts of data that would be too much for a small number of analysts. To replicate DataVis's capabilities, the Business Intelligence Manager says,

> "[…] you'd have an army of people trying to make sense of everything. Tens of thousands new pieces of information hit the systems every day. […] These people are moving around, addresses are changing. So, [DataVis]'s kind of doing that automatically" (Business Intelligence Manager).

Second, he argues that, given their local knowledge, the officers are better placed to interpret the data than someone in a central position.

> “They can identify all the issues that need to be prioritised and raised for tasking and all the rest of it. So […], our Chief Constable […] wants all members of staff to be empowered to make the right decisions at the right levels. So, we don’t want for anyone to […] go up all the chains of command […], ‘cause actually that person there, as long as they are informed, they’re going to be the best person to make that decision” (Business Intelligence Manager).

And elsewhere,

> “[the] people who are best placed to know all of that nuance are the people working in those areas day-in day-out, not analysts sat at headquarters, who aren’t connected to that” (Business Intelligence Manager).

The distribution of knowledge to those that have the local knowledge to interpret the data also means that the decision making is pluralised. While the effects of a centralised structure would have been relatively consistent, the ways officers use DataVis can vary, as would the consequences. While the term ‘empowerment’ that the Business Intelligence Manager uses here has the sound of an empty marketing term, section 8.2.2 further below shows how the accessibility of data can to some extent actually have that effect.

The changes in scale brough about by the arrangement described here sit awkwardly with a description as a ‘centre of calculation/translation’ (Callon, 1986; Latour, 1987; Law, 2003) and could perhaps be better referred to as ‘distributed centre of calculation’. On the one hand, DataVis secures flows of incoming information about the periphery. This information is aggregated and automatically produces risk scores according to a centrally produced analysis, as well as pre-programmed standardised visualisations in the form of charts, maps, and tables – what Latour (2005: 175ff) would call an ‘oligoptic’ view. At least in the managerial phantasy, these ‘facts’ would then have automatic consequences like the prioritisation of offenders. On the other hand, this translation into actions is way more complicated, as the previous chapter demonstrated. Crucially, it is dependent on the interpretations of the periphery, thus relocating ‘analysis’ away from the centre and onto the relation between centre and periphery. Although this does not mean that the centre is actually ‘democratised’. Clearly those that define the mechanisms by which risk scores are produced or the way data is displayed exert a different influence than the users. The network is both less asymmetric and more pervasive than centrally performed analysis and instruction. This is also where the structure of DataVis deviates from the scaling assumed for centres of calculation. As Law and Hetherington (2000) note,

> “Knowing at a distance, […] necessarily implies pretty heroic simplifications and reductions. And it therefore also implies pretty heroic manipulations of scale. This means that that which is large in the geographical sense, spread out over time and over space, gets reduced to a report, to a map (and the development of mariners’ maps counts as an exemplary case here) or […] to a set of figures in a spreadsheet” (Law and Hetherington, 2000: 42).

Yet, this scaling typical for the representations produced in centres of calculation[40] is not quite the same in DataVis where detail and abstraction are collocated and transformable into one another via different levels of aggregation allowing for a mixture of logics of interpretation similar to that found in the US case – however, without the epistemological gap between crime numbers and crime accounts. DataVis (and its digital precursors) have replaced a very physical system of paper shuffling.

> “So, going back probably 15 years ago, everything was on paper. So, in events of crime we would record the whole crime on a carbonated piece of paper. All the details, suspects, victims, witnesses, what actually happened, details of property. And that paper would then be pushed around the force, physically” (Offender Manager 2).

[40] See also Latour’s (Latour, 2005: 178) example of Wall Street as ‘centre of calculation’.

Now, officers record crimes and intelligence on laptops and it is instantly available across the system reducing the need for preparing briefing documents by hand. But DataVis brings about and distributes to its users a new kind of work: ‘data work’. Apart from inputting information, the sense-making process involves an element of data maintenance, spotting and fixing errors. The Business Intelligence Manager describes the force’s progress on data quality:

> “[…] important context is that we’ve become so much better nationally as for recording crime correctly. Because we were woeful three, four years ago and some forces still got way to go. We’re a lot better. But what that meant, is for kind of 30 to 40 percent of incidents that were rang into us, didn’t get recorded properly as a crime. And what that means is that people didn’t get linked to an incident, get investigated and have any victim care and all the rest of it. […] we’ve […] probably never been better at capturing that [than now]” (Business Intelligence Manager).

However, while he mentions it as a reassurance to the validity of the risk scores, this data quality has only become relevant given the new accessibility of files. When before it was a slow physical process to retrieve a case file, most data errors were not important, the files would never be retrieved. Now, *every* file not only is retrievable in an instant, but *is* retrieved by the software to calculate a score. If the error influences the score, the software suggests a file to the officer that otherwise would have collected dust in the archive. If a file is brought up it must be dealt with, even if that means amending the error. “[…] if it’s necessary we’ll go back and amend Niche. So that DataVis is reading or providing a more accurate result” (Offender Manager 1). From how the Offender Manager continues this, it becomes clear that having to fix errors at one end motivates stopping errors at the other, i.e. when the data is fed into the system:

> “As, obviously, DataVis is still relatively new, I think it’s about 18 months. As time’s going on, I think people can understand how it’s fed, and how

> important it is to get that initial information right. So, it's getting better and better all the time" (Offender Manager 1).

As the force becomes more and more reliant on DataVis as the system of knowledge vis-à-vis the reductions in officers on the ground given budget cuts, data quality takes an ever more important role. Hence, as mentioned earlier, the Chief Inspector points out that data quality is on the force's 'risk register'. Moreover, data quality becomes a criterium by which officer's performance is (automatically) assessed. "This is now picking up from where there's been errors on Niche. I think this is very picky, very picky" (Offender Manager 2). The next section will return to this aspect.

The focus of this section has been the consequences of the decentralisation of analysis and decision making enabled by DataVis. However, somewhat counter-intuitively, DataVis also enables a retraction out of functions that were concerned with the creation of local knowledges. As discussed in section 7.2, replacing local knowledge with the knowledge created by DataVis is of concern to the offender managers:

> "And I don't want to speak ill of it, 'cause it's a great system, but that would be my biggest concern. Is that we become too orientated on this and we lose a bit of that local knowledge, that local connection with an area. […]. Now we're becoming more centralised, you're losing that local knowledge. That's my opinion. Others might say different" (Offender Manager 1).

The Offender Manager coins this new form of policing based on data insights rather than in-depth local knowledge "faceless policing".

8.2. Power, management, and governance

The obvious way in which DataVis translates power are access rights. While some of this is because not everyone will have clearance for all types of information, some of the access rights are also there because developers make decisions about who ‘needs’ to see what. “[…] this app is for call handler supervisors. Clearly, if I am a police officer in neighbourhood policing, I don’t need to see that, so I don’t. So, there’s an element of governance of who is seeing what” (Business Intelligence Manager). The activated functions in the software premeditate what an officer can know and do.

However, there are less trivial ways in which DataVis makes officers do things, i.e. exerts power. One of these has become quite clear in previous sections: While ‘democratization’ of knowledge has the sound of an equal distribution of powers, the access of every officer to DataVis comes with the responsibility to use it. In the previous section, the Tasking Coordinator sees DataVis as creating a duty to look at the highest scoring offenders, and the Chief Inspector is concerned that one day something that is flagged on the system gets missed by an officer. The Business Intelligence Manager points out that officers, like beat managers, are expected to use DataVis to know about their area and offenders. But as the views of the Tasking Coordinator and the Chief Inspector show, the availability of knowledge creates a double-edged sword where the ability to know can turn into an ability to have known before something went wrong, consequentially resulting in an accountability towards the technology in line with Douglas’ (1992) interpretation of risk referred to in section 7.1. However, as previously discussed, these accountabilities are embedded in organisational power structures such as tasking meetings that provide an organisational mechanism relieving this individual responsibility.

The rest of this section will explore the power relations that emerge from DataVis further. It will first analyse how DataVis stabilises strategies by turning them into a thing and then discuss potential sources of legitimacy for the ‘facts’ DataVis creates and their use as argumentative devices.

8.2.1. Power of DataVis as a thing

A central tenet of actor-network theory is the instance on the inclusion of non-human objects in explaining the stability of social relations over time (Latour, 1990). Based on this premise, this section explores how DataVis stabilises ways of approaching different tasks in the force. As described in the section on risk scores, DataVis makes officers think of risk in terms of the risk scores of offenders or in terms of geographical patterns of crime. This is not to say that officers do not exert discretion in multiple ways, but it institutionalises the threat-harm-risk approach by adding it to the considerations - repeatedly. This section identifies three ways in which DataVis stabilises approaches: 1) the allocation of resources given how it renders priorities and workloads visible, 2) performance management and supervisor discretion, and 3) the structuring of workflows into tasks to be logged on the system. Here, the platform reinforces a kind of data-driven managerialism that relies on the constant surveillance of officer actions and – in establishing DataVis as an 'obligatory point of passage' (Callon, 1986) for the allocation of resources – anticipatory conformity with organisational priorities. As argued in the section 2.2, this configuration is closer to the disciplinary power of a 'surveillant assemblage' (Haggerty and Ericson, 2000) than the data analysis targeting crime. However, far from being only a top-down way of institutionalising procedures, DataVis also re-distributes approaches outside of organisational hierarchies – in analogy to the distribution of knowledge described in the previous section.

1) DataVis makes priorities and workloads visible and thereby informs logics of resource allocation within the organisation. The governance of the tasking process is strongly supported, albeit not determined, by the software: First, the software is used to identify issues, albeit officers can argue for their own. Then, the issues are transferred into 'problem solving plans' and logged in the software. In consequence, tasking is based on these plans and their progress is

tracked. Neighbourhood officers are expected to know about their area. Hence, the officer app shows them aggregated data about the locations of recent crime and their riskiest offenders. Call handlers will see information on open calls, supervisors will see how their officers are performing. According to one of the offender managers, DataVis is informing what people focus on.

> “[The tasking] meeting’s driven by DataVis. So, DataVis is very much highlighting to us where the risk is, either from a suspect or from a victim, or in this particular area, and that’s what’s driving those focus and resources” (Offender Manager 2).

DataVis reifies the force’s threat-harm-risk strategy. In the words of the Chief Inspector:

> “[…] our focus shifted from dealing with priority crime types, we used to have burglary teams, vehicle crime teams. When we had our operating model changes, we decided to go for an approach that assessed every job based on its threshold of risk. We disbanded all those priority crime teams, and then we wanted to look and develop DataVis in terms of looking at threat and risk vulnerability” (Chief Inspector).

The Tasking Coordinator describes how DataVis is used to manage demand in the emergency call centre: A view in DataVis shows how many logs have been created for calls for service, how many of those were active, and how many of them were on backlog. The chief officer in charge would use this information to re-distribute resources across the force to tackle surges in demand. One option to do so would be to move officer out of their back offices if necessary. During the interview, there are 583 open logs and 43% of the previous day’s log have not been dealt with yet. There is a backlog of 10496 incidents. The Tasking Coordinator asserts that the force was unable to deal with the simultaneous increase in calls and budget cuts: “We can’t cope with our demand”. Call handlers would soon have to tell callers that the police would not be able to attend less severe calls. Not only, would the software help monitoring demand live, it would also provide a forecast of expected demand to plan resource allocation accordingly.

Similarly, DataVis helps in the allocation of resources through tasking processes as described in the previous section. For example, if the Chief Inspector responsible for neighbourhood policing cannot carry out a problem-solving plan with the resources at his discretion, he can request additional resources from the headquarters. Every policing area, the Tasking Coordinator explains, produces through briefing meetings assessments of what the main problems and drivers of demand are. These are then put into relation to the force's overall strategic goals, such as fighting child sexual abuse. The ratings and their trends, he continues, are then recorded in DataVis and discussed in force-wide tasking meetings. The use of DataVis in assessing workloads across the force has two consequences: the visibility of demand and workloads becomes important in defending priorities and the way workloads are recorded change the previous balance of workloads between different sections of the force.

There are 55 issues that can be tasked in the software. Anything that falls outside of that scope means busy officers appear idle. The Chief Inspector describes how making neighbourhood policing's workload visible through tasking problem solving plans has allowed them to refocus on some of their core activities.

> "I think for us what's happened with neighbourhood policing is that we had become absorbed really into the patrol function. We were being utilized for the last few years really as a fallback for patrol. When they were too busy everything would come to us. It got to a point actually where we were doing just as much as patrol were, and when you look at the level of our staff compared to patrol […] we were actually doing more. Having synced our data, we realized that things became totally skewed, patrol were tending to deal with some longer-term neighbourhood type jobs. We were dealing with the

> priority jobs and needed to change that around. […] We should go back to the basics of actually building relationships, listening to what the community want, understanding their priorities, tackling those local issues, problem solving rather than being a slave to the radio, which is what we'd become" (Chief Inspector).

He continues by distinguishing the calls for service as 'visible demand' from the 'invisible demand' of engaging with the public.

> "The invisible demand is the sort of stuff that is tying us up with a huge amount of time, you can't see what problem-solving work we're undertaking as neighbourhood officers. […] We're actually working on ways at the moment in which we can try and capture some of that demand. So, within our systems, we would create say, a problem-solving plan" (Chief Inspector).

As soon as the workload becomes visible on the system resources can be defended against requests from higher ranks. DataVis bridges the knowledge between parts of the organisation by providing an 'object' that can be talked about.

> "Developing [DataVis] to show some of the hidden demands and stuff that neighbourhood [policing] are doing, because the only thing that chief officers have looked at for the last four, five years is how many logs are on the screen? 'Right, everyone's got to focus on the logs on the screen'. We've been saying for years, 'No, we're busy'. 'Well, we can't see you're busy'. Now you're going to. That's really useful" (Chief Inspector).

The Tasking Coordinator further underlines the power that recorded and visualised demand has in meetings. He reckons that with DataVis it is not anymore the ones who argue the loudest in a tasking meeting that receive the resources, but those that are backed up with DataVis's numbers describing the gravity of the problem. The next section will return to this power of 'facts'.

Not only unrecorded, but also missing or improperly linked data can render workloads invisible. This in turn drives a process of creating these links. As one of the offender managers describes,

> "So, when DataVis was first implemented, it was very new. Lots of links on Niche were missing. […] if it's not linked, then it looks like we haven't seen them, although we could have done stuff. So, that's where the data quality work and the back to basics work has brought us more up to... So, when you log on to DataVis, now it actually reflects the true picture rather than something that's completely different" (Offender Manager 1).

Altogether, the software coupled with the hierarchical organisational tasking process forces officers to a) find ways of recording their workload, to turn it into visual 'fact', and b) address data errors that cause workloads to be misrepresented. In this way the introduction of the software causes an expanse in the extent and accuracy of data collected.

DataVis stabilises various orderings through controlling the way resources are allocated. In this, it can be regarded as a successful delegation of a strategy to non-human materials ensuring the 'obduracy' of this configuration (Law, 2003: 3f). Particularly the institutionalisation of the 'threat-harm-risk'-approach is an example of this. Simultaneously, the platform affords some flexibility in allowing other priorities, even if they have to comply with the logic of 'problem-solving plans'. The platform thus positions logics of resource allocation as 'obligatory passage points' (Callon, 1999) and reifies them in its pre-conceived logic. Containing these passage points then allows for the monitoring of 'performance' central to the managerialism discussed next.

2) While DataVis is used in the above cases to (re-)allocate resources, it can also be used more directly as a performance monitoring tool for supervisors. All actions on the system are tracked

and officers are held accountable to the data logs of their work. As the Neighbourhood Sergeant describes,

> "All […] they do, all of the crime reporting, the way in which they process stuff, what has and hasn't been done. That's all monitorable through Data-Vis. Where people go, mapping that against priority areas and hot spots, how much time we're spending in priority areas, that's all viewable through Data-Vis. […] how long it's been since the victim has been updated, how long it's been since various things have been reviewed. It's all on DataVis basically" (Neighbourhood Sergeant).

However, the interviewees are clear that this data needs as much interpretation and discretion as the risk scores for offenders:

> "[DataVis] has a useful function as a performance monitoring tool. I don't think it should ever be used as a tool to beat people over the head with, some people do. Some people, you hear them, 'You got X amount of data quality issues, you're failing'. You're busy, you're actually doing a really, really good job. You did a terrific job out on the streets. That, where it's really important" (Chief Inspector).

Similarly, the Neighbourhood Sergeant has

> "[…] heard of people just sending screenshots of DataVis around to their staff to say 'sort out your heads'. And that's about their interaction with DataVis and that's not the way in which it was designed or it's not really the best or most productive value you're going to get out of it" (Neighbourhood Sergeant).

On the contrary, multiple interviewees mention the perception of DataVis as a performance tool as one of the main obstacles in adoption. For example, "[…] it can have a real cultural impact on DataVis, as people see it as the bearer of problems as opposed to helping you" (Neighbourhood Sergeant).

Instead of scolding their staff for issues on DataVis a supervisor would be supposed to initiate a conversation. The Business Intelligence Manager explains,

> “So, if I’m managing 10 PCSOs who are the visible face of police and I can see that […] everyone else has spent 80% of their time over the last two weeks out and about in the community and this individual is being only out 20% of their time, it’s appropriate for me to ask that question? And there might be a very good [reason], you know, ‘I’ve been working on this big, massive problem-solving plan, it’s taken up all my time. It’s appropriate to have that conversation and that the data is being the enabler for that conversation. What’s wrong is if that supervisor doesn’t ask it in a question and in an understanding way and it’s like a ‘I want to see you out [on the street], this is not good enough’” (Business Intelligence Manager).

Moreover, the offender managers and the Detective Chief Inspector are all clear that the recorded data is not all to go by. Similar to the offender risk scores, supervisors decide to overrule the software’s assessment. This may either be because the indicators are dismissed:

> “No. I mean, those crimes that he's dealing with, they are fine. He's not underperforming, he's not making errors out there, or ... They are admin errors. You know, a date might not have been entered in a certain field, or something's not quite reported properly. So, it's down to me now to scrutinize; are things right, what needs to be adjusted, and what we can kinda live with. Like [the other Offender Manager] said, that is not an indication of their performance in the slightest” (Offender Manager 2).

Or they may need further scrutiny. The Detective Chief Inspector explains how DataVis is used to review investigations:

> “It’s where, as supervisors, we believe that the role of a sergeant and the inspector is to, when it comes to major and serious crimes, to review the crime. If you review it regularly with the officer, you do get a better-quality investigation and get a better outcome for the victim. We use it to monitor

> where our work [is], our supervisors, have they done the reviews or not, our victim contact, our suspect management. If you've got a suspect that you haven't arrested yet, it tells you how long that arrest has been outstanding for. […] What we try and use it for is to drive quality" (Detective Chief Inspector).

As becomes apparent from the number of factors that decide the 'quality' of an investigation according to the Detective Chief Inspector, this is difficult to capture in a rating or check mark. Hence, the Detective Chief Inspector stresses the further scrutiny that the software's assessments need.

> "If I'm a sergeant, I put supervisor review, type in my review, save it. Our recording mechanism will say, 'Ah, a review is being done'. What it doesn't say is the quality of that review. I could've written on there 'As last review'. Save. […] Hitting the target rather than missing the point or whatever the expression is. […] I think we've gotta be really careful around quality with DataVis because I think you need the people bit of it as well. You need to read the reviews. You need to see the standard of the reviews" (Detective Chief Inspector).

The consequence of DataVis's records can thus be mediated by the supervisors, although it will not always be.

One of the scores produced by DataVis is a 'demand score' that has a purpose similar to the offender risk scores. It weighs an officer's cases by their associated risk and seeks to prevent burn-out:

> "[…] So, like same as the harm score, we can actually see that this officer is carrying a more complex workload. So, the sergeant can select on them, can get a good feel for what this individual is carrying […]. […] this is a patrol officer, so not a specialist investigator, they got some really nasty crimes they're investigating. Hence, they are popping out as a high-complex. […]

> the supervisors can see the teams at an individual level as well to best support them. 'Cause what we know is that officers don't always put their hands up saying that ‘I'm drowning’. What you'll see it's probably service deterioration happens and then that officer has got welfare, go off on stress or something like that. […] we've built a burn-out model. We're identifying members of staff that are at highest risk of going off on a long-term stress related sickness. So, the areas are using that, working with their HR managers to try and get upstream […] or to support before that worst case happens” (Business Intelligence Manager).

While the Business Intelligence Manager describes the score here as being used in a similar discretionary fashion as the other participants described the use of other measures before, the demand score has the interesting property of being aggregated for different levels of the organisation. The more the values get aggregated, that is the higher the rank of the officer looking at them, the less likely it seems that they are used as pointers to individual files and the more likely it becomes that they are regarded as facts. It has to remain open at this point to what degree that leads to misperceptions at higher levels and subsequent arguments around the validity of the scores – especially where crimes may be categorised the same way but require different investigatory effort.

3) While the discussion so far revolved around how DataVis pre-structures processes by reifying the force’s threat-harm-risk strategy (highlighting persons and locations) and performance management, it is worth noting that at a more granular level the software is structuring workflows and nudging officers to complete tasks logged on the system. It visualizes tasks:

> “[…] they can see their property tasks more visible. Are they getting rid of property or returning it back or destroying it and things like that. Are their tasks on Niche? Are they getting through them? Is there any there that they haven’t done? It’s about that efficiency” (Detective Chief Inspector).

One of the offender managers shows his colleague’s account which has 53 data quality errors; errors that officers may be held accountable for, although he reckons that many of them would be old crimes with no current relevance. However, as one of the offender managers points out, it is not the supervisor alone that creates pressure to address these issues. The software itself has an effect:

> “Ultimately, we all strive to be good at what we do. I think it's built into our genetics to do that, so when you see your data quality's less than 50%, or you got 59% or whatever, you want to put that right, but sometimes that's like you said, it's not really relevant” (Offender Manager 1).

The Tasking Coordinator highlights that DataVis visualizes intelligence gaps for every person on the system and prompts users to fill information such as known vehicles (driver or owner), associations with others, locations, phone numbers and other intelligence. Together with what the Offender Manager says, it is quite clear how the software’s design by itself drives the collection and processing of information.

Given the three examples of how DataVis supports the maintenance of approaches above, does the power structure described here mean that the software is solely used to enforce a strategy top-down? The relations are certainly more complex than this. While the Business Intelligence Manager mentions that the central element, the risk scores, was a decision by the Chief Constable, other tasks and visualisations are the result of officers at lower levels requesting them. The Chief Inspector speaks highly of the flexibility that is involved:

> “After 29 years of policing, I've finally got something, a computer product that I like, that is helpful. Everything else seems to work against what we're trying to do, but this is the one thing that actually seems to be trying to give us the right stuff, and it's quite flexible. […] the parameters it works in are not tightly defined. We can manipulate it. I can go to [the Business

> Intelligence Manager] and I can say, '[…], this is what I want, how can you get it?' […] 'Yes, I can bring that information. How do you want it presented?' 'Well, actually what would be useful to me is as if it'd have this information.' 'Yes, I can do that for you'. Actually, it's not just the computer saying this is what you want, this is how you'll have it. […] it's based upon what practitioners want. I would say a good 50-75% of those apps have been developed as a result of what people on the ground have said. That I really like, and I think that's what makes it rhyme with people" (Chief Inspector).

Consequentially, the software is reifying, and therefore stabilizing, approaches from various parts of the force and distributes them to organisational equivalents. If a neighbourhood policing officer in one beat has an idea for a data visualization, this can lead to another officer taking up the same approach through the software. In this sense, the software is harmonizing approaches. The Business Intelligence Manager believes that only by fulfilling functions for the officers using DataVis it gets adopted:

> "[…] inventing things that no one wants. Like we're not in the business of inventing things, we're in the business of solving business problems and business is a key to that. As soon as you forget that, and don't involve [...], you know it's not gonna work" (Business Intelligence Manager).

This practicality of DataVis is one of its sources of legitimacy discussed in the next section.

8.2.2. Power of facts

As mentioned before, the Tasking Coordinator is of the opinion that DataVis would replace officer's 'knee-jerk' assessments and the Chief Inspector refers to it as 'putting a little bit of science into that', although not 'absolute science'. The Tasking Coordinator also speaks of the offender management app providing a "so to say scientific score" for risk. Interestingly, the Tasking Coordinator chooses yet another formulation. He says that "DataVis factualises the issues" (Tasking Coordinator). DataVis does something. DataVis turns issues into facts. It lends the issues an authority that the ‘knee-jerk’ assessments did not have. Perhaps only the Tasking Coordinator and the Chief Inspector spoke of DataVis in terms of science because the numbers appear more as facts from central parts of the organisation. However, given the small number of interviews this cannot be answered definitively. Yet, the Business Intelligence Manager underlines the Tasking Coordinator’s argument: “So that’s the massive benefit here […], having a data-literate workforce that are operationally connected to reality, kind of real what’s going on” (Business Intelligence Manager). The scaling described in section 8.1 functions as a source of legitimacy for DataVis where every connection is traceable to the data that was entered. Given the awkward fit with a description of DataVis as a ‘centre of calculation/translation’ in the same section, this section considers some of the sources of its legitimacy reflected in statements contrasting its use with ‘knee-jerk’ assessments and then shows how this legitimacy is translated into uses of its outputs as argumentative device. These sources of legitimacy may explain why the information displayed by DataVis drives the co-construction of knowledge found in section 7.1.

Facts are complicated assemblies. Unsurprisingly, several interviewees struggle in explaining the technical details of what the software does. “I don’t know how *all* these algorithms work” (Tasking Coordinator). “Then, this is the one you’d have to talk to the real clever people about” (Offender Manager 2). Or, “I don’t know. I think it’s a combination of various things in terms of the history and things like that. That’s why you need to be cautious around [individual scores], because it may throw up Joe Blocks with a huge score” (Detective Chief Inspector). This is not to say that they do not have an abstract understanding of what the software is supposed to do and what some of the criteria are that it takes into account. But the technicalities are opaque, if not considered irrelevant. Irrelevant also because, as discussed earlier and apparent from the Detective Chief Inspector's quote, the scores are considered suggestions, the software's opinion so to say, the underlying case files constitute the 'facts'.

It is somewhat puzzling how DataVis is at the same time 'connected to reality' while its 'facts' can be dismissed based on various grounds as described previously. Perhaps, this is a source of strength; the facts are never absolute as they never hide their origin and their origin – individual case files – can serve as a basis for discussion. DataVis also provides 'facts' of different kinds: The risk scores are probabilistic measures, while crime trends and workloads are based on counts. So, it is unlikely that every 'fact' will have the same weight. Apart from DataVis' connection to 'reality', legitimacy may come from a series of factors: 1) As discussed above, apps on DataVis are based on what officers thought would be useful for their work. Being based on what officers do rather than an imagination of what they should do, as well as displaying the information they request, probably helps DataVis's legitimacy. The Detective Chief Inspector, for example, describes how DataVis helped in identifying the perpetrator of a random stabbing captured on CCTV because it brought up a similar case from 20 years ago.

> "We would not have been able to have done that a year ago. […] The one where the person got stabbed in the neck, that came about from DataVis. That wasn't a public appeal. That was desktop, 'I think that's, him, or it is him. Let's go and arrest him', and he was arrested within an hour" (Detective Chief Inspector).

Part of the software's usability and hence legitimacy may also come from the quality of its visualisations.

> "In my police service, I've seen lots of bits of technology come and lots of bits of technology go. Hand on heart, without a shadow of a doubt, this is probably the best bit of just even the way it presents the data, the way you can use it, this is by far the best that the police have come up with I've seen.

> I know we didn't make it, but without a shadow of a doubt” (Detective Chief Inspector).

2) In a similar fashion, usefulness is demonstrated in cases where the software correctly and unexpectedly suggests a person of interest before they commit a crime. The Detective Chief Inspector tells the story of stalker that was shown as escalating in risk and who later broke into the stalked person’s house. The Tasking Coordinator tells the story of a person rated high risk who later stabbed someone, as well as of an offender with a high risk of domestic violence who then tried to run over his family with a car. These cases of surprise build trust in the software’s capability to surface the right individuals. 3) For the Business Intelligence Manager, as one of the staff developing DataVis’s capabilities, trust comes from testing it.

> “So, we will train our models with a target set. […] So, we can tell, we know the accuracy, we know the precision, recall. So, we won’t let a model leave the desktop if we’re not happy that it’s being able to predict accurately what we want to” (Business Intelligence Manager).

Beyond the quantitative measures of predictive accuracy built into these methods, the predictions would also be reviewed by officers:

> “And of course, we test it. Right, ok, these people that are popping out as high risk, are these the right people? Great, it may look good on a desktop modelled thing, so we got our intel unit to test like loads of these outputs and they were pretty happy with it” (Business Intelligence Manager).

4) Whether it is the Cambridge Harm Index mentioned by the Neighbourhood Sergeant that supports a strategy based on quantifying harm rather than solely counting crimes, or one of the offender managers explaining that the harm weightings are based on home office figures, or, as the Business Intelligence Manager points out, the risk scores being modelled after the

probation system’s OGRS scores: Outside institutions provide legitimacy to the processes and calculations used inside.

Officers can use data held on DataVis as argumentative device, that is, use it to convince others. This is to an extent possible because of the legitimacy that is ascribed to it by the above mechanisms. Data can be used to legitimate one’s work. The offender managers, for example, use risk scores to defend their work with acquisitive offenders that does not constitute a statutory duty. As one of the offender managers explains,

> “[with] inquisitive criminals, so the shoplifters, we don’t have to do offender management with them, but we work in a way to try and break those cycles. So, we have to justify to various people why we do that” (Offender Manager 1).

The risk scores and their underlying data analysis is used as an argumentative device in arguing for the necessity of a task.

Recording tasks associated to problem solving plans and thereby rendering ‘invisible demand’ visible shifts the allocation of resources between different policing functions. It is therefore unsurprising that the measurement of performance through DataVis incentivises an expansion of recording practices as discussed above. The offender managers mention that they “[…] struggle with this work particularly to give performance evidence of success, because we don’t want to work with the ones more successful [….]” (Offender Manager 1). Hence, they created a new scoring system.

> “We’ve created a new system now to try and give us a bit of a measurement tool. So, every two weeks, the offender managers will score [the offenders] on a scale of one to five for each of those pathways. So, on one extreme, they might be homeless, and then you go through the sliding scale. Homeless to

> hostel to supported housing, until you get to the end, being in their own place" (Offender Manager 2).

While potentially useful for the task itself, the scales allow for a quantification of the officers' performance.

New data also means new discussions to be had. The Chief Inspector mentions the introduction of staff surveys through DataVis, which consequentially offer material for arguing political position within the force.

> "[…] this estate is absolutely awful because they've crammed everyone on one floor, and you got two floors that are unused. Now I've got a bit where I can build a business case and I can say, 'Well, look at the staff survey, this is what officers said'" (Chief Inspector).

An open question is if the different nature of the 'facts' created by DataVis have different effects on the negotiations that take place. As noted in relation to the visibility of workloads, aggregation means making individual cases computable by categorizing them and, hence, making them count equally. It is unclear what effects this has without observational data from tasking meetings. However, at the very least, it means that officers working at lower levels and possessing local knowledge will be pressed to either agree or challenge the knowledge that higher ranking officers in central positions will gain about their area from looking at DataVis. The Neighbourhood Sergeant became convinced of DataVis's capabilities because it was able to give him a picture of the local situation before going there.

> "We could then do a lot of the research from our place, from headquarters, around their issues, around what was affecting stuff. To be able to then go out and start have conversations about what's affecting them. […] so, it shows how much you could do in advance of trying dealing with an issue" (Neighbourhood Sergeant).

The software can bridge knowledges between different parts of the organization. But what happens when this picture and the local perception collide? And, what happens when the officers' experience is supplemented with data because there is not enough funding for neighbourhood policing anymore?

8.3. Discussion

Taking the two previous chapters together, the analysis offered by the UK case study demonstrates how DataVis straddles a position between the standardization and harmonization of approaches through a unified approach to assessing risk and features like the automated detection of data quality issues, and the simultaneous pluralisation of decision-making by making analysis tools widely available and providing the flexibility of aggregations that are traceable down to the underlying files. The redistribution of knowledge within this 'distributed centre of calculation' allows for a multiplication of viewpoints from which data is interpreted, an increase in the use of data analysis previously reserved to specialist functions, an acceleration in producing calculative knowledge, new insights from integrated data sources, and the interpretation of data by those who have relevant tacit knowledge.

On the one hand, risk scores institutionalise the force's 'risk-threat-harm' strategy by requiring justification in relation to which scores are or are not acted upon. Similarly, the recording of workloads on DataVis becomes a self-reinforcing process in which officers seek for ways to render their workload visible. Data becomes an argumentative device used in convincing superiors of existing workload or the need of allocating more resources in an area. This raises questions for future research on what arguments can and cannot be made where data gains these political powers. DataVis also implicates the supervisor-officer relation in ensuring officers adhere to workflows and complete data input, otherwise issues are automatically flagged and presented to supervisors. Where it does not draw on hierarchical relations, the information on DataVis gains legitimacy from a range of sources, including its usefulness in supporting everyday work, surprising and ‘correct’ risk assessments, statistical testing in the development of risk models, and similar methods of quantifying risk used in outside institutions.

On the other hand, the use of DataVis is not techno-deterministic. Rather it enables an interplay between tacit and calculative knowledge, allowing for professional judgement based on analysis officers can carry out themselves. The risk scores, although designed to manage uncertainty, create new uncertainties in questions of who on the list needs to be dealt with, what the consequences are of ignoring a risk rating, and a new necessity to prevent and correct data errors which otherwise become part of the scores. The empirical analysis in chapter 7 demonstrates that risk is better described as the outcome of a process of co-construction rather than an ‘objective’ score determined by the software and enacted by the officer. Risk is produced in a complex process which involves a) officers checking underlying case files where the software brings someone unexpected to their attention and, where necessary, correcting underlying errors in the database, b) officers asserting their own priorities either in how they pre-filter the listed offenders, or in including individuals that are not ranked highly by the algorithm, and c) officers dynamically deciding whether and how they can act regarding a risk score, what resources are available and how they may need to be reallocated when someone ceases to be deemed risky. This co-construction of risk is different from the imagined, biased, and deterministic automated decision-making that for example O’Neil (2016) associates with ‘weapons of math destruction’. Instead of a singular approach, the risk scores are part of pluralised decision making. Nonetheless, attention on the risk scores themselves points to the need of transparency around the encoded normativity of ‘harm’ that shapes the politics of prioritisation, as well as to the risk rating’s indifference to the individual being suspect or convicted offender.

Given the results from the US department, further research is also needed on the consequences of files being readily accessible.

The actions officers take based on risk assessments range from enforcement to support. The frame for this approach is determined by the UK’s Anti-Social Behaviour, Crime and Policing Act 2014 and the associated relations with social services in so-called multi-agency public protection arrangements. Cuts to social services under the austerity regime instated by David Cameron’s Conservative government raise two critical questions for further research and debate: a) where social services are unable to provide offenders with essential support, does police tend towards enforcement via CBOs as the only viable option? And b) should risk scores and professional risk assessments determine who receives support? Particularly on this last question Harcourt’s (2007) elasticity argument would suggest that such an approach would merely help police cope with the issue but fail to address underlying social problems and only result in ever new individuals at the top of the risk ranking. The combination of austerity with risk ratings brings to the fore the normative decisions police organisations (and consequentially individual officers) must make in prioritising among offenders, victims, and crimes. As one of the offender managers stresses,

> “We have to do the things that are gonna make the difference, and there's quite a lot of them that believe moving forward police won't be able to do [those], generally. And there are other forces. There's forces that don't manage low-risk sex offenders. We choose to manage all of our sex offenders. So that there's lots of things happening, where [we have] to compete with the high demands that we're faced with” (Offender Manager 1).

Finally, DataVis enables officers to explore patterns in the data to generate starting points for investigations (such as identifying possibly connected burglaries by modus operandi and location) and identify sources of demand to be addressed in ‘problem-solving plans’. In the context of budget cuts, this ability to diagnose problems at a distance, possibly without the necessity for detailed tacit knowledge especially given the easy access to case files, spurs concerns of a centralisation of policing and what one of the interviewees calls ‘faceless policing’ (for Scotland and the Netherlands, Terpstra et al. (2019) describe this trend as ‘abstract policing’).

9. Discussion and conclusion

Policing has seen and still sees a push to digitize and datafy everything aiming for increases in efficiency, to render the organisation governable, and to increase clarity and coherence within the myriad of data that police collects. But in this process, new conflicts and uncertainties arise – an infrastructure for data collection must be built and maintained, numerical 'facts' need to be interpreted, technologies break down, discretionary decisions are complicated, and technologies have unforeseen outcomes in practice. This thesis contributes a rare, empirical counterweight to techno-deterministic and largely theoretical accounts of technology in policing. While the breadth of issues covered allows for a holistic view of digital technologies in policing and their interactions across different organisational sections, this means that this research can often only scratch at the surface of the variations of human-technology interactions that would become visible in studies focussed on singular technologies. However, from this emerges a research program that takes the practice of technologies in policing seriously.

This section will discuss the main findings from the UK and US case studies in the context of the theoretical framing introduced in chapter 2 and it will locate them in the wider context of the discourse on technologies in policing. The discussion addresses the collection of data, its use in strategy meetings, the use of digital technologies in everyday policing from frontline to investigations, and the use of data for oversight. Finally, it discusses practical considerations for both research and police agencies that follow from this research.

9.1. The politics of collecting data

The Latin word 'data' translates as 'givens' (or 'given things'). The word, as much as the day to day usage of it, renders opaque where these givens come from – who gives them? Rather, as Kitchin (2014b) suggests, data should be thought of as 'capta' ('things taken') to highlight the underlying careful selection of information encoding human biases and subjectivities. As the previous chapters (particularly sections 4.1 and 5.3) demonstrate for the police, the production and processing of data implicate the whole organisation: from officers and detectives filling forms, to analysts shaping the digital infrastructure for the whole process, to senior officers communicating their data interpretations as strategy. This section foregrounds the politics of integrating data, the affordances of electronic forms mobilised for timely data collection, the work of cleaning data, the close link between data use and the underlying categorisations, and the duration data needs to consolidate. It thus relates to how the production of representations in 'centres of calculation' (Latour, 1987) is organised and maintained while highlighting the messiness of parallel efforts for the US case.

The collection of data requires a considerable amount of politics: people must be convinced to enter information in a predefined way and existing datasets must be integrated. While a lot of these processes had already become invisible in the UK police force, the work of the analysts in the US department demonstrates this clearly. Here, analysts, first driven by the consent decree's requirement of data collection for oversight and later by the function creep of this data collection having turned out useful for operational purposes, seek to continually integrate new sources of data previously held in separate databases. For this purpose, analysts often have to negotiate with external agencies such as the sheriff's department under which conditions access is possible. Whether due to political animosities or the cost of setting up new systems, these efforts are not always fruitful. While this may be expected for inter-agency data exchange, analysts also have difficulty integrating the department's own databases with the consequence that sometimes only workarounds such as scripts continually copying information from one database to the other solved the issues. Making existing databases interoperable is certainly not as smooth a process as implied in the 'surveillant assemblage' (Haggerty and Ericson, 2000).

While there is existing research highlighting problems of inter-agency information sharing (Boba et al., 2009; Sanders and Henderson, 2013; Taylor and Russell, 2012), information exchange is frequently framed as opening opportunities and the potential safeguards these practical restrictions pose against data misuse need further attention.

Not only the integration of existing data but the input of new data itself must be organised. In both case studies, the bulk of the data collection stems from officers and detectives filling forms, recording body-worn camera video, collecting CCTV recordings, writing warrants for data from social media and phone companies, and more. Some of this data is fed directly into databases accessible to most in the department, while other information is held in separate files for investigations. To solicit the contributions from officers, the design of the database makes use of the affordances of electronic forms. These pre-structure the kind of information that can be entered and can thus render information immediately available. However, while electronic forms aim at ensuring the completeness of data through mandatory fields (and to some extent a feature for accountability that would, for example, check if all conditions for a lawful stop had been met), flaws in their implementation at times make filling them take time. Thus, organisationally they accelerate the availability of information while in individual instances they may take longer to complete. This especially becomes a problem where technologies malfunction, like in the case of automated dashcam video recordings that cause a recording deluge with officers having to label videos as ‘non-event’. As much as the affordances of electronic forms provide control over what can be input in fields (e.g. not allowing letters in the field for date of birth) and allow editing of mistakes, information will always be entered wrongfully. In the US department, this means that analysts spend considerable time cleaning data and, at the time of the research, developing scripts to catch misspellings of names to unify records. It also means that search results will not always be accurate so that officers and detectives must try multiple spellings to find all records on the database. Errors also exist in the UK police force's database, but here users can correct any errors they spot thereby distributing 'data work' and improving data quality over time. Both the existence of errors in the data and the duration of filling forms are crucial factors in officer decision making discussed further below.

Perhaps most surprisingly, different districts in the US department maintain their own, parallel crime statistics. This further highlights the fragmentation of these systems as opposed to a unified 'surveillant assemblage' (Haggerty and Ericson, 2000). These idiosyncrasies in counting crime are a result of a) the centrally used categorisation system of crimes not matching with the information district commanders strategic decision making (e.g. misdemeanour arrests including so-called 'catch-and-release' arrests) and b) the timing between a crime recorded on the database and it appearing in the crime statistics causing confusion (i.e. officers know of crimes that are not yet in the statistics). While nationally the uniform crime reports prepared by the FBI have a contested history part of which concerns the categories used (Maltz, 1977), it stands out that within the same department different counting systems are used. Whereas crime statistics are regularly discussed in their relation to (the manipulation of) public discourse on rising or falling crime rates (e.g. Maguire and McVie, 2017; Seidman and Couzens, 1974), this highlights the importance ascribed to crime statistics for management purposes as well as the close relationship between how crime is counted and the use these counts are put to. Moreover, the time it takes for crime counts to consolidate – because of, among other reasons, unfounded calls, multiple calls for the same incident, reports that have to be written and reviewed, and crimes being reported late – calls into question the logic of 'real-time' forecasting of crime in predictive policing[41].

[41] In addition to the duration of the bureaucratic process of registering a crime, the exact time of an incident is also often unknown.

9.2. Strategy and the entanglement of knowledges

This section interrogates the entanglement of quantitative knowledge and experiential knowledge in strategic decision making. It returns to this question within the frames of 'bi-opower' (Foucault, 2009) and 'centres of calculation/translation' (Callon, 1986; Latour, 1987; Law, 2003) introduced in more detail in the literature review (chapter 2). It highlights the role of data analysis as an argumentative device with its implicit superiority over tacit knowledge. It further problematizes the influence of underlying categorizations and the time it takes for data to consolidate in contrast with the 'objectivity' associated with data.

The design of the data platforms in the two case studies allows in principle[42] for completely different approaches to crime statistics. In both cases, crime statistics are available to anyone in the organisation. However, the platform used by the US department allows seeing crime counts arranged by predefined categories such as crime types and districts, while the one in the UK allows officers to 'drill down' into aggregated data and identify the underlying casefiles. This connection between individual cases and crime statistics is opaque in the US department. Consequentially, in the UK anyone has the capability to detect patterns in the data and suggest 'problem-solving plans', while the connection of crime counts to knowledge of the underlying cases is only available to district commanders in the US who rely on officers reporting the details. Thus, while both platforms could be considered as 'centres of calculation' (Latour, 1987), the configuration in the UK is also markedly different. In decentralising the view that a 'centre of calculation' affords, the UK police force tasks the periphery with the analysis while simultaneously pre-structuring the analysis with the logics of individual risk and allocation of

[42] Whether these capabilities are employed by other users than the subset of 'superusers' interviewed in the UK is unclear.

resources to ‘problem-solving plans’. Yet, pre-structuring does not imply determination as the multitude of other priorities mobilised by officers in section 7.1 on the interpretation of risk scores demonstrates. Here, digital technologies transform the star-like shape[43] of the ‘centre of calculation’ (Latour, 1987) into something new. This difference highlights the importance of detailed studies like the one carried out here in examining the features of new technological systems in policing. In the UK police force, coinciding efforts to centralize policing functions to save money because of financial pressures in the context of austerity politics and interviewees’ fear of this leading to ‘faceless policing’ relying more on data than tacit knowledge[44], do not take away from the platform’s capability to pluralise decision making – or ‘democratize insight’ as the slogan goes – but stresses the need for non-techno-deterministic approaches to studying police technology in practice.

One of the main questions raised in the literature review (chapter 2) is how the statistical knowledge of crime associated with ‘biopower’ (Foucault, 2003, 2009, 2010) is translated into actions and how this translation interacts with officers’ experiential knowledge. The use of quantitative data requires interpretation, first in its reading (what constitutes, for example, a cluster of crimes) and then in its translation into action. This is because the categorization necessary to count has to eliminate information from the individual case to equate those within the same category. The loss in detail is compensated with the emergence of counts that indicate the frequency of these categories (e.g. types of crime) and patterns in these frequencies (e.g. spatial clusters of crimes). This creates an epistemological gap between an epistemology of *crime* (knowing crime through numbers) and an epistemology of *crimes* (knowing detailed accounts of individual incidents of crimes). This gap is particularly apparent in the US

[43] See Latour (2005: 177).

[44] Calling it ‘Abstract Police’, Terpstra et al. (2019) identify a similar tendency in the Netherlands and Scotland.

department’s CompStat style meetings where district commanders starting from the position of crime numbers come together with sergeants who know of the underlying cases (see section 4.2). Where individual crimes drive priorities, the resulting actions are clear: investigation and, where leads exist, sending out patrols to look out for people or cars. The centre of calculation follows a command and control structure (see chapter 2). What actions to take based on crime counts is not as clear. In the US department a mixture of addressing the patterns as patterns, that is ordering increased patrols wherever more crimes happen and tasking detectives to solve crimes that recently increased (the ‘aggregation and reaction’ structure), and addressing patterns by looking for underlying factors, that is reintroducing the tacit knowledge of crime in the district to differentiate ‘random’ crimes from crimes that could constitute a series committed by the same actors (the ‘attributing causes’ structure). Solely addressing quantitative crime patterns with increases in patrol leads to territorial policing that the department aims to avoid because the resulting ‘jump-out work’, as officers called it, had been harmful to community relations and central to the consent decree. Given the short sentences associated with this strategy, it is also deemed ineffective by some. The problem here is that, without other knowledges, officers have no further instructions than to be in an area and so they search for (minor) infractions that have no relation to the reason they are there. Instructions to patrol certain areas are not well communicated to frontline officers who also regularly do not know where assigned areas are. This observation fits well with Benbouzid’s (2019) argument that predictive policing is first and foremost a managerial tool which seeks to solve exactly these issues. It also stresses that the managerial ideal of how the organisation is supposed to function and the resulting practice diverge, and in consequence the influence of ‘biopower’ becomes less direct. Instead, officers know what to look out for and in which areas when it is communicated more horizontally by detectives. However, in parts of the organisation this does not happen because detectives rely on officers receiving this information through a ‘be-on-the-lookout’-email-system that produces an information overload with irrelevant information (see section 4.3.3). Yet, the possibility to improve the system to distribute messages only to relevant recipients, a task force's use of a chat app for updates on investigations, and the ability to investigate the case files that make up the crime statistics in the UK police force, suggest that technology can not only support strategies based on crime statistics but also those based on a jointly produced experiential knowledge of crimes.

Whether territorial policing or the more targeted policing based on accounts of the individual crimes, the logic of policing here follows a simple model of stimulus-response – what Manning (2008) has described as the 'reactivity theme' of policing. There are no deeper questions on why crimes happen. Rather, police react to spikes in crime rates (whether arbitrary or for a reason) with patrol for deterrence, or targeted investigation and arrest of perpetrators. While surely the same strategies exist for the UK police department, the data analysis allows for another logic of dealing with crime. Here, patterns of crime are addressed with 'problem-solving plans', some of which seek to look beyond the perpetrators and seek for reasons in the social environment. That is, police liaise with social services on how to address some of the conditions believed to cause problems[45]. Thus the larger biopolitical question of how to govern crime as a statistical phenomenon – a question that is closely related to the 'aetiology crisis' in criminology (Matthews, 2014; Young, 1997) – shapes the availability of different possible reactions that police can have towards the occurrence of a crime (or crimes) and towards offenders. Deterrence and addressing the social conditions of crime can be clearly associated with the logic of 'security' identified by Foucault (2009). In this framework crime only receives special attention when the numbers increase more than 'normal', and the solutions aim at changing the

[45] While not focussed at living conditions, a similar logic of identifying 'causes' to crime exist in the field of environmental criminology. For example, an element of risk terrain modelling may be modifying the built-up environment (e.g. lighting) to reduce crime (Caplan and Kennedy, 2011).

conditions under which perpetrators act to reduce the possibility of crimes. Yet, the translation of crime numbers via tacit knowledge of the individual crimes into targeted actions also points to a new perspective: not only do diverse mechanisms of power coexist (Foucault, 2009: 21f), the priorities deduced from statistical knowledge of a population (of crime) can also be translated into actions that do not target the population and reduction in risk but that target individuals. In policing practice not only the mechanisms but also the logics of governmentality are entangled – or, in the vocabulary of Law's (1994) *Organizing Modernity*, plural, incomplete, and interacting orderings form a complex and messy social world.

What perhaps stands out more than the entanglement of different knowledge practices are the ways numbers link with power relations. In the US department, the ritual of weekly CompStat meetings with their display of hierarchy maintains the importance of these numbers. But perhaps more importantly, the comparison of crime statistics between districts that is enshrined in the visualisations and tables on the department's dashboard suggests a competition in which commanders compare their districts' 'performance'. The numbers get assigned a high degree of importance exemplified by a lieutenant who recites the current week's numbers by heart. Even if strategies for the week are decided based on detailed knowledge of the crimes that occurred, rises in crime numbers focus the attention on those types of crime that are more frequent. However, this is not a completely deterministic relation as variation between commanders exist. Importantly, the necessity for the 'objective' crime statistics to be interpreted affords moments of subjectivity in which decreases in crime are attributed to past police action while increases are unfortunate events independent of police action.

This function of data analysis as an argumentative device is, in a different fashion, also prevalent in the UK police force. Here, the development of new data sources is set to become a self-perpetuating process in which officers use data analysis to give weight to their 'problem-solving plans' and to make their own workloads visible to senior officers. Further, ethnographic research of tasking meetings would be necessary to identify to what degree arguments receive more weight if they are supported by data analysis. Similarly, this thesis argues that the risk scores reify the force's 'threat-harm-risk' strategy towards dealing with those offenders causing the biggest share of incidents. The prominence of the risk scores is a constant reminder of this logic of prioritisation and further research will need to identify the degree to which the responsibility to use risk scores creates a new professional risk where an officer decides not to act on them (often because of other constraints or priorities, see section 7.1.2).

Whether in the form of weekly crime counts or as individualised risk ratings, numbers are performative and exert a specific influence on how police prioritise the allocation of different resources from investigations to patrol. For this reason, the particularities of this quantitative knowledge need to be problematized. As mentioned above, crime data needs time to consolidate and different preferences for categorizations exist. The issue of timing means that decisions taken on very recent data not only regularly chase random noise in the data (Wheeler, 2016), but also introduce an element of uncertainty to the reality of the patterns that are addressed. This second issue alone requires qualitative knowledge of crimes to identify those recorded incidents that may have turned out not to be crimes. The focus on crime categories creates another problem, highlighted by a detective in the US department: while the categorization of crimes may render patterns and trends within these categories visible, patterns across the categories (which are part of officers' tacit knowledge) are rendered invisible. The connection between guns stolen from glove boxes and armed robberies would not be discussed in a violent crime meeting because there only the latter are relevant. This can become a problem for the police's capability to investigate crimes when detectives' role descriptions become equally compartmentalised into investigating only certain types of crime. Finally, the categorization necessary for counting at times renders equitable what is not equitable. This issue is prevalent where the same indicators of officer 'productivity' are applied to officers with different sets of tasks. This is further discussed in the section on oversight below.

9.3. Digital technologies in practice

This section discusses three distinct areas in which this thesis contributes new perspectives through the analysis of rare empirical data on the uses of technologies in police practice. It starts with the role of breakdowns in fragmenting practice but also creating a new technological practice that forms a complementary process to the top-down adoption of new technologies. It then outlines a non-deterministic perspective on the role of databases in discretionary decision-making in the US department and describes the co-construction of risk in the UK. Finally, it draws attention to the interpretation of data in investigations and the various spatio-temporal affordances of digital technologies that transform investigatory practices.

9.3.1. Breakdown and the fragmentation of technological practice

Techno-deterministic accounts of technologies in policing have no space for the breakdowns of technologies and subsequent fragmentations of practice resulting from individual workarounds to the problems officers are faced with. Yet this is a recurrent theme throughout the US case study and the mere fact that the UK case is based on interviews with 'superusers' suggests different degrees of adoption. Simultaneously, access to technologies is unevenly distributed across the US department due to restrictions to roles, access through personal connections, limited software licenses, different affinities for technology and varying degrees of training. This section discusses the consequences of breakdowns, the workarounds officers find, and how breakdowns can become productive.

A simple consequence of breakdown, especially where there are no workarounds, can be distrust and disuse. For example, officers reverted to the paper versions of forms recording attended incidents because of a story of an officer having been held accountable to missing forms which were lost due to a server error[46]. In a different type of breakdown – a breakdown of the organisational context required for the use of the technology – license plate readers fitted to patrol cars are not used because those driving the vehicle are tasked with answering calls for service with little time to recover stolen cars or learn how to use the technology. However, more than the plain disuse of technology, technologies would be used by some while others would create their own workarounds. These range from the use of private phones for group chats, photos, and navigation to general-purpose tools like Excel and Google Drive, but also include non-digital technologies such as paper forms, push-pin walls, and direct communication via radio or in person. Apart from resulting concerns for data safety, the makeshift character of some of these solutions causes other problems such as officers driving with a phone for navigation or increased radio traffic for communications that duplicate existing but malfunctioning systems. Workarounds can also be seen as demonstrating the need for updates and new technologies. What might become visible here is a process in which the use, breakdown, and repair of technologies in practice drive the change and adoption of police technologies rather than the top-down process of providing new technology and forcing adoption. This is one of the ways in which breakdowns can be productive. Another way lies in fostering a healthy amount of scepticism towards the data contained in police databases. Where search results repeatedly include unrelated persons, officers check carefully before acting on the information. Lastly, officers can also use breakdowns creatively to their advantage. This happens where

[46] The story had consequences – perhaps because of other experiences with the (un)reliability of the system –, although it did not include the full truth of additional factors that led to the officer’s sanctioning.

officers seat suspects in the car during rain to wait for a warrant to be verified allowing them to carry out a pat-down[47]. Thus, breakdowns inform the development and adoption of technologies, they mediate the trust put into data systems and their ’objectivity’, and they sometimes allow for creative uses in practice.

9.3.2. Discretionary decision-making

This work empirically and conceptually contributes to the existing literature on discretionary decision making. As discussed in the literature review (see section 2.3.1), the literature has focussed mostly on human factors of discretion, proponents and opponents of new technologies like predictive policing provide mostly techno-deterministic views of the relationship between officers and technology, and even the insightful works of Brayne and Christin (2020) and Sandhu and Fussey (2020) adopt a perspective in which machine and officer decision are set up to compete. While the managerial aspect of area-based predictive policing may provide such an adversarial relationship, the individualised risk scoring studied here suggests rather a co-construction of risk in which officers add their own interpretations and priorities[48]. Moreover, viewing discretion as a socio-technical network in which technologies have non-deterministic affordances renders the influences that longer-existing digital technologies like databases have on officer decision making visible. Here, the human factors commonly associated with suspicion formation (stereotypes, known persons and locations, incongruencies, and nonverbal

[47] The underlying interpretation of department policy is contentious among officers.

[48] There are indications that such a perspective of co-construction would also be productive for area based predictive policing. Not only would it include the possibility for rejection as discussed by Brayne & Christin (2020), and Sandhu & Fussey (2020), but it also includes the possibility that officers use patrol instructions to ‘discover’ new areas and build their experiential knowledge as observed by Ratcliffe et al. (2019) (in addition to rejection). The degrees between these variants point to the varying power differentials that are possible in predictive policing implementations from direct orders to a decision aid. Thus, as argued in section 2.3.1, adopting a perspective in which discretion is a power-infused, socio-technical network allows to empirically study this power variance in different configurations.

clues, see Johnson and Morgan, 2013) are extended by an element of digital congruency in which stories and observations have to match the database and mismatches have to be explained. This study also provides unique insight into the moral questions officers deal with when enforcing laws – coupled with the information on historical violations accessible through the database. This raises the question of what data should be available to officers. The following discusses first the findings regarding the database's role in decisions to engage and the outcomes of interactions and then addresses the co-construction of risk in the use of individualized risk scores.

Technologies increasingly play a role in prompting officer engagements with the public. Examples of this are the proliferation of automated number plate recognition, tests of live facial recognition[49], or predictive policing solutions that predicate where and with who officers engage. None of these alert-based systems exist in the US department (the number plate recognition is only used for investigations). Consequentially the contrast with these technologies renders the timing by which technology comes into play visible. Only after the 'human' factors of suspicion have caused an initial interest, officers can perhaps search the license plate, or, more commonly, upon a stop do a routine search for the stopped individual and look for outstanding warrants, paid car insurance, and validity of driver's license. In these cases, the database contains clear instructions for the officer which force discretion on questions such as whether to write a ticket. Without the knowledge held on the database, there is no decision to make, the database creates discretion. Sometimes the information on the database may conflict with a person's story or the officer's observation. When this happens, the database forces discretion on trust and a drive towards resolving the discrepancy. The other way around, the database can

[49] For early research on live facial recognition see Fussey & Murray (2019).

match a story and decrease suspicion. Just as incongruency is one of the ‘human’ reasons for suspicion formation, officers seek digital congruency, a matching of reality and database. Thus, this research demonstrates that digitally held information is crucial to the discretionary decision-making during stops.

When it comes to deciding on whether to hand out a ticket, officers weigh the fairness and effectivity of the penalty. Officers for instance would think twice where they sense financial hardship as the reason for fraudulent license plates or problems in the maintenance of a car. However, this considerable degree of compassion afforded by officers is complicated where databases provide a record of previous stops that resulted in warnings instead of fines. Further research will need to identify to what degree this information pushes officers towards enforcement. This issue situates police officers as an important buffer between the law and its potentially socially unjust consequences – a function of discretion highlighted by Pepinsky (1984). While in this instance opinions may vary on whether officers should or should not have this role and whether the database’s suggestion to act is problematic, another point of influence further problematizes officers’ access to an archive of past police encounters: what if previous attributions of guilt bias present ones so that officers do not further enquire? Past encounters made accessible during moments of discretion have the potential to enable a technologically mediated form of what Young (1977) termed ‘deviancy amplification’.

The UK police force’s use of risk scores for individuals, as analysed in section 7.1, is a clear example of the need to go beyond techno-deterministic descriptions of officers’ interactions with technology. Officers do not just enact the risk scores. Instead, in a process of co-construction of risk, officers filter the listed individuals according to their own priorities (e.g. by area or type of crime), review ‘surprising’ risk ratings tracing the algorithm’s ‘reasoning’ and correcting underlying errors in the database, add their own list of offenders based on experiential knowledge, and, importantly, have to decide how many of the top offenders receive attention, for how long, and in what ways. For the last question, more than the risk rating, conditions of austerity influence whether officers choose supportive measures like housing and drug programs or rely on powers like Criminal Behaviour Orders to seek fast (re-)imprisonment of offenders. While the exact factors and weightings that go into the risk ratings are opaque to officers, the correlational logic of the algorithm does not, as authors like Chan & Bennett Moses (2016) fear, lead to the disappearance of causation as it is reintroduced by officers seeking reasons in the underlying files to explain unexpectedly high-risk ratings. If risk is *co*-constructed, what then is the influence of risk ratings? First, the algorithm sometimes surfaces names that officers are not aware of and thus prompts engagement in a radically new way. While this property is supposed to reduce risk overall (cases are processed that otherwise would not gain attention and lead to future incidents), it introduces a new professional risk in needing to justify why someone on the list does not receive attention (and has not received attention in the case of a future incident). In the perspective of Mary Douglas (1992): they allow for the allocation of blame. This leads to the second and perhaps main influence of risk scores which is more about organisational priorities than risk: they institutionalise a strategy focussed on individuals and the encoded priorities for different types of crime – what the institution calls a ‘threat-harm-risk’-approach. Senior officers can ask for justifications in relation to the risk scores. This also highlights that in supporting the power of these tools factors outside the mere ‘objectivity’ of quantitative knowledge evoked in much of the literature on this topic are important. Risk scores are embedded in hierarchical communications, they gain legitimacy from their practicality, from surprises that turn out to be correct, from predictive accuracy scores during development, and from other authorities, like in this case the Home Office, using similar approaches.

9.3.3. Digital technologies in investigatory practice

This section highlights some of the affordances of technologies in shaping the spatio-temporal conditions of investigatory practice. Continuing with the theme of the previous section it first outlines the influences of data on decision-making before showcasing how technologies shift what information is available to investigators and, finally, what temporal affordances these technologies have in enabling looks into the past but also competing for officer time. Many of these affordances can only come into effect because these technologies have become 'obligatory passage points' (Callon, 1999) indispensable to the problem of solving criminal cases. Covering a wide range of technologies relevant to investigations, this thesis provides a unique perspective on the use of technologies in investigations and contributes coordinates for future research.

Like the risk scores described above, investigators collocate data with other sources of information to interpret it. Perhaps more so than officers who accept information logged onto the police databases as fact, detectives stress the need for verifying information. An example of the need for combining different knowledges is the interpretation of phone records which detectives insist requires detailed knowledge of the case. This is despite concerns for the time this analysis takes because of the vast amounts of unfiltered data received through warrants. Furthermore, detectives not only interpret data but also consider the future use of this data in court. This is, for example, reflected in concerns of misinterpretation of social network graphs as established connections as opposed to mere co-occurrences in the database. The 'facts' do not speak for themselves. Interestingly, the concern for possible interpretations can lead detectives to think about possible ways to curate this data for prosecution by avoiding collecting all information. In child sexual abuse investigations screenshots could, for instance, be preferable to a 'phone dump' potentially including the victim's own nude pictures which, so the detectives' concern, could be used by the defence to question the victim’s character. Thus, contrary to the common perception of police trying to collect all data possible, it becomes a double-edged sword that is not only useful to investigations but can overwhelm the investigation in its amount and allow an undesired defence in court.

The previous sections have already discussed the new visibility that data bring about: risk scores bring attention to some individuals that would otherwise not have received police attention. This also includes the prioritisation of proactive investigations of incidents associated with ‘risky’ individuals. Similarly, the spatio-temporal crime patterns discussed above not only drive strategies from area-based patrol to problem-solving plans, but they can also reveal patterns relevant for investigations (for example burglaries along the main motorway indicating how the burglars operate).

More radically than showing crime patterns on maps, the underlying database now gives detectives access to a large body of frontline knowledge routinely recorded in field information cards (FICs) during stops for eventual future use. This accessibility of the past is also central to the sensor networks of license plate readers and surveillance cameras. What all these new visibilities have in common is the central role of space: the ‘management’ of individuals is organised along a spatial differentiation of responsibility (e.g. neighbourhood teams), the patterns come into view by mapping incidents spatially, the information recorded on police databases reflects the spatial presence of police and patrol strategies based on spatial clusters of crime, the surveillance cameras concentrate surveillance activity on a limited set of spaces where cameras are installed with officers waiting for something to happen within their view, and the license plate readers segment the city by setting up virtual borders recording every entry and exit by car. The spatiality permeating daily police patrols and surveillance infrastructure thus not only informs potential feedback loops in predictive policing (Lum and Isaac,

2016) but possibly also influences the success of investigations – an aspect that needs to be studied further. This is particularly relevant because it may provoke tensions with concerns of over-policing which usually disregard investigations.

One data source for investigations is social media. Although commonly referred to in spatial metaphors, one of the challenges for proactively working task force officers is to link information on social media such as photos to places for potential further physical surveillance. While the analytical category of space may not be very productive here, social media creates a new space of visibility employed by both criminals and police. It is a space in which crimes are facilitated (as in gun sales through Instagram chats) and where criminals maintain their street credibility in a semi-public environment (e.g. posting pictures with guns). In reviewing the use of social media in investigatory practices, section 6.6 highlights the tension existing between the discoverability of otherwise invisible crimes online and the danger of 'fishing expeditions' where officers can access information that is publicly visible as well as through fake accounts without needing to apply for a warrant. This thesis provides rare empirical data on the use of social media in investigations and by highlighting this tension sets up debate on the regulation of this practice. The National Police Chief's Council's guidance for police in the UK, for instance, proposes a definition of levels of engagement from browsing to sustained contact through fake accounts which relate to levels of required training and oversight (Egawhary, 2019).

The empirical analysis in this thesis addresses two temporal aspects of the use of technologies in policing: 1) as mentioned above sensor networks, but also the bureaucratic apparatus of recording information in forms, record the present for eventual future use. They function as what Waterton (2010) calls 'epistemic time machines'. Digital technologies have allowed for an expanse in the amount of data routinely recorded and the subsequent accessibility of this past through search tools (however flawed they may still be). This at first sight perhaps trivial mechanism transforms investigations in supplying new forms of evidence where previously detectives could only rely on witness statements. Body-worn cameras, for example, can make responding officers' experience available to detectives with an amount of detail that written reports could never achieve. Beyond the frequently discussed concerns for privacy and proportionality of state surveillance in relation to these technologies (e.g. see Ferguson, 2017b; Merola and Lum, 2012; Miller, 2014; Newell, 2013), this research highlights ethical concerns that come from the use of this data in investigations: On the one hand, evidence, like information collected from social media, can make a witness statement unnecessary for prosecution. This can reduce the burden the legal process places on the victim, especially in cases like child sexual abuse. On the other hand, recorded information may allow investigation and prosecution where the victim changes their mind on pressing charges leaving investigators with the decision of whether to use previously recorded statements to continue with the case, nonetheless. 2) Technologies are regularly discussed in their time-saving potentials for police work (Koper and Lum, 2019; Lum et al., 2017), which can certainly be the case as in the example of electronic warrants that relieve officers of needing to drive and see the judge in person. Similarly, 'artificial intelligence'-based software for video analysis can speed up the review of video footage considerably. Yet, this research shows that the direction is not as unidirectional: Instead of an acceleration, technology can complicate and slow down processes. This happens, for example, in the long search necessary to recover 'be-on-the-lookout'-emails when needed, in the time consuming coding of phone records, or just during the plain breakdown of computer systems that need to be rebooted. Moreover, technology use not only impacts the duration of tasks, but officers also have to subscribe to the technologies' inherent rhythms. Data on social media may be deleted after a fixed amount of time and officers thus must prioritise writing a warrant to other tasks, surveillance on social media requires staying up to date to retain the potential to act in the physical world, and video recordings periodically overwrite because of storage limitations setting a time window for detectives to retrieve footage from a crime scene. The temporal affordances of technologies in policing revealed here may easily go unnoticed in day-to-day practice but, for future research, raise the question of how detectives' time is best allocated.

9.4. Indeterminacy of oversight through data

The technological monitoring through data and its goal of anticipatory conformity are, as outlined in the literature review (section 2.2), central elements to many accounts of data-driven managerialism (e.g. Beer, 2016; Espeland and Sauder, 2007; Muller, 2018; Power, 1997) – a managerialism that also features in Feeley & Simon's (1992) 'actuarial justice' thesis. This section discusses the empirical insights from sections 4.4 and 8.2 focusing on the use of data in compliance and workload monitoring. Mirroring previous sections above, the data do not stand for itself but need interpretation and the categorizations that underly counts pose problems of comparability. Again, this work contributes a more nuanced perspective on the role of data in police decision-making going beyond techno-deterministic accounts.

Compliance management is an important aspect of data collection in the US department and central to its fulfilment of the consent decree. Here, digitization allows for the centralisation of review and the ranked judgement of districts enables competition on compliance. For example, the compliance department scores body-worn camera footage from stops and reviews the justifications for officer actions given in reports. Where problems are identified the solutions are in direct connection with the data and misconduct can be addressed. This example sets a counterpoint to the largely negative perspectives on the use of scores in management. However, it contrasts with an attempt of employing normalization[50] – identifying those for intervention that deviate from the statistical average – to guide managerial attention. In the US department officers are compared against departmental averages for measures such as numbers of arrests or uses of force. But the underlying categorizations equate officers in very different roles which causes supervisors to question their value. The normal distribution fails to create a norm. Instead, supervisors rely on their direct interactions with officers. In the UK police force, a similar phenomenon of numbers equating disparate functions that police officers fill is apparent in the measuring of workloads. Although a similar reliance on personal connections exists here too, the system allows for the flexibility of officers recording and adding previously unrecognized workloads. Thus, not every data-driven system for oversight has the same consequences. The ones discussed here showcase changes in behaviour, preference for tacit knowledge, and changes in recording input.

9.5. Critical considerations

This final section highlights four concerns arising from this research that are relevant for further research and police departments. These are related to the role of categorization, the temporal affordances of digital technologies, the limits of data use, and the context of austerity.

First, the work that categories do and the consequences they have, both in the collection of crime data and in monitoring work, needs attention in practice and future research. Crime statistics are a powerful tool for identifying patterns and adjusting strategies, but they can also draw attention to spurious ‘trends’ and render connections between crimes invisible (especially where crime types are used to functionally separate roles in the department). Thus, a challenge

[50] In *Security, Territory, Population*, Foucault (2009: 72ff) distinguishes this biopolitical *normalization* with regard to a normal distribution from disciplinary *normation* through training in accordance with a pre-defined norm.

for police departments is to ensure that officers' experiential knowledge finds a way into strategic meetings as a critical backdrop for the interpretation of crime data and that senior officers know how to analyse crime statistics. Nourishing this experiential knowledge also means ensuring exchange between different (often hierarchically organised) roles like between detectives and patrol officers. Choosing a design for data visualisation that allows examining underlying case files, like in the UK police force studied here, can also enable a stronger engagement with crime statistics. For accountability and oversight, measuring the degree of compliance with policy in officers' actions seems to be a more promising approach than comparing officer 'productivity' based on contentious categorisations of work roles.

Second, digital technologies not only make work more efficient but can similarly slow work down. This can be deployed strategically, as in paperwork that regulates the amount of stops officers are willing to make, or slow speed for license plate reader updates preventing car chases. But it can also happen by accident (as in the recording deluge associated with automated camera activations) and, for lack of training, software tools, or personal preferences, may significantly impact workloads (as in the case of detectives manually sifting phone records). Research needs to pay attention to these temporal affordances of technologies in policing and police departments need to be conscious of how technology use can impact, for instance, time budgets of investigations whether in allocating more time for certain investigations, improving training in the use of digital tools, or monitoring unintended consequences and breakdowns.

Third, beyond questions of privacy, bias, and feedback loops raised in the discourse on predictive policing, this research raises more fundamental questions of whether data should be used for the purposes that it is being put to. Under which circumstances should body-worn camera video replace witness statements, should patrol officers have access to records of past police encounters where it is not relevant to their safety, how should officers make use of social media for investigations, should police records of cases that do not lead to convictions be part of risk ratings? Clear policies addressing the conditions for accessing and using data including the requirements of oversight and warrants are necessary to address these questions and engage with positions critical of the police as well as give guidance to officers.

Last but not least, allocation of resources for policing has been at the heart of the ‘efficiency in times of austerity’ argument for predictive policing (see e.g. Beck and McCue, 2009) and, more recently, become a topic of public debate in the context of calls for defunding the police in the wake of the Black Lives Matter movement (see e.g. Sharkey, 2020; Thompson, 2020; Vitale, 2017; Yglesias, 2020). While much of this debate is American, it largely resonates with concerns in the UK case discussed here. Risk scores introduced to focus police activity to reduce future ‘demand’ only highlight those cases that are not prioritised. Most importantly, the analysis underpinning risk scores can reveal the failures of social services caused by years of austerity politics which now appear as ‘risk factors’. As much as officers might prefer supportive measures of rehabilitation, under these conditions seeking enforcement and arrest may be the only option they see. In the face of housing problems and a mental health crisis, of poverty and racial segregation, police could use the same analysis to point to the larger social issues. In some places these issues could be addressed with reducing oversized police budgets; in others, police budgets are already too stretched to bring justice to victims of crime.

These considerations demonstrate the value detailed empirical research can bring not only to scientific understandings of technology in policing but also in contributing to practical considerations within police departments and the wider societal discourse on the limits of police power. This thesis reveals the multifaceted nature of technology in policing, its affordances in practice and governance, and provides a theoretical vocabulary for future studies of technology in policing.

10. References

ACLU (2013) *You Are Being Tracked. How License Plate Readers Are Being Used To Record Americans' Movements*. July. New York: American Civil Liberties Union.

Amoore L and Piotukh V (2015) Life beyond big data: governing with little analytics. *Economy and Society* 44(3): 341–366. DOI: 10.1080/03085147.2015.1043793.

Asdal K (2011) The office: The weakness of numbers and the production of non-authority. *Accounting, Organizations and Society* 36(1): 1–9. DOI: 10.1016/j.aos.2011.01.001.

Ashworth A and Zedner L (2008) Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure, and Sanctions. *Criminal Law and Philosophy* 2(1): 21–51. DOI: 10.1007/s11572-007-9033-2.

Ashworth A and Zedner L (2014) *Preventive Justice*. First edition. Oxford monographs on criminal law and justice. Oxford, United Kingdom: Oxford University Press.

Baker K (2010) More Harm than Good? The Language of Public Protection: More Harm than Good? The Language of Public Protection. *The Howard Journal of Criminal Justice* 49(1): 42–53. DOI: 10.1111/j.1468-2311.2009.00596.x.

BBC News (2017) Avon and Somerset Police 'at tipping point'. *BBC News*, 19 September. Bristol. Available at: https://www.bbc.com/news/av/uk-england-bristol-41319548 (accessed 27 September 2020).

Beck C and McCue C (2009) Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession? *The Police Chief* LXXVI(11).

Beck U (1992) *Risk Society: Towards a New Modernity*. Theory, culture & society. London ; Newbury Park, Calif: Sage Publications.

Becker HS (2014) *What About Mozart? What About Murder?: Reasoning From Cases*. Chicago: University of Chicago Press.

Beer D (2016) *Metric Power*. Palgrave Macmillan UK. DOI: 10.1057/978-1-137-55649-3.

Benbouzid B (2019) To predict and to manage. Predictive policing in the United States. *Big Data & Society* 6(1): 2053951719861703. DOI: 10.1177/2053951719861703.

Benjamin R (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*. John Wiley & Sons.

Berk R (2013) Algorithmic criminology. *Security Informatics* 2(1): 1. DOI: https://doi.org/10.1186/2190-8532-2-5.

Bialik C (2016) How To Make Sense Of Conflicting, Confusing And Misleading Crime Statistics. In: *FiveThirtyEight*. Available at: https://fivethirtyeight.com/features/how-to-make-sense-of-conflicting-confusing-and-misleading-crime-statistics/ (accessed 22 June 2019).

Blumstein A and Moitra S (1980) The Identification of “Career Criminals” from “Chronic Offenders” in a Cohort. *Law & Policy* 2(3): 321–334. DOI: 10.1111/j.1467-9930.1980.tb00219.x.

Blumstein A, Cohen J, Roth JA, et al. (eds) (1986) *Criminal Careers and ‘Career Criminals’*. National Academy Press.

Boba R, Weisburd D and Meeker JW (2009) The Limits of Regional Data Sharing and Regional Problem Solving: Observations From the East Valley, CA COMPASS Initiative. *Police Quarterly* 12(1): 22–41. DOI: 10.1177/1098611107309279.

Bottoms AE (1977) Reflections on the Renaissance of Dangerousness. *Howard Journal of Penology and Crime Prevention* 16(2): 70–96.

Bottoms AE and Brownsword R (1982) The Dangerousness Debate After the Floud Report. *The British Journal of Criminology* 22(3). Oxford Academic: 229–254. DOI: 10.1093/oxfordjournals.bjc.a047310.

Bowker GC and Star SL (1999) *Sorting Things Out: Classification and Its Consequences*. MIT Press.

Bowling B (1999) The rise and fall of New York murder: zero tolerance or crack’s decline? *British Journal of Criminology* 39(4): 531–554. DOI: 10.1093/bjc/39.4.531.

boyd danah and Crawford K (2012) Critical Questions for Big Data. *Information, Communication & Society* 15(5): 662–679. DOI: 10.1080/1369118X.2012.678878.

Braga AA (2014) Problem-Oriented Policing. *Encyclopedia of Criminology and Criminal Justice* Bruinsma G and Weisburd D (eds). New York: Springer.

Brantingham PJ, Valasik M and Mohler GO (2018) Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial. *Statistics and Public Policy* 5(1): 1–6. DOI: 10.1080/2330443X.2018.1438940.

Brayne S (2017) Big Data Surveillance: The Case of Policing. *American Sociological Review* 82(5): 977–1008. DOI: 10.1177/0003122417725865.

Brayne S and Christin A (2020) Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social Problems*: 1–17. DOI: 10.1093/socpro/spaa004.

Brown KJ (2020) Punitive reform and the cultural life of punishment: Moving from the ASBO to its successors. *Punishment & Society* 22(1). SAGE Publications: 90–107. DOI: 10.1177/1462474519831347.

Burney E (2008) The ASBO and the shift to punishment. In: Squires P (ed.) *ASBO Nation: The Criminalisation of Nuisance*. Bristol: Bristol University Press, p. 15.

Callon M (1986) The Sociology of an Actor-Network: The Case of the Electric Vehicle. In: Callon M, Law J, and Rip A (eds) *Mapping the Dynamics of Science and Technology*. London: Palgrave Macmillan UK, pp. 19–34. DOI: 10.1007/978-1-349-07408-2.

Callon M (1999) Some Elements of a Sociology of Translation. Domestication of the Scallops and the Fishermen of St. Brieuc Bay. In: Biagioli M (ed.) *The Science Studies Reader*. New York: Routledge, pp. 67–83.

Caplan JM and Kennedy LW (2011) *Risk Terrain Modeling Compendium*. Newark, NJ: Rutgers Center on Public Security.

Carrabine E, Cox P, Fussey P, et al. (2014) *Criminology: A Sociological Introduction*. Third edition. Abingdon: Routledge.

Chan J and Bennett Moses L (2016) Is Big Data challenging criminology? *Theoretical Criminology* 20(1): 21–39. DOI: 10.1177/1362480615586614.

Cheliotis LK (2006) How iron is the iron cage of new penology?: The role of human agency in the implementation of criminal justice policy. *Punishment & Society* 8(3): 313–340. DOI: 10.1177/1462474506064700.

Chen M, Mao S and Liu Y (2014) Big Data: A Survey. *Mob. Netw. Appl.* 19(2): 171–209. DOI: 10.1007/s11036-013-0489-0.

Christin A (2020) The ethnographer and the algorithm: beyond the black box. *Theory and Society*. DOI: 10.1007/s11186-020-09411-3.

Cohen J (1983) Incapacitation as a Strategy for Crime Control: Possibilities and Pitfalls. *Crime and Justice* 5. The University of Chicago Press: 1–84. DOI: 10.1086/449093.

Conrad JP (1982) The Quandary of Dangerousness. *The British Journal of Criminology* 22(3): 255–267. DOI: 10.1093/oxfordjournals.bjc.a047311.

Côté-Boucher K (2018) Of "old" and "new" ways: Generations, border control and the temporality of security. *Theoretical Criminology* 22(2). SAGE Publications Ltd: 149–168. DOI: 10.1177/1362480617690800.

Crawford A (2009) Governing Through Anti-social Behaviour. Regulatory Challenges to Criminal Justice. *The British Journal of Criminology* 49(6). Oxford Academic: 810–831. DOI: 10.1093/bjc/azp041.

Davis KC (1969) *Discretionary Justice. A Preliminary Inquiry*. Champaign, IL: University of Illinois Press.

de Maillard J and Savage SP (2012) Comparing performance: the development of police performance management in France and Britain. *Policing and Society* 22(4): 363–383. DOI: 10.1080/10439463.2012.718777.

Deflem M and Chicoine C (2014) History of Technology in Policing. In: Bruinsma G and Weisburd D (eds) *Encyclopedia of Criminology and Criminal Justice*. New York, NY: Springer, pp. 2269–2277.

Deleuze G (1992) Postscript on the Societies of Control. *October* 59: 3–7.

Deleuze G and Guattari F (1987) *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.

DeLisi M (2005) *Career Criminals in Society*. Thousand Oaks, CA: SAGE Publications.

Denis J and Pontille D (2019) Why do maintenance and repair matter? In: Blok A, Farías I, and Roberts C (eds) *The Routledge Companion to Actor-Network Theory*. 1st ed. Routledge, pp. 283–293. DOI: 10.4324/9781315111667-31.

Derrida J (1998) *Archive Fever: A Freudian Impression*. Chicago, IL: University of Chicago Press.

Di Ronco A and Peršak N (2014) Regulation of incivilities in the UK, Italy and Belgium: Courts as potential safeguards against legislative vagueness and excessive use of penalising powers? *International Journal of Law, Crime and Justice* 42(4): 340–365. DOI: 10.1016/j.ijlcj.2014.04.001.

Díaz Á and Levinson-Waldman R (2020) Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use | Brennan Center for Justice. Available at: https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations (accessed 29 September 2020).

Dodd V (2019) Criminals going unpunished because of cuts, says police chief. *The Guardian*, 1 May. Available at: https://www.theguardian.com/uk-news/2019/may/02/criminals-going-unpunished-because-of-cuts-says-police-chief (accessed 27 September 2020).

Dodson L (2009) *The Moral Underground: How Ordinary Americans Subvert an Unfair Economy*. New York: The New Press.

Donoghue J (2008) Antisocial Behaviour Orders (ASBOs) in Britain: Contextualizing Risk and Reflexive Modernization. *Sociology* 42(2). SAGE Publications Ltd: 337–355. DOI: 10.1177/0038038507087357.

Donoghue JC (2012) Anti-Social Behaviour, Community Engagement and the Judicial Role in England and Wales. *British Journal of Criminology* 52(3): 591–610. DOI: 10.1093/bjc/azr079.

Douglas M (1992) *Risk and Blame: Essays in Cultural Theory*. London and New York: Routledge.

Dworkin D (1977) *Taking Rights Seriously*. London ; New York: Bloomsbury.

Dymond A (2019) Towards a socio-technical understanding of discretion: a case study of Taser and police use of force. *Policing and Society* 0(0). Routledge: 1–15. DOI: 10.1080/10439463.2019.1660338.

Eck J and Weisburd DL (2015) Crime Places in Crime Theory. Rochester, NY: Social Science Research Network.

Eck JE and Maguire ER (2005) Have changes in policing reduced violent crime?: An assessment of the evidence. In: Blumstein A and Wallman J (eds) *The Crime Drop in America, Revised Edition*. Cambridge: Cambridge University Press, pp. 207–265.

Economic and Social Research Council (2015) ESRC Framework for Research Ethics. Available at: https://esrc.ukri.org/files/funding/guidance-for-applicants/esrc-framework-for-research-ethics-2015/.

Egawhary EM (2019) The Surveillance Dimensions of the Use of Social Media by UK Police Forces. *Surveillance & Society* 17(1/2): 89–104. DOI: 10.24908/ss.v17i1/2.12916.

Egbert S (2018) About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany. *European Journal for Security Research*: 1–20. DOI: 10.1007/s41125-017-0027-3.

Egbert S (2019) Predictive Policing and the Platformization of Police Work. *Surveillance & Society* 17(1/2): 83–88. DOI: 10.24908/ss.v17i1/2.12920.

Elden S (2007) Governmentality, Calculation, Territory. *Environment and Planning D: Society and Space* 25(3). SAGE Publications Ltd STM: 562–580. DOI: 10.1068/d428t.

Ensign D, Friedler SA, Neville S, et al. (2018) Runaway Feedback Loops in Predictive Policing. In: *arXiv:1706.09847 [cs, stat]*, 2018, pp. 1–12. Proceedings of Machine Learning Research. Available at: http://arxiv.org/abs/1706.09847 (accessed 20 February 2019).

Ericson RV (1982) *Reproducing Order: A Study of Police Patrol Work*. Canadian studies in criminology 5. Toronto ; Buffalo: Published in association with the Centre of Criminology, University of Toronto by University of Toronto Press.

Ericson RV and Haggerty KD (1997) *Policing the Risk Society*. Clarendon studies in criminology. Oxford: Clarendon Press.

Espeland WN and Sauder M (2007) Rankings and Reactivity: How Public Measures Recreate Social Worlds. *American Journal of Sociology* 113(1): 1–40. DOI: 10.1086/517897.

Espeland WN and Stevens ML (2008) A Sociology of Quantification. *European Journal of Sociology* 49(03): 401. DOI: 10.1017/S0003975609000150.

Eubanks V (2018) *Automating Inequality*. New York, NY: St Martin’s Press.

Evans T and Harris J (2004) Street-Level Bureaucracy, Social Work and the (Exaggerated) Death of Discretion. *The British Journal of Social Work* 34(6). Oxford Academic: 871–895. DOI: 10.1093/bjsw/bch106.

Falk Ö, Wallinius M, Lundström S, et al. (2014) The 1 % of the population accountable for 63 % of all violent crime convictions. *Social Psychiatry and Psychiatric Epidemiology* 49(4): 559–571. DOI: 10.1007/s00127-013-0783-y.

Farivar C (2014) Due to license plate reader error, cop approaches innocent man, weapon in hand. Available at: https://arstechnica.com/tech-policy/2014/04/due-to-license-plate-reader-error-cop-approaches-innocent-man-weapon-in-hand/ (accessed 18 April 2020).

Fassin D (2017) Ethnographying the Police. In: Fassin D (ed.) *Writing the World of Policing: The Difference Ethnography Makes*. Chicago ; London: University of Chicago Press, pp. 1–32. DOI: 10.7208/chicago/9780226497785.001.0001.

Feeley MM and Simon J (1992) The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology* 30(4): 449–474.

Feeley MM and Simon J (1994) Actuarial Justice: The Emerging New Criminal Law. In: Nelken D (ed.) *The Futures of Criminology*. Thousand Oaks: Sage, pp. 173–201.

Ferguson AG (2017a) Policing Predictive Policing. *Washington University Law Review* 94(1109). Available at: https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/5 (accessed 6 October 2020).

Ferguson AG (2017b) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press. DOI: 10.2307/j.ctt1pwtb27.

Fitch A (2020) Microsoft Pledges Not to Sell Facial-Recognition Tools to Police Absent National Rules. *Wall Street Journal*, 11 June. Available at: https://www.wsj.com/articles/microsoft-pledges-not-tosell-facial-recognition-technology-to-police-absent-national-rules-11591895282 (accessed 1 October 2020).

Floud J (1982) Dangerousness and Criminal Justice. *British Journal of Criminology* 22(3): 213–228.

Foody K (2020) Chicago police end effort to predict gun offenders, victims. *AP NEWS*, 23 January. Available at: https://apnews.com/41f75b783d796b80815609e737211cc6 (accessed 18 February 2020).

Foucault M (1977) *Discipline and Punish: The Birth of the Prison* (tran. A Sheridan). New Ed edition. London: Penguin.

Foucault M (2003) *Society Must Be Defended: Lectures at the Collège de France, 1975-76*. Allen Lane The Penguin Press.

Foucault M (2009) *Security, Territory, Population: Lectures at the College De France, 1977 - 78* (ed. AI Davidson). Michel Foucault, Lectures at the Collège de France. Palgrave Macmillan UK. DOI: 10.1057/9780230245075.

Foucault M (2010) *The Birth of Biopolitics: Lectures at the Collège de France, 1978-79* (ed. M Senellart; tran. G Burchell). Paperback edition. Michel Foucault's lectures at the Collège de France. New York, NY: Palgrave Macmillan.

Frangoul A (2013) Minority report: Predicting where to put your policeman. *CNBC*, 8 November. Available at: https://www.cnbc.com/id/101182057?view=story (accessed 8 March 2019).

Fussey P (2002) An interrupted transmission? Processes of CCTV implementation and the impact of human agency. *Surveillance & Society* 4(3). Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3449.

Fussey P (2013) Contested topologies of UK counterterrorist surveillance: the rise and fall of Project Champion. *Critical Studies on Terrorism* 6(3). Routledge: 351–370. DOI: 10.1080/17539153.2013.823757.

Fussey P and Murray D (2019) *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. July. Human Rights, Big Data and Technology Project, University of Essex. Available at: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

Fussey P and Sandhu A (2020) Surveillance arbitration in the era of digital policing. *Theoretical Criminology*: 1–20. DOI: 10.1177/1362480620967020.

Gandy OH (2009) *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Aldershot: Ashgate.

Gerstner D (2018) Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany. *European Journal for Security Research* 3(2): 115–138. DOI: 10.1007/s41125-018-0033-0.

Giddens A (1991) *Giddens, A: Consequences of Modernity*. New edition. Cambridge: Blackwell Publishers.

Goldstein H (1979) Improving Policing: A Problem-Oriented Approach. *Crime & Delinquency* 25(2): 236–258. DOI: 10.1177/001112877902500207.

Gottfredson M and Hirschi T (1986) The True Value of Lambda Would Appear to Be Zero: An Essay on Career Criminals, Criminal Careers, Selective Incapacitation, Cohort Studies, and Related Topics*. *Criminology* 24(2): 213–234. DOI: 10.1111/j.1745-9125.1986.tb01494.x.

Graham S and Thrift N (2007) Out of Order: Understanding Repair and Maintenance. *Theory, Culture & Society* 24(3). SAGE Publications Ltd: 1–25. DOI: 10.1177/0263276407075954.

Graham SDN (2005) Software-sorted geographies. *Progress in Human Geography* 29(5). SAGE Publications Ltd: 562–580. DOI: 10.1191/0309132505ph568oa.

Grint K and Woolgar S (1997) *The Machine at Work: Technology, Work, and Organization*. Cambridge, UK ; Malden, MA : Blackwell Publishers: Polity Press.

Grogger J and Ridgeway G (2006) Testing for Racial Profiling in Traffic Stops From Behind a Veil of Darkness. *Journal of the American Statistical Association* 101(475). Taylor & Francis: 878–887. DOI: 10.1198/016214506000000168.

Guilfoyle S (2012) On Target?--Public Sector Performance Management: Recurrent Themes, Consequences and Questions. *Policing* 6(3): 250–260. DOI: 10.1093/police/pas001.

Gutting G (2005) *Foucault: A Very Short Introduction*. A very short introduction. Oxford: Oxford University Press.

Hacking I (1982) Biopower and the avalanche of printed numbers. *Humanities in Society* 5: 279–295.

Haggerty KD (2006) Tear down the walls: on demolishing the panopticon. In: Lyon D (ed.) *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton: Willan Publishing, pp. 23–45.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *The British Journal of Sociology* 51(4): 605–622. DOI: 10.1080/00071310020015280.

Harcourt BE (2001) *Illusion of Order: The False Promise of Broken Windows Policing*. Cambridge, MA: Harvard University Press.

Harcourt BE (2007) *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. Chicago: University of Chicago Press.

Harford T (2014) Big data: are we making a big mistake? *Financial Times*, 28 March. Available at: https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0 (accessed 29 May 2017).

Heilweil R (2020) Big tech companies back away from selling facial recognition to police. That's progress. Available at: https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police (accessed 1 October 2020).

Henley J (2019) Denmark frees 32 inmates over flaws in phone geolocation evidence. *The Guardian*, 12 September. Available at: https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations (accessed 29 September 2020).

Home Office (2017) *Anti-social Behaviour, Crime and Policing Act 2014: Anti-social behaviour powers. Statutory guidance for frontline professionals*. December. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/679712/2017-12-13_ASB_Revised_Statutory_Guidance_V2.1_Final.pdf (accessed 22 June 2019).

Hood C (1991) A Public Management for All Seasons? *Public Administration* 69(1): 3–19. DOI: 10.1111/j.1467-9299.1991.tb00779.x.

Howard P, Francis B, Soothill K, et al. (2009) *OGRS 3*. Ministry of Justice.

Hu H, Wen Y, Chua TS, et al. (2014) Toward Scalable Systems for Big Data Analytics: A Technology Tutorial. *IEEE Access* 2: 652–687. DOI: 10.1109/ACCESS.2014.2332453.

Hutchby I (2016) Technologies, Texts and Affordances: *Sociology*. DOI: 10.1177/S0038038501000219.

Ifmpt (2018) Ifmpt - Institut für musterbasierte Prognosetechnik. Available at: https://www.ifmpt.de/ (accessed 1 June 2018).

Jackson SJ (2014) Rethinking Repair. In: Gillespie T, Boczkowski PJ, and Foot KA (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. The MIT Press, pp. 221–240. DOI: 10.7551/mitpress/9780262525374.003.0011.

Joh EE (2007) Discretionless Policing: Technology and the Fourth Amendment Essay. *California Law Review* 95(1): 199–234.

Joh EE (2016) The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing. *Harvard Law & Policy Review* 10: 15–42.

Johnson RR and Morgan MA (2013) Suspicion formation among police officers: an international literature review. *Criminal Justice Studies* 26(1): 99–114. DOI: 10.1080/1478601X.2012.705784.

Johnson SD, Bowers KJ, Birks DJ, et al. (2009) Predictive Mapping of Crime by ProMap: Accuracy, Units of Analysis, and the Environmental Backcloth. In: Weisburd D, Bernasco W, and Bruinsma GJN (eds) *Putting Crime in Its Place*. Springer New York, pp. 171–198. DOI: 10.1007/978-0-387-09688-9_8.

Kaufmann M, Egbert S and Leese M (2019) Predictive Policing and the Politics of Patterns. *The British Journal of Criminology* 59(3): 674–692. DOI: 10.1093/bjc/azy060.

Kavanagh D and Araujo L (1995) Chronigami: Folding and unfolding time. *Accounting, Management and Information Technologies* 5(2): 103–121. DOI: 10.1016/0959-8022(95)00010-7.

Kemshall H (2010) Community protecion and multi-agency public protection arrangements. In: Nash M and Williams A (eds) *Handbook of Public Protection*. Abingdon; New York: Willan, pp. 199–216.

Kemshall H and Wood J (2008) Public protection in practice: Multi-Agency Public Protection Arrangements (MAPPA). In: Clark CL and McGhee J (eds) *Private and Confidential? Handling Personal Information in the Social and Health Services*. Bristol, UK: Policy Press, pp. 111–127.

Kennedy LW and Dugato M (2018) Forecasting Crime and Understanding its Causes. Applying Risk Terrain Modeling Worldwide. *European Journal on Criminal Policy and Research* 24(4): 345–350. DOI: 10.1007/s10610-018-9404-3.

Kitchin R (2014a) Big Data, new epistemologies and paradigm shifts. *Big Data & Society* 1(1): 2053951714528481. DOI: 10.1177/2053951714528481.

Kitchin R (2014b) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. New Auflage. Los Angeles, California: SAGE Publications Ltd.

Koen MC and Willis JJ (2019) Making sense of body-worn cameras in a police organization: a technological frames analysis. *Police Practice and Research*: 1–17. DOI: 10.1080/15614263.2019.1582343.

Koper CS and Lum C (2019) The Limits of Police Technology. In: Weisburd D and Braga AA (eds) *Police Innovation. Contrasting Perspectives*. 2nd ed. Cambridge: Cambridge University Press.

Koper CS, Lum C and Willis JJ (2014) Optimizing the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behavioural Aspects of Implementing Police Technologies. *Policing: A Journal of Policy and Practice* 8(2). Oxford Academic: 212–221. DOI: 10.1093/police/pau015.

Kovandzic TV, III JJS and Vieraitis LM (2004) “Striking out” as crime reduction policy: The impact of “three strikes” laws on crime rates in U.S. cities. *Justice Quarterly* 21(2). Routledge: 207–239. DOI: 10.1080/07418820400095791.

Latour B (1987) *Science in Action: How to Follow Scientists and Engineers through Society*. Cambridge, Mass: Harvard University Press.

Latour B (1990) Technology is Society Made Durable. *The Sociological Review* 38(1_suppl): 103–131. DOI: 10.1111/j.1467-954X.1990.tb03350.x.

Latour B (2004) Why has critique run out of steam? From matters of fact to matters of concern. *Critical inquiry* 30(2): 225–248.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory*. Clarendon lectures in management studies. Oxford: Oxford University Press.

Latour B (2008) *What Is the Style of Matters of Concern?* Spinoza lectures. Assen: Van Gorcum.

Law J (1991) Power, Discretion and Strategy. In: *A Sociology of Monsters. Essays on Power, Technology and Domination*. Sociological Review. London: Routledge, pp. 165–191. Available at: http://dx.doi.org/10.1111/j.1467-954X.1990.tb03352.x (accessed 27 February 2017).

Law J (1992) Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems practice* 5(4): 379–393. DOI: 10.1007/BF01059830.

Law J (1994) *Organizing Modernity*. Oxford, UK ; Cambridge, Mass., USA: Blackwell.

Law J (2003) Ordering and Obduracy. Centre for Science Studies, Lancaster University, Lancaster LA1 4YN, UK. Available at: https://www.lancaster.ac.uk/fass/resources/sociology-online-papers/papers/law-ordering-and-obduracy.pdf (accessed 27 December 2020).

Law J and Bijker WE (1992) Postscript: Technology, Stability, and Social Theory. In: Bijker WE and Law J (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Inside technology. Cambridge, Mass: MIT Press, pp. 290–308.

Law J and Callon M (1992) The Life and Death of an Aircraft: A Network Analysis of Technical Change. In: Bijker WE and Law J (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Inside technology. Cambridge, Mass: MIT Press, pp. 21–52.

Law J and Hetherington K (2000) Materialities, spatialities, globalities. In: Bryson JR, Daniels PW, Henry N, et al. (eds) *Knowledge, Space, Economy*. 1st ed. London: Routledge, pp. 34–49. DOI: 10.4324/9780203186107.

Lawrence P (2017) The Vagrancy Act (1824) and the Persistence of Pre-emptive Policing in England since 1750. *The British Journal of Criminology* 57(3): 513–531. DOI: 10.1093/bjc/azw008.

Lemke T (2007) *Biopolitik. Zur Einführung*. Zur Einführung. Hamburg: Junius.

Levallois C, Steinmetz S and Wouters P (2013) Sloppy data floods or precise social science methodologies? Dilemmas in the transition to data-intensive research in sociology and economics (Chapter 5). In: Wouters P, Beaulieu A, Scharnhorst A, et al. (eds) *Virtual Knowledge: Experimenting in the Humanities and the Social Sciences*. Cambridge, Mass; London: The MIT Press, pp. 151–182.

Levy Y and Hall E (2019) Annex H. A guide to prohibitions updated Nov 19. In: Crown Prosecution Service (ed.) *Criminal Behaviour Orders. Legal Guidance*. Available at: https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/A%20guide%20to%20prohibitions%20updated%20Nov%2019.docx.

Liggins A, Ratcliffe JH and Bland M (2019) Targeting the Most Harmful Offenders for an English Police Agency: Continuity and Change of Membership in the “Felonious Few”. *Cambridge Journal of Evidence-Based Policing* 3(3): 80–96. DOI: 10.1007/s41887-019-00039-7.

Linder T (2019) Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service. *Surveillance & Society* 17(1/2): 76–82. DOI: 10.24908/ss.v17i1/2.12903.

Lipsky M (2010) *Street-Level Bureaucracy, 30th Anniversary Edition: Dilemmas of the Individual in Public Service*. Russell Sage Foundation.

Loftus B, Goold B and Mac Giollabhui S (2016) From a Visible Spectacle to an Invisible Presence: The Working Culture of Covert Policing. *British Journal of Criminology* 56(4): 629–645. DOI: 10.1093/bjc/azv076.

Los Angeles Times (2016) Police push back against using crime-prediction technology to deploy officers. 4 October. Available at: http://www.latimes.com/local/lanow/la-me-police-predict-crime-20161002-snap-story.html (accessed 15 November 2016).

Lum C, Koper CS and Willis J (2017) Understanding the Limits of Technology’s Impact on Police Effectiveness. *Police Quarterly* 20(2). SAGE Publications Inc: 135–163. DOI: 10.1177/1098611116667279.

Lum C, Koper CS, Willis J, et al. (2019) The rapid diffusion of license plate readers in US law enforcement agencies. *Policing: An International Journal* 42(3). Emerald Publishing Limited: 376–393. DOI: 10.1108/PIJPSM-04-2018-0054.

Lum K and Isaac W (2016) To predict and serve? *Significance* 13(5): 14–19. DOI: 10.1111/j.1740-9713.2016.00960.x.

Lupton D (2016) *The Quantified Self*. Cambridge: Policy Press.

Lynch J (2020) Courts Issue Rulings in Two Cases Challenging Law Enforcement Searches of License Plate Databases. Available at: https://www.eff.org/deeplinks/2020/05/courts-issue-rulings-two-cases-challenging-law-enforcement-searches-license-plate (accessed 29 September 2020).

Lyon D (1994) *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Lyon D (2003) Surveillance as social sorting. Computer codes and mobile bodies. In: Lyon D (ed.) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London, New York: Routledge.

Maguire M (2000) Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Policing and Society* 9(4): 315–336. DOI: 10.1080/10439463.2000.9964821.

Maguire M (2018) Policing Future Crimes. In: Maguire M, Rao U, and Zurawski N (eds) *Bodies as Evidence: Security, Knowledge, and Power*. Durham: Duke University Press, pp. 137–158.

Maguire M and McVie S (2017) Crime Data And Criminal Statistics: A Critical Reflection. In: Liebling A, Maruna S, and McAra L (eds) *The Oxford Handbook of Criminology*. Sixth edition. Oxford: Oxford University Press, pp. 163–189.

Maltz MD (1977) Crime Statistics: A Historical Perspective. *Crime & Delinquency* 23(1). SAGE Publications Inc: 32–40. DOI: 10.1177/001112877702300103.

Manning PK (1992) Information Technologies and the Police. *Crime and Justice* 15: 349–398. DOI: 10.1086/449197.

Manning PK (2008) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New perspectives in crime, deviance, and law series. New York: New York University Press.

Mantello P (2016) The machine that ate bad people: The ontopolitics of the precrime assemblage. *Big Data & Society* 3(2): 1–11. DOI: 10.1177/2053951716682538.

Marks M (2004) Researching Police Transformation. The Ethnographic Imperative. *The British Journal of Criminology* 44(6). Oxford Academic: 866–888. DOI: 10.1093/bjc/azh049.

Mason J (2002) *Qualitative Researching*. 2nd ed. London: SAGE.

Mastrobuoni G (2020) Crime is Terribly Revealing: Information Technology and Police Productivity. *The Review of Economic Studies* 87(6): 2727–2753. DOI: 10.1093/restud/rdaa009.

Matthews R (2014) *Realist Criminology*. Palgrave Macmillan UK. DOI: 10.1057/9781137445711.

Mayer-Schönberger V and Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

McCabe JE, Kaminski RJ and Boehme HM (2020) Racial profiling and CT motor vehicle stops: an observational study in three towns. *Police Practice and Research* 0(0). Routledge: 1–18. DOI: 10.1080/15614263.2020.1749620.

McCulloch J and Wilson D (2015) *Pre-Crime: Pre-Emption, Precaution and the Future*. Routledge frontiers of criminal justice 28. Abingdon: Routledge.

McIlwain CD (2019) *Black Software: The Internet & Racial Justice, from the AfroNet to Black Lives Matter*. New York, NY: Oxford University Press.

Merola LM and Lum C (2012) Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition (LPR) Technology. *Judicature* 96(3): 119–126.

Meyer JW and Rowan B (1977) Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology* 83(2): 340–363.

Miller K (2014) Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm. *J. Tech. L. & Pol'y* 19: 105.

Millie A (2008) Anti-Social Behaviour, Behavioural Expectations and an Urban Aesthetic. *The British Journal of Criminology* 48(3). Oxford University Press: 379–394.

Mittelstadt BD, Allo P, Taddeo M, et al. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society* 3(2). SAGE Publications Ltd: 2053951716679679. DOI: 10.1177/2053951716679679.

Mohler GO, Short MB, Malinowski S, et al. (2015) Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association* 110(512): 1399–1411. DOI: 10.1080/01621459.2015.1077710.

Monahan T (2018) Algorithmic Fetishism. *Surveillance & Society* 16(1): 1–5. DOI: 10.24908/ss.v16i1.10827.

Monahan T and Fisher JA (2015) Strategies for obtaining access to secretive or guarded organizations. *Journal of contemporary ethnography* 44(6): 709–736.

Muller JZ (2018) *The Tyranny of Metrics*. Princeton University Press.

Murray D and Fussey P (2019) Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review* 52(1). Cambridge University Press: 31–60. DOI: 10.1017/S0021223718000304.

Nash M and Walker L (2009) Mappa—Is Closer Collaboration Really the Key to Effectiveness? *Policing: A Journal of Policy and Practice* 3(2). Oxford Academic: 172–180. DOI: 10.1093/police/pap007.

National Audit Office (2018) *Financial sustainability of police forces in England and Wales 2018*. 11 November.

National Institute of Justice (2009) *Predictive Policing Symposiums*. NCJ 242222, NCJ 248891. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/242222and248891.pdf (accessed 2 March 2017).

Newell BC (2013) Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information Symposium: Who's Governing Privacy: Regulation and Protection in a Digital Era. *Maine Law Review* 66(2): 397–436.

Norris C and Armstrong G (1999) *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.

Nowotny H (1992) Time and Social Theory. Towards a social theory of time. *Time & Society* 1(3): 421–454.

O'Neil C (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. London: Allen Lane.

Oosterloo S and Schie G van (2018) The Politics and Biases of the "Crime Anticipation System" of the Dutch Police. In: *Proceedings of the International Workshop on Bias in Information, Algorithms, and Systems co-located with 13th International Conference on Transforming Digital Worlds (iConference 2018)* (eds J Bates, PD Clough, R Jaschke, et al.), Sheffield, United Kingdom, 2018, pp. 30–41. Available at: https://ir.shef.ac.uk/bias/bias2018_proceedings.pdf.

Palantir (2013) Palantir at the Los Angeles Police Department. Available at: https://www.youtube.com/watch?v=aJ-u7yDwC6g (accessed 14 July 2020).

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Pasquino P (1991) Theatrum Politicum: The Genealogy of Capital - Police and the State of Prosperity. In: Burchell G, Gordon C, and Miller P (eds) *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press, pp. 105–118.

Patton MQ (2015) *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*. Fourth edition. Thousand Oaks, CA: SAGE Publications, Inc.

Pepinsky HE (1984) Better Living through Police Discretion. *Law and Contemporary Problems* 47(4). Duke University School of Law: 249–267. DOI: 10.2307/1191692.

Perry WL, McInnis B, Price CC, et al. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND.

Pierson E, Simoiu C, Overgoor J, et al. (2020) A large-scale analysis of racial disparities in police stops across the United States. *Nature Human Behaviour*. Nature Publishing Group: 1–10. DOI: 10.1038/s41562-020-0858-1.

Piquero AR, Farrington DP and Blumstein A (2003) The Criminal Career Paradigm. *Crime and Justice* 30. The University of Chicago Press: 359–506. DOI: 10.1086/652234.

Porter TM (1996) *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton, N.J: Princeton University Press.

Power M (1997) *The Audit Society. Rituals of Verification*. Oxford University Press.

Power M (2000) The Audit Society - Second Thoughts. *International Journal of Auditing* 4(1): 111–119. DOI: 10.1111/1099-1123.00306.

PredPol (2016) About Us | Predictive Policing. Available at: http://www.predpol.com/about/ (accessed 8 December 2016).

Public Administration Select Committee (2014) *Caught red-handed: Why we can't count on Police Recorded Crime statistics*. 13, 9 April. London: House of Commons. Available at: https://publications.parliament.uk/pa/cm201314/cmselect/cmpubadm/760/760.pdf (accessed 14 July 2020).

Quinton P (2011) The formation of suspicions: police stop and search practices in England and Wales. *Policing and Society* 21(4). Routledge: 357–368. DOI: 10.1080/10439463.2011.610193.

Rabinow P and Rose N (2003) Foucault today. In: *The Essential Foucault: Selections from the Essential Works of Foucault, 1954-1984*. New York: New Press.

Rabinow P and Rose N (2006) Biopower Today. *BioSocieties* 1(2): 195–217. DOI: 10.1017/S1745855206040014.

Ragin CC (1992) Introduction: Cases of 'What is a case?' In: Ragin CC and Becker HS (eds) *What Is a Case?: Exploring the Foundations of Social Inquiry*. New York: Cambridge University Press, pp. 1–17.

Raso F, Hilligoss H, Krishnamurthy V, et al. (2018) Artificial Intelligence & Human Rights: Opportunities & Risks. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.3259344.

Ratcliffe JH, Taylor RB and Fisher R (2019) Conflicts and congruencies between predictive policing and the patrol officer's craft. *Policing and Society*: 1–17. DOI: 10.1080/10439463.2019.1577844.

Reeves C (2013) How multi-agency are Multi-Agency Risk Assessment Committees? *Probation Journal* 60(1). SAGE Publications Ltd: 40–55. DOI: 10.1177/0264550512470187.

Richardson R, Schultz JM and Crawford K (2019) Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online* 94: 41.

Rubel A, Castro C and Pham A (2019) Agency Laundering and Information Technologies. *Ethical Theory and Moral Practice* 22(4): 1017–1041. DOI: 10.1007/s10677-019-10030-w.

Sagiroglu S and Sinanc D (2013) Big data: A review. In: *2013 International Conference on Collaboration Technologies and Systems (CTS)*, May 2013, pp. 42–47. DOI: 10.1109/CTS.2013.6567202.

Sanders CB and Henderson S (2013) Police ‘empires’ and information technologies: uncovering material and organisational barriers to information sharing in Canadian police services. *Policing and Society* 23(2): 243–260. DOI: 10.1080/10439463.2012.703196.

Sanders CB, Christensen T and Weston C (2015) Constructing Crime in a Database: Big Data and the Mangle of Social Problems Work. *Qualitative Sociology Review* 11(2): 180–195.

Sandhu A and Fussey P (2020) The ‘uberization of policing’? How police negotiate and operationalise predictive policing technology. *Policing and Society* 0(0). Routledge: 1–16. DOI: 10.1080/10439463.2020.1803315.

Saunders J, Hunt P and Hollywood JS (2016) Predictions put into practice: a quasi-experimental evaluation of Chicago’s predictive policing pilot. *Journal of Experimental Criminology* 12(3): 347–371. DOI: 10.1007/s11292-016-9272-0.

Scannell RJ (2019) This Is Not Minority Report. Predictive Policing and Population Racism. In: Benjamin R (ed.) *Captivating Technology. Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life.* Durham and London: Duke University Press, pp. 107–129.

Schlehahn E, Aichroth P, Mann S, et al. (2015) Benefits and Pitfalls of Predictive Policing. In: *Intelligence and Security Informatics Conference (EISIC), 2015 European*, September 2015, pp. 145–148. DOI: 10.1109/EISIC.2015.29.

Scott WR (1995) *Institutions and Organizations*. Foundations for organizational science. Thousand Oaks: Sage.

Seidman D and Couzens M (1974) Getting the Crime Rate Down: Political Pressure and Crime Reporting. *Law & Society Review* 8(3): 457. DOI: 10.2307/3053084.

Sharkey P (2020) Why do we need the police? Cops prevent violence. But they aren’t the only ones who can do it. Available at: https://www.washingtonpost.com/outlook/2020/06/12/defund-police-violent-crime/ (accessed 20 September 2020).

Sherman L, Neyroud PW and Neyroud E (2016) The Cambridge Crime Harm Index: Measuring Total Harm from Crime Based on Sentencing Guidelines. *Policing: A Journal of Policy and Practice* 10(3). Oxford Academic: 171–183. DOI: 10.1093/police/paw003.

Simester AP and Hirsch A von (2006) *Incivilities: Regulating Offensive Behaviour*. Oxford and Portland, Oregon: Hart Publishing.

Souhami A (2020) Constructing tales of the field: uncovering the culture of fieldwork in police ethnography. *Policing and Society* 30(2). Routledge: 206–223. DOI: 10.1080/10439463.2019.1628230.

Squires P (2006) New Labour and the politics of antisocial behaviour. *Critical Social Policy* 26(1): 144–168. DOI: 10.1177/0261018306059769.

Squires P (2008) Introduction: why ‘anti-social behaviour’? Debating ASBOs. In: Squires P (ed.) *ASBO Nation: The Criminalisation of Nuisance*. Bristol: Bristol University Press, p. 35.

Star SL and Ruhleder K (1996) Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *INFORMATION SYSTEMS RESEARCH* 7(1): 25.

Stolzenberg L and D’Alessio SJ (1997) “Three Strikes and You’re Out”: The Impact of California’s New Mandatory Sentencing Law on Serious Crime Rates. *Crime & Delinquency* 43(4): 457–469. DOI: 10.1177/0011128797043004004.

Taylor RW and Russell AL (2012) The failure of police ‘fusion’ centers and the concept of a national intelligence sharing plan. *Police Practice and Research* 13(2): 184–200. DOI: 10.1080/15614263.2011.581448.

Terpstra J, Fyfe NR and Salet R (2019) The Abstract Police: A conceptual exploration of unintended changes of police organisations. *The Police Journal* 92(4). SAGE Publications Ltd: 339–359. DOI: 10.1177/0032258X18817999.

Thompson D (2020) Unbundle the Police. Available at: https://www.theatlantic.com/ideas/archive/2020/06/unbundle-police/612913/ (accessed 20 September 2020).

van Brakel R (2016) Pre-Emptive Big Data Surveillance and its (Dis) Empowering Consequences: The Case of Predictive Policing. In: van der Sloot B, Broeders D, and Schrijvers E (eds) *Exploring the Boundaries of Big Data*. The Hague: Amsterdam University Press, pp. 117–141. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2772469 (accessed 30 November 2016).

van Brakel R and De Hert P (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies.|. *Cahiers Politiestudies* 2(4): 165.

Visher CA (2016) Unintended Consequences: Policy Implications of the NAS Report on Criminal Careers and Career Criminals. *Journal of Research in Crime and Delinquency* 53(3). SAGE Publications Inc: 306–320. DOI: 10.1177/0022427815603770.

Vitale AS (2017) *The End of Policing*. London: Verso Books.

Wacquant L (2009) Deadly symbiosis: when ghetto and prison meet and mesh. In: Newburn T (ed.) *Key Readings in Criminology*. Cullompton: Willan, pp. 759–765.

Ward JS and Barker A (2013) Undefined By Data: A Survey of Big Data Definitions. *arXiv:1309.5821 [cs]*. Available at: http://arxiv.org/abs/1309.5821 (accessed 29 May 2017).

Waterton C (2010) Experimenting with the Archive: STS-ers As Analysts and Co-constructors of Databases and Other Archival Forms. *Science, Technology, & Human Values* 35(5). SAGE Publications Inc: 645–676. DOI: 10.1177/0162243909340265.

Weiner NA and Wolfgang ME (eds) (1989) Violent criminal careers and 'violent career criminals': An overview of the research literature. In: *Violent Crime, Violent Criminals*. 1st Edition. Newbury Park, Calif: SAGE Publications, Inc, pp. 35–138.

Weisburd D (2016) *Place Matters: Criminology for the Twenty-First Century*. New York, NY: Cambridge University Press.

Weisburd D, Mastrofski SD, McNally A, et al. (2003) Reforming to preserve: Compstat and strategic problem solving in American policing. *Criminology & Public Policy* 2(3): 421–456.

Weisburd D, Willis JJ, Mastrofski SD, et al. (2019) Changing Everything so that Everything Can Remain the Same: CompStat and American Policing. In: Weisburd D and Braga AA (eds) *Police Innovation Contrasting Perspectives*. 2nd ed. Cambridge: Cambridge University Press, pp. 417–435.

Weitekamp EGM and Herberger S (1995) Amerikanische Strafrechtspolitik auf dem Weg in die Katastrophe. *Neue Kriminalpolitik* 7(2): 15–21. DOI: https://doi.org/10.5771/0934-9200-1995-2-15.

Wheeler AP (2016) Tables and graphs for monitoring temporal crime trends: Translating theory into practical crime analysis advice. *International Journal of Police Science & Management* 18(3). SAGE Publications Ltd: 159–172. DOI: 10.1177/1461355716642781.

Wiliams A and Nash M (2014) The Realities of Legislating Against and Protecting the Public from Risky Groups. In: McCartan K (ed.) *Responding to Sexual Offending*. London: Palgrave Macmillan UK, pp. 1–19. DOI: 10.1057/9781137358134.

Willis JJ (2014) Compstat. In: Bruinsma G and Weisburd D (eds) *Encyclopedia of Criminology and Criminal Justice*. New York, NY: Springer, pp. 496–505.

Willis JJ and Mastrofski SD (2012) Compstat and The New Penology: A Paradigm Shift in Policing? *British Journal of Criminology* 52(1): 73–92. DOI: 10.1093/bjc/azr063.

Wilson D (2019) Platform Policing and the Real-Time Cop. *Surveillance & Society* 17(1/2): 69–75. DOI: 10.24908/ss.v17i1/2.12958.

Wilson D (2020) Predictive Policing Management: A Brief History of Patrol Automation. *new formations: a journal of culture/theory/politics* 98(1): 139–155.

Winner L (1980) Do Artifacts Have Politics? *Daedalus* 109(1). The MIT Press: 121–136.

Winner L (1993) Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology. *Science, Technology & Human Values* 18(3): 362–378. DOI: 10.1177/016224399301800306.

Wolfgang ME, Figlio RM and Sellin T (1972) *Delinquency in a Birth Cohort*. Studies in Crime and Justice. Chicago: University of Chicago Press.

Woolgar S and Cooper G (1999) Do Artefacts Have Ambivalence? Moses' Bridges, Winner's Bridges and Other Urban Legends in S&TS. *Social Studies of Science* 29(3). Sage Publications, Ltd.: 433–449.

Yglesias M (2020) The End of Policing by Alex Vitale, reviewed and critiqued. Available at: https://www.vox.com/2020/6/18/21293784/alex-vitale-end-of-policing-review (accessed 20 September 2020).

Young J (1977) The police as amplifiers of deviancy. In: Rock PE (ed.) *Drugs and Politics*. New Brunswick and London: Transaction Publishers, pp. 99–134.

Young J (1997) Left Realist Criminology: Radical in its Analysis, Realist in its Policy. In: Maguire M, Morgan R, and Reiner R (eds) *Oxford Handbook of Criminology*. 2nd ed. Oxford: Clarendon Press, pp. 473–497.

Zedner L (2007) Pre-crime and post-criminology? *Theoretical Criminology* 11(2): 261–281. DOI: 10.1177/1362480607075851.

11. Appendix

11.1. Research outline for US case study

University of Essex

The Human Rights, Big Data and Technology Project

Compliance by the numbers: Officer perceptions of data-driven measures in the context of [department]'s consent decree

Researchers

Daniel Marciniak (PhD Candidate at University of Essex, UK), contact: d.marciniak@essex.ac.uk

Professor Pete Fussey (University of Essex, UK), contact: pfussey@essex.ac.uk

Dr Daragh Murray (University of Essex, UK), contact: d.murray@essex.ac.uk

Research Outline

- Research Goals: [the police department] has put extensive data-driven management strategies in place to insure compliance with its consent decree. This study examines how officers of different experience, rank, and assignment perceive of these changes. Its purpose is to gather empirical qualitative evidence to gain a general understanding of how data-driven changes can inform officer actions and compliance. The research is also interested in how data driven practices help inform and improve policing more generally and assess officers' perspectives to such approaches. The project also holds scope to consider accommodating further research aims as defined by [the department].

- Research Value:
  - Gathering data on the perspectives of police officers will be valuable as it will improve understandings of the subjective views of the individuals directly affected by the implemented measures and thus can serve as a gauge for their long-term effects.
  - The research can provide valuable feedback on the consent decree's implementation. It gives the opportunity to adjust measures if necessary and to highlight the progress that has been made so far.
  - The research will also assess officer's level of engagement with data-driven and related technologically assisted policing tools.
  - Lastly, the research output will lend visibility to [the department's] efforts in the academic literature, positioning the [department] as an example of transformation.

Research Questions

- How does available data and routinely collected data affect officer decision making?
  - Does data collection encourage compliance?

  - How do computer systems inform the formation of reasonable suspicion?
- What are officers' attitudes towards the consent decree and its implementation process?
  - Are officers aware of departmental policies (e.g. regarding stop and search, and use of body-worn cameras)?
  - Do regulatory or oversight arrangements assist or hinder the ability of officers to carry out their work?
  - Do officers see their perspectives reflected in the changes that have been made?

Methodology

Researchers intend to collect primary data using qualitative methods including semi-structured interviews and participant observation. Researchers expect to complete a minimum of 45 interviews with a mix of police officers with different experience, ranks, and assignments, as well as with personnel tasked with implementing [the department]'s data-driven management processes. Subject to consent from the participant, the interviews will be audio recorded and transcribed. Questions will address the key priorities outlined in each research theme above.

Research Ethics

- Our research is subject to strict ethical standards - covering issues including but not limited to consent, anonymity, appropriate data handling and participants' right of withdrawal - in advance of any fieldwork. The proposed project has received ethical approval from the University of Essex in accordance with accepted international standards of ethics for social science research.
- Participants will receive an information sheet informing them about the research goals and providing them with the contact details of the researchers and the relevant ethics body at university.
- Participants will then be asked to fill a confidential consent form to ensure they are fully informed of and willing to participate in the research. In cases where this is not practical consent will be audio-recorded.
- Researchers are committed to upholding participants' anonymity. Transcripts will be anonymized by replacing any type of identifying information such as name, rank, location or position within the organisation. This information will be held separately to the data.
- Only the identified researchers will have access to the data. Data will be stored in a secure and encrypted digital space.

Action Plan

1) *Recruitment*: To conduct the study researchers will stay in [the city] for around a month in the first instance. This is completely funded by academic grants and scholarships that have already been awarded. The [department] will not carry any financial cost. Research will begin by recruiting research participants supported by the department. In the past, this has been most effective if researchers contact information is shared across the department, and researchers are able to complete 3-5 ride-alongs with police officers.
2) *Interviews*: Researchers will complete the interviews over the course the month. It is deemed practical to start with interviewing personnel tasked with implementing the consent decree. Interviews can be conducted wherever and whenever suits individual research

participants. To maintain objectivity and independence, interviews will be scheduled by interviewees and interviewers.

3) *Analysis*: Researchers will analyse research data over the course of 2 months before producing outputs. Outputs will include:
   a) A plain language report of research findings for the [department].
   b) Researchers will seek independent publication of the study's findings in academic journals. These will contribute to the understanding of transformation processes towards constitutional policing. The intention is to fairly represent interviewee's perspectives in the academic literature.
   c) Other internal documents, briefing notes and reporting tools that are deemed useful to [the department].

11.2. Detailed methodology and interview schedule. US case study

University of Essex

The Human Rights, Big Data and Technology Project

Headline Research Aim

[The department] has put extensive data-driven management strategies in place to enhance its delivery of policing and to monitor the performance of the organisation as a whole. This study proposes to examine the role of data and technology within current police work in [the city]. In doing so, it also seeks to co-develop a number of research aims identified by [the department] as important and valuable to them. The project is fully funded and is designed to incorporate questions and themes deemed useful by the host organization. Input in this regard is very welcome.

The purpose of the research is to gather empirical qualitative evidence to gain a general understanding of how data-driven changes can inform officer actions. The research is interested in how data driven practices help inform and improve policing more generally and will assess officers' perspectives regarding such approaches.

The core focus of the research analyses the increasing data richness of policing environments and seeks to understand how such data and technology shapes policing practices, its deployment within operational settings and examine officer engagement with technology. In particular the research proposes to focus on what data is available to officers, how it is used in an operational sense, what value is attributed to it, how individuals engage with and receive information and how technologies are used as tools for policing. Findings could also be used to inform an understanding of officers' perspectives on the most useful forms of data (i.e. what they would like to receive and how they would like to receive it), the enablers and blockers for realising the potential of data-driven policing, and ways of improving officer engagement with data and technology.

This document is intended as a provisional outline and a means to develop further discussion and scope out areas of shared interest between the department and the research team.

Detailed methodology and interview schedule

Research tasks will be shared between team members with Daniel Marciniak being present for four weeks and Prof Pete Fussey and Dr Daragh Murray conducting interviews during one week. Prof Fussey is the named individual with overall responsibility for matters of research management, governance and ethics.

As researchers we take the position that our research subjects are experts in their professional fields and have the potential to reveal important insights that may not be anticipated at the outset. This is why we retain an element of flexibility in our interview schedule and provide space for participants to voice their perspectives and experiences on their own terms.

For this reason, we adopt a semi-structured interview approach to provide a degree of structure across, and comparability between, responses yet offering the space to explore emerging areas of importance. We aim to set out our core interview schedule below along with a clarified outline of ideal participants. We are very open to discussing ways to further direct and shape the research.

The following sets out the kind of questions we are intending to ask, and the topics we would like to address to meet the main research aims. It is not intended to be a complete set of questions, nor do all of them need to be addressed in every interview.

In order to address the research questions stated in the research outline we propose to adopt a two-step approach:

1) Interviewing employees whose main tasks are in designing, processing and analysing data handled by the department, particularly data made available and designed to inform the decision making of officers on duty. The units named below are based on publicly available information on [the department's] organisational structure. Feedback on these choices would be very welcome.

i. Interviews with members of the [compliance monitoring unit] on the role of data collection and analysis in the implementation of the consent decree

1. How do you see your role in the department?
2. What was/is your role relating to the consent decree?
3. How is data used for the purpose of the consent decree?

ii. Interviews with [internal investigations] on the routine data collection on use of force incidents

1. How do you see your role in the department?
2. Have you seen changes brought about by the consent decree?
3. How do you use data in your everyday processes?
4. Which initiatives have improved the collection of data?

iii. Attending a number of [CompStat] sessions to observe how data is used and integrated into the management framework.

2) Police uses of data and technology

In a second step we would like to speak to [the department's] staff about how they a) access data b) engage with data and technology, c) how data and technological policing tools affects and enhances their work, and d) how data and technology influences the management of the department. We aim for participants from varied levels of experience, rank and assignment. It would be valuable for us to participate in ride-alongs with officers on duty. This allows for a rich supplement to the interviews and observational data on themes that otherwise might not be readily articulated by the officers.

i. Interviews with detectives stationed centrally at headquarters and decentralised within districts.

1. How does data analysis inform your work?

2. What types of data do you use?

3. What data would you like to have that is not currently available?

4. Do you think that there are certain types of crimes that should allow for wider data access than others?

5. Where do you see potential for data-driven approaches?

ii. Interviews with officers about the use of numerous technological tools including social media data and other online resources, LPR, body work cameras, real-time crime analysis data and other data and technology-driven policing tools.

1. How important is technology to your work?

   a. How do you see technology and digitally-generated data as a tool for your job? What data and technology do you use in your decision making?

   b. How do you engage with the following technologies: LPR, BWC, in car cameras, real-time crime analysis?

2. What are the best ways of receiving/engaging with data? Should information be made available or sent proactively via briefings etc.?

3. Which sources of data do you consider the most credible?

4. What data would you like that is not currently available?.

5. How do you see the relationship between data driven insights and your own experience and knowledge? How does the data connect with what patrol officers know. Are officers confident of preserving their own discretionary judgement and experiential knowledge? Are there training needs to leverage greater value from data-driven insights?

iii. Interviews with supervisors about how the use of data driven insights and technological tools influence police work and their management of individuals and teams.

1. How does digitally-derived data affect, inform and enhance policing?

2. How can officer discretion be preserved in the face of the growth of data-driven insights?

3. How does data help you do your job more efficiently?

4. Does this data allow you to become better informed to enhance overall management of the department?

iv. Interview with the [crime analysts]

1. How do you see your role in the department?

2. What types of analysis do you carry out?

3. What data is available to you?

4. How does your analysis inform strategies and action?

5. What are the strengths and weaknesses of the data you are working with?

6. What data would you like to have? What data would you find useful?

11.3. Research outline for UK case study

University of Essex

The Human Rights, Big Data and Technology Project

Officer perceptions of data-driven insights: The use of [DataVis] at [UK police force]

Researcher

Daniel Marciniak (PhD Candidate at University of Essex), contact: d.marciniak@essex.ac.uk

Research Outline

[The police force] has given officers at every level of the force extensive access to data visualisations and predictive analytics enabling them to be their own analysts within a self-service environment. The system allows officers to triangulate the newly available digital information with the tacit knowledge about the communities they work with. The proposed study examines how officers of different experience, rank, and assignment make use of these tools. Its purpose is to gather empirical qualitative evidence to gain a general understanding of how data-driven changes can inform officer actions. The research is interested in how data-driven practices help inform and improve policing more generally and assess officers' perspectives to such approaches.

The researcher intends to collect primary data using qualitative methods including semi-structured interviews and, where possible, participant observation. The researcher aims to complete a minimum of 10 interviews with a mix of police officers with different experience, ranks, and assignments. Subject to consent from the participant, the interviews will be audio recorded and transcribed.

The researcher takes the position that the research subjects are experts in their professional fields and have the potential to reveal important insights that may not be anticipated at the outset. The research question and example interview questions below shall serve as an orientation towards the main research aims and the kind of questions the researcher is going to ask. Participants will be given room to voice their own perspectives and experiences.

Research Questions

A) Triangulation of data-driven insights and tacit knowledge:
   a. How does the data inform your decision-making?
   b. How do you see the relationship between data-driven insights and your own experience and knowledge?
   c. Which elements of [DataVis] do you use?
      i. How do you use the risk scores available to you?
      ii. What are your experiences with the mapping feature of [DataVis]?

B) Perceived changes brought about:
   a. Has the availability of data through [DataVis] changed your work? How?

C) Evaluation:
   a. Would you rate the information available to you as reliable and objective?

b. What opportunities and risks do you see?
c. Which aspects of [DataVis] do you find most useful?
d. What data would you like to have that is not available to you at the moment?

Research Ethics

- The research is subject to strict ethical standards - covering issues including but not limited to consent, anonymity, appropriate data handling and participants' right of withdrawal - in advance of any fieldwork. The proposed project has received ethical approval from the University of Essex in accordance with accepted international standards of ethics for social science research.
- Participants will receive an information sheet informing them about the research goals and providing them with the contact details of the researcher and the relevant ethics body at university.
- Participants will then be asked to fill a confidential consent form to ensure they are fully informed of and willing to participate in the research. In cases where this is not practical consent will be audio-recorded. This will be the case with any interviews conducted via phone calls.
- The researcher is committed to upholding participants' anonymity. Transcripts will be anonymized by replacing any type of identifying information such as name, rank, location or position within the organisation. This information will be held separately to the data.
- Only the identified researcher will have access to the data. Data will be stored securely.

Action Plan

4) *Recruitment*: The research will begin by recruiting research participants supported by the department. This would be most effective, if the researcher's contact information is shared with possible participants in the force. The researcher would aim to speak to between 10 and 15 officers with different experience that work in **neighbourhood policing, investigations, offender management and as supervisors**. Ideally, the researcher would be able to accompany 2-4 police officers on duty.
5) *Interviews*: Interviews can be conducted wherever and whenever suits individual research participants. This includes the possibility of phone interviews. To maintain objectivity and independence, interviews will be scheduled by interviewees and interviewer.
6) *Outputs*:
   d) The findings from this study will contribute significantly to the researcher's PhD thesis.
   e) The researcher will also seek independent publication of the study's findings in academic journals. These will contribute to the understanding of the use of data-driven insights in policing. The intention is to fairly represent interviewee's perspectives in the academic literature.
   f) A plain language report of research findings or other internal documents, briefing notes and reporting tools that are deemed useful to [the police force].

pant information sheet

Participant Information Sheet (07/07/2017)

Project Title: Predictive Policing: A change in the generation of suspicion?

My name is Daniel Marciniak. I am a doctoral researcher on Work Stream Two (Surveillance and Human Rights) of the Economic and Social Research Council and University of Essex-funded Human Rights, Big Data and Technology Project. I would like to invite you to take part in a research study. This document sets out key information about the focus, approach and ethical guidelines governing the project. Also listed are contact details for named individuals holding overall responsibility for the project and its ethical standards of research.

1. What is this specific research study hoping to achieve?

This research study will be based on a series of qualitative interviews. The aim of these interviews is to gain a greater insight into what 'predictive policing' means, the reasons for which it is adopted, and the ways in which it transforms policing. Results from this study will inform research carried out in the Human Rights, Big Data and Technology Project.

2. What is the Human Rights, Big Data and Technology Project?

The Human Rights, Big Data and Technology Project is a five-year project funded by the Economic and Social Research Council ('ESRC') and the University of Essex. It is housed at the Human Rights Centre of the University of Essex. The project is divided into four work streams:

- Work Stream One: ICT, Big Data and Human Rights
- Work Stream Two: Surveillance and Human Rights
- Work Stream Three: Health and Human Rights
- Work Stream Four: Advancing Human Rights and Humanitarian Responses Through Big Data

More information about the project as a whole can be found at: www.hrbdt.ac.uk. An up-to-date list of researchers can be found at: www.hrbdt.ac.uk/about-us/our-team/#researchers.

3. Why am I approaching you?

I am seeking the involvement of individuals within the police services and security agencies, as well as individuals from organizations that produce predictive policing technologies and supply such technologies to policing organizations, researchers that contribute to the development of predictive policing technologies, regulatory bodies and/or individuals from a range of non-governmental organizations that focus on scrutinizing police activities.

4. What will be involved in participating?

The (group) interviews will be semi-structured and will take place in a location of your choosing. It is envisaged that the interviews will normally take place within your organization, subject to invitation.

Interviews are scheduled to last around 45-60 minutes and will relate to the main research aims of the project, namely exploring participants' experiences and understandings of predictive policing and its uses. More specifically, these questions will seek to focus on:

- The types of predictive policing practices;
- The reasons for their adoption;
- The efficacy of such practices;
- The ways in which performance is analyzed and systems subsequently improved; • Anticipated ethical concerns and the ways in which these are addressed;
- The ways predictive policing technologies shape operational practice.

5. How will the data be used?

The interview will be audio recorded if you consent to this. The audio recording will only be used to ensure the accuracy of the transcription and will be destroyed once the transcription process is complete. You also have the option to undertake the interview without an audio recording.

The audio recording and/or any interview notes will be transcribed, anonymized (i.e. anything that could identify you removed including your name, organization and position within the organization) unless you consent to having your data attributed to you by name and analyzed for the research. Extracts or observations from the interviews may be written up in publications that arise from the research.

The transcript and/or any interview notes can be shared with you upon request. To ensure that you receive this before any analysis takes place I strongly encourage you to contact me **within two weeks of participation.**

The personal information you provide, such as your name, organisation and contact details, will be treated confidentially and personally identifiable details will be stored separately to the data. Data will be digitally encrypted and securely stored. Personal details will be replaced with an anonymised ID number. Any personally identifiable details will be destroyed once the analysis is completed, or at the end of the project if it is required for systematic comparisons of methods and techniques.

As a participant you have a right to request to see any data or personal information held about you. If you wish to do so, please contact me.

In order to archive the data gathered within this project and to make it available for future research, it will be offered to the UK Data Archive. This will be done following the above principles of data anonymization unless you consent to having your data attributed to you by name. The UK Data Archive is specialised in the secure storage and management of economic and social research data.

6. What are the benefits of taking part?

You will have the opportunity to participate in a research study on an important issue. The information that you provide will be used to inform a thesis on predictive policing. It will also feed into the Work Stream's research on understanding the human rights impacts of the use of technology and big data. I will disseminate my research findings in a variety of formats.

7. Are there any risks involved?

The central risks of participating in this research interview include concerns over anonymity, correct representation of the interviewee's position and participant unwillingness to continue his/her engagement with the research once it has started. I have anticipated these risks and have implemented measures to mitigate them.

Any interviews will have gained ethical approval from the University of Essex prior to taking place. This research is guided by the British Sociological Association standards of ethical research and prioritizes the wellbeing of the research participant above all other concerns.

8. How do I withdraw from the research?

Participation in the interviews is entirely voluntary. I will provide information about the research and give you an opportunity to ask questions at the beginning of the interview. I will then check that you agree to continue. You can exit from the interview at any time, or you can ask me to temporarily stop the interview if you wish to stop participating. You do not need to provide an explanation for this and there will be no penalty for doing so.

If you retrospectively want to withdraw from the research after the interview, please contact me. Please note that there are certain points beyond which it will be impossible to withdraw from the research – for instance, once I have published the results of the research. Therefore, I strongly encourage you to contact me **within a month of participation** if you wish to withdraw your data.

9. Do you have any questions?

You can contact me at:

Daniel Marciniak
Essex Law School
University of Essex
Wivenhoe Park
CO4 3SQ
Colchester

d.marciniak@essex.ac.uk

You can contact the PhD supervisor, Prof Pete Fussey, at:

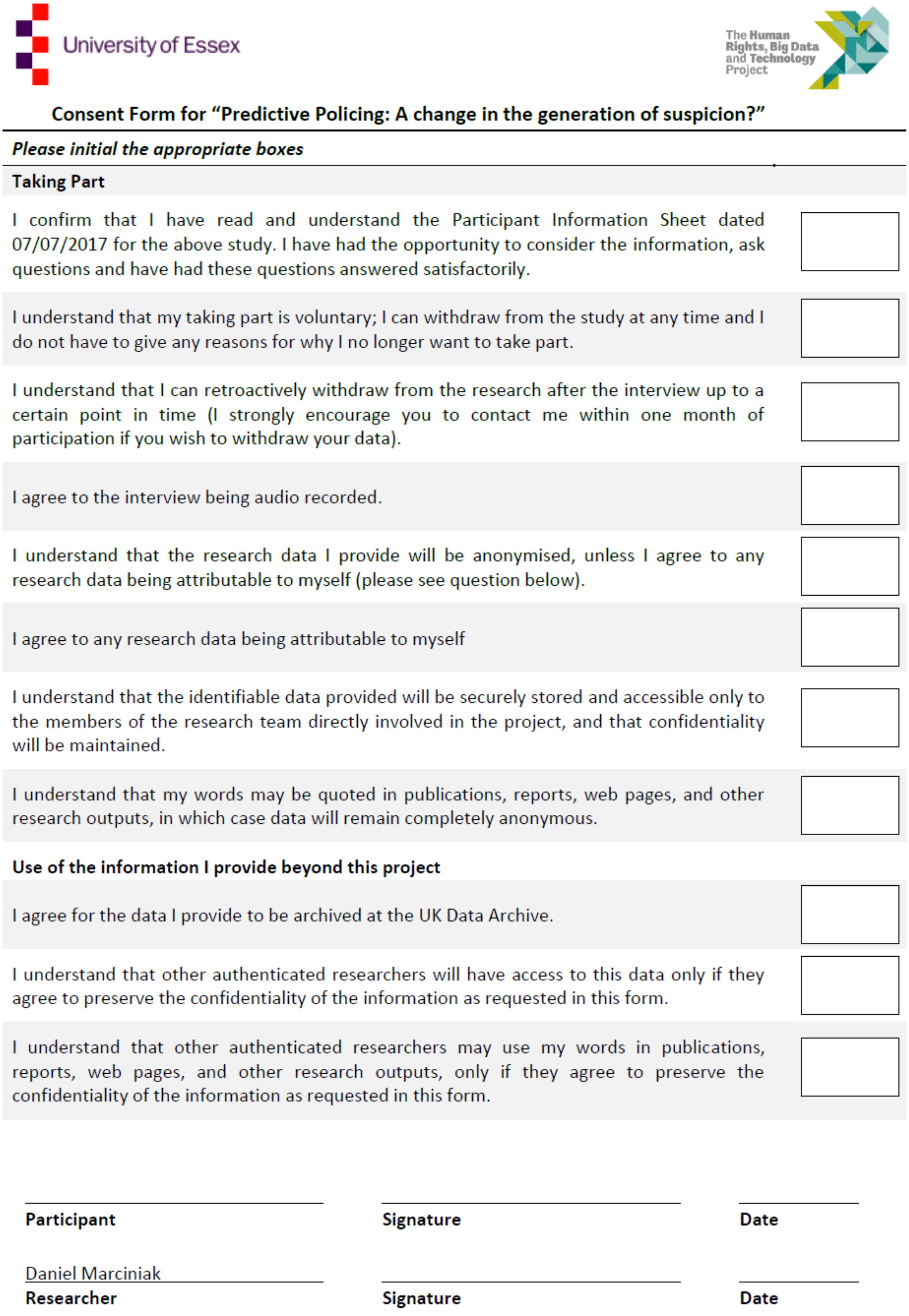
Department of Sociology
University of Essex
Wivenhoe Park
CO4 3SQ
Colchester

01206 872748
pfussey@essex.ac.uk

10. Do you wish to make a complaint?

If you have any ethical concerns about any aspect of this project, you should ask to speak to the researcher Daniel Marciniak (d.marciniak@essex.ac.uk) in the first instance. If you remain unhappy you can contact my PhD supervisor Prof Pete Fussey (pfussey@essex.ac.uk). If you wish to complain formally you can do this by contacting the Research Governance & Planning Manager, University of Essex, Wivenhoe Park, Colchester, Essex, CO4 3SQ or by email at sarahm@essex.ac.uk.

11.5. Consent form



University of Essex

The Human Rights, Big Data and Technology Project

Consent Form for "Predictive Policing: A change in the generation of suspicion?"

Please initial the appropriate boxes

Taking Part

I confirm that I have read and understand the Participant Information Sheet dated 07/07/2017 for the above study. I have had the opportunity to consider the information, ask questions and have had these questions answered satisfactorily. □

I understand that my taking part is voluntary; I can withdraw from the study at any time and I do not have to give any reasons for why I no longer want to take part. □

I understand that I can retroactively withdraw from the research after the interview up to a certain point in time (I strongly encourage you to contact me within one month of participation if you wish to withdraw your data). □

I agree to the interview being audio recorded. □

I understand that the research data I provide will be anonymised, unless I agree to any research data being attributable to myself (please see question below). □

I agree to any research data being attributable to myself □

I understand that the identifiable data provided will be securely stored and accessible only to the members of the research team directly involved in the project, and that confidentiality will be maintained. □

I understand that my words may be quoted in publications, reports, web pages, and other research outputs, in which case data will remain completely anonymous. □

Use of the information I provide beyond this project

I agree for the data I provide to be archived at the UK Data Archive. □

I understand that other authenticated researchers will have access to this data only if they agree to preserve the confidentiality of the information as requested in this form. □

I understand that other authenticated researchers may use my words in publications, reports, web pages, and other research outputs, only if they agree to preserve the confidentiality of the information as requested in this form. □

Participant	**Signature**	**Date**
Daniel Marciniak		
Researcher	**Signature**	**Date**

11.6. Codes in the US case study

- 1 Technological Practices
  - Accountability, Insight
  - Aesthetics, Presentation
  - Age, Attitude, Adoption
  - Aggregation
  - ALPR
  - Analogue
  - Bank Records
  - BOLO
  - Breakdowns, Workarounds
  - CAD
  - Categorization
  - Change
  - Warrants
  - Counterveillance
  - Datawork
  - Deception
  - Digi-Ticket
  - DNA
  - Efficiency
  - Evidence
  - Face Rec
  - FIC, EPR, other DB
  - Filter, Search, Pattern, Puzzle
  - G Drive
  - Imagination, Futures
  - Maps
  - Pawn DB
  - Phones
  - Proficiency, Training
  - Radio, Dispatch
  - Reliability, Trust, Verification
  - Sense Making, Understanding
  - ShotSpotter
  - Social Network Analysis, NIBIN
  - Social Media
  - Strategy
  - Supervision, Tracking of Police
  - Tips
  - Unnamed Program
  - Vehicles
  - Video
    - BWC and In-Unit
    - Covert
    - Private Cameras
    - RTCC
  - Web
- 2 Assemblages
  - Relations with Companies
  - Relations with other Law Enforcement
- 3 Space and Time
  - Alerts
  - Events
  - Navigation
  - Structuring Process
- 4 Improvements
- 5 Connectivity and Association
- 6 Visibility
  - Of the Police
- 7 Method
- 8 Various
  - Adoption
  - Discretion
  - Investigation, Suspicion

11.7. Codes in the UK case study

Accountability
Adoption, Opinion
Alert, Visibility
Inside
Analysis, Sense-making , Data Literacy
Fact-Making
Filtering
Assemblage
Availability of Data
Breakdown
Comparison with Others
Consequence
Areas
Offenders
Critique
Data Power
Buying
Objectivity and Bias
Purpose
Responsibility
Data Quality
Data-Work
Definition
Demand
Diffusion and History
Actors
Evaluation, Effectiveness
Future
History
Method
Presentation
DataVis
Requirements
Risk, Prediction
Area
Offender
Time and Place