PREDICTIVE POLICING AND THE POLITICS OF PATTERNS

Mareile Kaufmann[*], Simon Egbert and Matthias Leese

Patterns are the epistemological core of predictive policing. With the move towards digital prediction tools, the authority of the pattern is rearticulated and reinforced in police work. Based on empirical research about predictive policing software and practices, this article puts the authority of patterns into perspective. Introducing four ideal-typical styles of pattern identification, we illustrate that patterns are not based on a singular logic, but on varying rationalities that give form to and formalize different understandings about crime. Yet, patterns render such different modes of reasoning about crime, and the way in which they feed back into policing cultures, opaque. Ultimately, this invites a stronger reflection about the political nature of patterns.

Key words: predictive policing, patterns, data, algorithms, politics

Introduction

Software packages for predictive analytics have become increasingly implemented in police work across many countries (Bennett Moses and Chan 2016; Fyfe *et al.* 2018). Their analysis relies on the identification of patterns that indicate spatial and temporal distributions of crime. Patterns, in other words, make visible and give form to knowledge about regular occurrences of crimes that lie hidden in data sets. This trend grants patterns a considerable authority: they provide no less than the epistemic foundation for data-driven analyses of crime. In fact, they are the only way through which a software's algorithm can 'know' or conclude about the occurrence of crime in society. In the context of predictive policing, the promise of the pattern is thus to serve as a base for the extrapolation of possible criminal futures and to render those futures actionable for prevention programmes. This means that patterns pre-structure how the police act upon crime and society at large. Moreover, patterns legitimize this trend towards automated policing rationalities as they provide interventions with calculative rationalities.

Even though patterns are paramount in statistical analyses, they have received comparatively little attention in the literature that engages with crime and security (for exceptions, see Weisburd *et al.* 2009). Rather, contributions from criminology and beyond have focused on the modes in which information has become a key part of police work or modern society at large (Manning 1992: 352). Policing literature highlights fundamental distinctions between spatial (i.e. 'Where to police?') and object-related ('Whom to police?') modes of predictive analyses (Perry *et al.* 2013; Bennett Moses and Chan 2016; Ferguson 2017). Others foreground the sociotechnical nature of

*Mareile Kaufmann, Faculty of Law, Department of Criminology and Sociology of Law, Oslo University, St. Olavs Plass 5, 0130 Oslo, Norway, mareile.kaufmann@jus.uio.no; Simon Egbert, Department of Social Sciences, Institute for Criminological Research, Universität Hamburg, Allende-Platz 1, 20146 Hamburg, Germany; Matthias Leese, ETH Zurich, Center for Security Studies, Haldeneggsteig 4, 8092 Zurich, Switzerland.

predictive data analyses (Babuta 2017; Sanders and Condon 2017) and argue that predictive policing represents both a continuation, but also a transformation of analogue police practices in terms of time and scale (Brayne 2017; Chan and Bennett Moses 2017; Smith *et al.* 2017). Against the backdrop of data analyses for security purposes, some have put forward warnings about the perpetuation of existing social imbalances and injustices—especially vis-à-vis the authority of algorithmic technologies (Gill 2000; Harcourt 2007). These coincide with a larger trend towards a 'pre-crime society' (Zedner 2007) including 'prepressive' (Schinkel 2011) and other pre-emptive modes of governing crime (Harcourt 2007; Mantello 2016; Andrejevic 2017) that intervene in a 'world based on patterns available only to those with access to the data and the processing power' (Andrejevic and Gates 2014: 190). These critical literatures are crucial for an understanding of data-driven security practices in the context of policing and power.

In this article, we want to expand on the idea that information does not only inform, but also creates form (Heidegger 1997 [1957]: 182). We extrapolate Heidegger's argument by analysing patterns as the epistemological foundation of predictive policing software, and by studying the way in which they are productive in society. As we demonstrate throughout this article, patterns vary greatly in form and explanatory power. Thus, our critical argument is not one that *subtracts* something from the pattern by debunking the logic that it embodies and reducing it to a singular mode of operation. Rather, we seek to add, multiply and gather the many positions and rationalities that patterns stand for and give form to. With that, we suggest that patterns are less a 'matter of fact' than a 'matter of concern' (Latour 2004). As matters of concern, they depend on specific algorithms[1] and databases that bring them into being, as well as on decisions whether a pattern is considered meaningful in the specific context of predictive policing. We trace the different aspects, logics and decisions involved in the production of patterns.

We build our argument in four steps. First, we introduce method, empirical data sources and methodology. Then we engage the notion of the pattern vis-à-vis the increasing digitization of police work. Third, drawing on our empirical research and the conceptual discussion on patterns, we present examples for distinct patterns and approaches of pattern detection in policing. This includes our core contribution—four ideal-typical styles of predictive analytics that illustrate how patterns give form to knowledge about crime. Before concluding, we put the epistemological authority of patterns into perspective by discussing the limits of pattern-based policing strategies, such as their focus on rule-based crime, their conservative nature, their tendency to restrain reflection about how patterns come about and the way in which they influence our understanding of crime. Analysis and discussion are not only informed by academic literature, but also by critical voices from inside the empirical field.

Methodology

The development of our argument builds on qualitative empirical research carried out between 2016 and 2018. Data were collected mainly in the form of 48 in-depth

---

[1]An algorithm can be defined as 'a mathematical recipe, formulated as a finite set of rules to be performed systematically' (Martignon 2001: 382), thus producing as outcome a solution to a predefined problem.

interviews with police officers from Norway, Germany and Switzerland (strategic, tactical and operative level; police academy instructors), as well as with programmers and representatives of software companies from Europe, the United States and Australia. The analysis covers a total of seven different software models for predictive policing and specific forms of local implementation. All interviews have been recorded and transcribed. Those conducted in other languages than English have been translated by the authors. The interviews were complemented with multiple ethnographic field studies, mainly in the form of observations that provided us with an opportunity to analyse how predictive policing methods become a part of everyday police work. In some instances, we were also given access to internal police documents with regard to prediction software, such as documentation, instruction manuals and best-practice guidelines. Per agreement with our informants, all collected data have been fully anonymized. Interview transcripts, field notes and documents have been coded using qualitative data analysis software. The analysis of coding clusters on 'data/data analysis' and 'patterns' eventually yielded the four ideal-typical styles of pattern detection that we discuss in this article. Throughout our analyses, we tie each style to concrete empirical material, such as quotes, observations or notes.

The way in which we combined different empirical data reflects our methodological approach: in order to understand how patterns come about and how they influence policing, mere observation or software study would not have been sufficient. Especially the interviews helped us to prompt explanations and contextualize descriptions of work done by police officers, software developers and programmers alike. The multiplicity of empirical data provided us with information about the ideas and rationales underlying predictive policing, the work processes such as the collection of data or the detailed functioning of software, as well as the perspectives of manufacturers and police forces on software implementation.

While our research is geographically limited to local and regional examples of implementation in the Global North, these limitations do not necessarily interfere with our findings. The assumption that criminal behaviour shows forms of regularity over time, and that these patterns can be identified and used for predictive analytics, is a universal driver for the development of policing software. It is on this level that our analysis takes place. It hones in on the variegated ways in which patterns give form to knowledge about crime, how they intend to make human behaviour discernible and actionable, and foregrounds the sociotechnical processes that surround predictive policing. In doing so, we systematize the manifold ways in which patterns become part of crime intervention strategies and demonstrate that neither the notion of the pattern itself, nor the ways in which patterns are made visible, are a given. On the contrary, the identification of patterns, their reconnection to assumptions and knowledge about the world, and their application in preventive action imply epistemologically productive struggles that are tied to statistical methods and criminological theories.

Patterns Relaunched: Policing with Digital Data

Digital data, as Kitchin (2014b: 100) points out, 'only have utility if meaning and value can be extracted from them'. The extraction of meaning is generally related to the idea of the pattern that sketches out a 'statistically constructed future' (Schinkel 2011: 367).

With regard to policing, one software developer summarized the rationales at work as follows: 'It is really easy: if I recognize patterns, I can look into the future, and when I can look into the future, I can shape the future' (Int. O).[2] A pattern, per definition, is something that comes in a regular, intelligible form. Within a data set, this intelligibility refers to coherent interrelations between certain variables and their corresponding classification (Waske and Beneditksson 2014: 503). However, what can be considered coherent, what counts as a variable and how they are categorized, so we argue in this article, varies across the different software models. Equally, patterns vary according to the data they are based upon, as well as the analytical approaches applied to data collection and pattern identification.

The importance of patterns in policing must be read against a long-standing scientification of police work and the adoption of technological tools (Ericson and Shearing 1986; Ericson and Haggerty 1997; Manning 2008), which eventually led to the widespread digital practices that we encounter today. Police departments are now, at least in theory, capable of processing unprecedented amounts of data, and of putting insights from algorithmically supported analyses into practice. Accordingly, discourses of predictive policing are often inspired by narratives of Big Data and data mining (Beck and McCue 2009; McCue 2015; Babuta 2017) that echo a certain belief that the accumulation of sufficiently large amounts of data would render the world, if not better understandable, at least better predictable (Anderson 2008). Critical scholars have cautioned against such lopsided tales and have foregrounded the amount of work that is required for large-scale data analytics (Boyd and Crawford 2012; Kitchin 2014a), particularly in the field of policing and criminal justice (Bennett Moses and Chan 2016; Maguire and McVie 2017).

Our empirical material supports this observation, as two main implications of digitization for police work became prevalent throughout the analysis. First, there is a considerable variety in the scale of available and analysable data. Police departments work with anything from small to big data sets (Int. O; Int. P; Int. T). They work with data that are produced by themselves, or that comes from secondary sources such as public administration and publicly accessible parts of social networks. Some additionally buy commercial data to support their analyses (Int. O). This latter practice is supported by Interviewee F who argues that the expansion of available data towards larger and more disparate data sets allows for a greater variety of patterns to be identified: 'The digital approach allows you to work with much larger quantities of data, which allow you to recognize patterns in a way that analogue approaches just aren't gonna be capable of doing'.

Second, digital data provide for calculability in new ways, which are used to rationalize decisions about where and upon whom to intervene. One interviewee foregrounded that

[data] need to be calculable. If not, you cannot run the models. You need to make a definition and you need data on that. If you don't have data, it doesn't matter what your definition is, because you cannot do anything about it. (Int. K)

If policing becomes 'all about the calculus' (Int. K), new ways of rationalizing human behaviour emerge, as assumptions about behaviour, and especially about the

---

[2]Int. = interviewee, FP = field protocol, Doc. = police document.

demarcation between legal and illegal behaviour, need to be translated into digital terms. In other words, the social needs to be operationalized in such a way that it can be rendered computable through measurements of movement, interpersonal associations, emotions and the like. Calculability is therefore underpinned by a strong sense of classification, bureaucratization and compartmentalization.

This sense of classification is sustained in digital analytics (Kaufmann and Jeandesboz 2017), whether these are based upon large and disparate or small and homogeneous data sets. Dalton and Thatcher (2014: n.p.) draw attention to the fact that in 'its production and interpretation, all data – "big" included – are always the result of contingent and contested social practices that afford and obfuscate specific understandings of the world'. The production and selection of data is thus as much based on specific decisions about what and how to measure as is the ensuing analysis that is predicated upon the questions that one wishes to address to a data set (Kaufmann 2018). In Dalton and Thatcher's (2014: n.p.) words, 'all datasets are necessarily limited representations of the world that must be imagined as such to produce the meaning they purport to show'. This becomes quite tangible when looking at the amount of preparatory work that goes into rendering data sets analysable for crime prediction software. Our field notes describing observations of software operators show that the transfer of data from the police case processing system to the crime prediction software already entails numerous selection and translation processes in order to render data sets analysable (FP A; FP B; FP C). In addition, one interviewee hinted at the problems that police face when seeking to streamline and harmonize data from disparate sources:

We have very different information and we try to level up and to have very generic categories and that is what the police doesn't have. There is a lot of categorizing that isn't very logic. All over the place. Different labels on the same information and vice versa. (Int. D)

The work of categorizing becomes, for example, apparent in prediction software that seeks to distinguish professional from non-professional offenders based on their behavioural patterns. One software model captures behavioural patterns by means of crime-related variables. For instance, the theft of heavy goods would point to non-professional offenders, as heavy goods cannot be sold and turned into cash easily. Stealing jewellery, electronics or cash would, on the other hand, point to professional criminals (FP A; FP B; FP C). Another software model assesses offender behaviour via a score system. For example, if a window has been professionally drilled in order to access the crime scene, a certain amount of points is added to the case's overall score. If windows are smashed, points are subtracted from the overall score. If, after the analysis of all available information, a certain threshold score is reached, the offence will be categorized as professional conduct, which indicates that the case may belong to a series of burglaries (Int. Q; Int. U; FP D). These attributions illustrate the contingency and the creative work involved in the prediction of crime.

A closer look at the functioning of different software models then demonstrates that predictive policing is not based on a singular or abstract rhetoric of *the* pattern that responds to the users' queries. On the contrary, different understandings of the world and different patterns are at work—some of which might even be combined within one single software model. To illustrate this point, we now provide a brief overview of different kinds of patterns that are used for creating predictions before we move on to an analysis of ideal-typical prediction styles.

The quintessential category of patterns for predictive policing is the spatial one. The increasing use of GIS-tagging or digitized geographic information in police records has relaunched earlier approaches to the pen-and-paper mapping of hotspots (Chainey and Ratcliffe 2005; Bowers and Johnson 2014). Vis-à-vis its analogue counterpart, digital geographic information can be more easily integrated and processed, especially when it is collected over long periods of time. Such data can be used to identify spatial regularities within historical material and to project them into the future as risky areas. Geographic information is then key to targeting risk areas, such as 'the neighbourhoods that are preferably visited by those people that cause certain patterns' (Int. L). The near-repeat pattern is a specific subcategory of spatial patterns and currently one of the most common approaches to predict crimes. The 'Near-Repeat Hypothesis' (Townsley *et al.* 2003) has been formulated and most prominently tested in relation to domestic burglary. It is based on Rational-Choice theory, and the assumption that a successful offender will strike again within close spatial and temporal proximity of the initial offence, since the offender is familiar with the local circumstances and able to assess the benefits and risks of another raid (Johnson *et al.* 2007; Farrell and Pease 2014).

It is no surprise that such ideas of 'geographically applied criminology' (Middendorf and Schweer 2016: n.p.) coincide with the trend to relate as much information as possible to spatial coordinates. Indeed, ambitions to chart available data onto geographical maps are not limited to police or juridical efforts alone. For example, the Norwegian Mapping Authority's ('Kartverket') initiative to redefine what counts as geographic data plays into the development of predictive policing software (Int. D).

It is important to note that many software models identiyfing spatial patterns are not designed to pay attention to the individual level:

If you are considering looking at people at all, then you may want to anticipate where a lot of people would be […] If there is a lot of crime that probably means that there is a lot of people at the location. (Int. G)

Indeed, when scrutinized more closely, many of the utilized variables appear to be proxies for population density (Perry *et al.* 2013: 55). Even though the amount of different geographic patterns is as vast as the data that they are based upon—including weather and census data, information about ongoing events etc.—the variable of people and their movement is still a crucial one in geographic patterns (Int. O).

In addition to spatial patterns, we do find temporal patterns in predictive policing software. Both are closely related and usually combined, as criminal offenses are mapped over space *and* time. A different temporal pattern is in use when time itself is a determinant, namely when software predicts *at what time of day* incidents tend to happen in specific areas. Beyond spatial and temporal patterns, we also find behavioural ones. If the spatial coordinates of offenses are recorded over time, then effort is directed at distinguishing between different types of offenses or criminal behaviour.

Not all behavioural patterns are mapped in relation to geographic and temporal coordinates. Some are recorded in different kinds of maps, for example networks of relations or transaction records, in order to identify patterns in activities, deals, agreements, communication or the like. Such behavioural patterns are less likely to be used in software to be deployed in everyday and street policing situations. Rather, they are components in software for the intelligence police, which logs, maps and targets

individuals and their networks. While most police databases do not contain detailed information on individuals due to data protection regulations, future software versions that include such information are thinkable. One example is the Chicago Police Department's 'strategic subject list' (Saunders *et al.* 2016).

Patterns Rising: An Analysis of Prediction Styles

As predictions are increasingly based on the analysis of multiple data sources, it becomes prevalent how different styles of pattern identification produce knowledge in particular ways. In other words: the reasoning about crime varies with the chosen format of pattern identification. The analysis of our empirical material has shown that the shape of a pattern and the insight that it grants to police officers primarily depend on three factors: the available data, the variables that are included in the analysis and the way in which these are combined. In addition, most algorithms are designed to be deployed for a specific crime, a particular situation or selected group of offenders, which further determines the patterns that are meant to be found (Int. T; Int. V; Int. W). The combination of the available data plus the algorithm that evaluates the data ultimately determines the pattern—and theoretically the success of the software for a specific purpose.

Even though this seems straightforward, the variations of available data and conceivable algorithms exceed available software models on the market. This is where our key argument ties in. Most sociopolitical analyses of algorithms, Ziewitz observes, currently follow the same template of 'conventional politics', which answer the question 'what an algorithm actually *is*' with a general and 'disappointing "we don't know, but it surely is very powerful"' (2016: 6). Our analysis moves away from an understanding of algorithms as a singular entity with elusive powers, but seeks to be more concrete and focused on pluralities in its argument. Our empirical material shows that prediction algorithms do not follow one analytic logic. Rather, we find many styles of prediction, each driven by their own arguments and epistemic approaches to crime. What remains central in all software is that any prediction needs to be given a form. Yet, our analysis draws attention to the way in which each process of pattern identification is the result of decisions taken by software manufacturers, engineers, programmers and users, of data collected and algorithmic workings. For example, already the parameters used to decide whether a pattern is considered *meaningful*, vary considerably. In addition, some software developers take trial runs as precedence for the refinement of the algorithm (Int. G; Int. B), while others spend more effort on designing the algorithm in advance (Int. A; Int. D; Int. F; Int. I; Int. J; FP D; FP E).

The studied software models inspired a division of pattern identification into four styles, which illustrate their differences in an ideal-typical way. For a more systematic overview, these styles of pattern identification can be organized along three axes: (1) the use of axioms or parameters in programming algorithms that identify patterns; (2) the amount and kind of available data; and (3) the focus object of the pattern. Within the actual software models, the boundaries between each style tend to be blurred, and some software models combine aspects of different styles. Yet, generally we find that crime-related pattern detection varies from very broad and inclusive approaches, to very specific, select and targeted procedures. This variation in approaches is also

reflected in the sequence in which the styles are presented. Table 1 summarizes the styles of pattern identification.

We will now engage with each style in more depth and illustrate them with empirical examples. In order not to compromise the anonymity of our informants, we will not name any specific software models (for an overview of currently available software tools, see for example Ferguson 2017; Wilson 2018). Through that, we also underline that we seek to discuss prediction software on a general level. Thus, the styles presented here should be understood as narratives that allow us to capture the politics of patterns, and as analytic tools to recognize these politics in different software models.

Style 1 is not based on theories about the concrete intentions of offenders, but on assumptions about vulnerable environments. The degrees of vulnerability of certain areas would thus be influenced by structural factors such as the socio-economic make-up of a neighbourhood, traffic infrastructures such as highways or public transport stops, or live data on weather or mass events (Int. G; Kennedy *et al.* 2011). The characteristics of certain areas are then correlated with geo-referenced crime data, from which the degree of vulnerability of the environment is inferred. Analyses thereby usually invoke large and open-ended data sets, as these can include information that could serve as an indicator for spatial vulnerabilities. For example, census data are popular within this style of prediction (Int. O), as it can provide meaningful insights if analysed

[i]n terms of: what drives community crime patterns? Things like socio-economic status, residential stability, linguistic isolation and race and ethnicity - they are […] all available through a census. And while those things don't necessarily cause crime directly they provide you with information about the characteristics of places that might encourage or promote crime events to occur there. (Int. A)

Patterns are here not necessarily tied to specific types of offenders. On the contrary, the assumption is that any member of society might be seduced to commit crime if the possibility in the form of a vulnerable space presents itself.

Style 2 follows a different rationale as it sets the scope on persons rather than on space. It is based on general assumptions about rational offender behaviour and seeks to identify pattern-based criminal activity in a broad sense. While predictive policing is

TABLE 1   *Styles of pattern identification*

	Style 1	Style 2	Style 3	Style 4
Axioms/parameters	Environmentally related factors	General Theory on routine activity + selected axioms and empirically gained parameters	Specifically selected theory and axioms	Rule-based behaviour in actual individuals
Data	Big Data, no preselection	Big Data or selected data sets	Selected or small data sets	Selected data sets with additional narrative entries
Focus object	Spaces in which populations move and act	Anyone acting according to patterns, or routine offenders, or individuals	Professional, routine offenders	Individuals and their networks

often underpinned by notions of Big Data and the power of correlation in order to find new patterns about crime, some of our informants (Int. J; Int. H; Int. J) emphasized that simply 'crunching numbers' (Ayres 2007) does not necessarily work when it comes to criminal behaviour. Predictive policing without theory would lead to distortions in the analysis and would likely produce patterns that turn out to be spurious correlations rather than imprints of actionable distributions of crime. As Interviewee H explains:

If you don't have good [...] parameters you might define problems that are not really there. If you set the parameters wrong you get a huge heat map and it looks like the whole city is burning. But it's not really burning, it's the parameters in the GIS system and when you present the patterns from the data then you are actually telling a story that's not true.

This is why some styles of prediction include parameters in the algorithm, for example crime generators or near-repeat patterns (Int. F) that are either derived from empirical experience or theory (Int. E). Some interviewees argued that the explicit use of such parameters in algorithmic analyses would actually render the analyses more transparent (Int. E; Int. I) as opposed to informing police officers' decisions implicitly. Most software models include at least some parameters. Style 2 can be empirically encountered in a broad range of software models, ranging from approaches that analyse large databases to approaches that operate with more select, small data sets (as, for example, crime data of the past few years for one specific offence in certain areas). Equally, the resulting patterns may focus on anyone acting according to patterns—professional criminal or not.

This is different in *Style 3*, which is a more distinct form of pattern identification. Here, algorithms are designed according to specific theoretical assumptions that can be refined with each new version of the algorithm. By basing the algorithm on theoretical axioms, the patterns it identifies are no longer the result of mere correlations without explanatory power. Patterns, here, reflect causes for crime or at least tie the identified pattern to an explanation. For example, if near-repeat patterns are used as a basis for predictions, the identified patterns can be further refined by the boost-hypothesis and the flag-hypothesis. Both hypotheses provide an explanation of the reasons for the occurrence of spatio-temporal patterns. The boost-hypothesis is based on offender rationality, assuming that criminal activity depends on factors like familiarity with the target neighbourhood or the absence of residents during certain times of the day. This would then enable the police to refine certain behavioural patterns accordingly (Int. T; Int. P; Doc. A; Doc. B). Interviewee L summarizes it like this:

You have to imagine this like a deep-sea channel where the shark positions itself. And not in shallow waters. Predators know where they can find something that is interesting for them. And you don't have these channels in any given area, but there is a certain pattern that is known to the offender. But we know that pattern now as well, because we have seen the trail before.

The flag-hypothesis, on the other hand, builds on arguments that we have already discussed with regard to Style 1, which takes insufficiently protected objects or places as a starting point to explain where crimes are committed (Johnson 2008; Johnson *et al.* 2009). Accordingly, the preparation of data requires a more selective approach in Style 3, since data categories that do not fit the respective theories would only distract the analysis from the identification of meaningful patterns (Int. J; Int. O). Often, this results in small data sets that are created and handled by the same police officers who

later act as software operators, and these software models target professional routine offenders. Routine, however, need not necessarily be expressed in terms of near-repeat patterns alone:

The near-repeat pattern is of course only one pattern. And it does not cover all burglaries. In some neighbourhoods, 35–40 per cent can be classified as near-repeat phenomena, but you also have to deal with the other 60 per cent. In the meantime, we have started to work with far-repeats[3], which is a completely different pattern. […] And that's why criminological research is so important: you have to keep analysing […] to recognize new patterns, and to develop new ways of analysis and new methods. (Int. L)

While professional and routine offenders are the focus of Style 3, individuals and their relations are the focus of patterns identified in *Style 4.* Here, the pattern takes the shape of a network around a particular person. Interviewee H explains this approach:

We use pattern recognition in intelligence systems where you put in intelligence knowledge and mostly make a social network – like who's connected to who – you make maps where you graphically visualize who knows who – to identify the most important criminal, who is the boss in the network, how is the network organised, how does it work, is it hierarchical, is it more integrated? So, there we have some patterns in intelligence databases, to know which criminals are the most important ones. (Int. H)

This approach is so far only used for intelligence police operations, since it requires specific (and costly) data about individuals. Whereas the other styles seek to predict behaviour on the aggregate level, the aspiration is here to find out why and how individuals respond to rules. Like any other prediction software, the system is flawed if the rules are deficient, but since the target objects are individuals and their specific behaviours and relations, the definition of rules and parameters is more laborious. The data used in such software are not only highly selective, but they may even be complemented with adding a story to the statistical material that can be used for data evaluation:

In this field you put in that kind of data and so on. But what about the story? There is a storytelling here. […] We have the free-text story and […] we have this search engine that automatically indexes the free text and you can navigate the free text by using indicators. (Int. D)

With the use of individualized rules, free-text story-data and individual offenders as target, this is the most specialized style of pattern identification in the studied examples and introduces an element of network analysis into prediction styles.

Despite all the variation between them, what ties all four styles of pattern detection together is their overarching aim: to produce actionable prognostic knowledge. The insights they offer must be accommodated in the day-to-day routines and organizational practices of the police without causing too much disruption (Int. O; FP E). The notion of the pattern appeals to this need for practicality, as it can be adapted to the specific needs of the organization. Indeed, the promises of the pattern are quite seductive: they reduce complexity and can be deployed to decipher insights that are hidden

---

[3]Such approaches apply the idea of near-repeats to rural areas. The higher level of social control in rural areas leads to a different repetition pattern of burglaries: offenders are not expected to strike again in the same village, but in the next. The prediction of crime sites would then be guided by roads, which are used to drive quickly from one crime scene to the next (Int. C.; Schweer 2018: 13).

in data sets (Int. X). Moreover, patterns can easily be visualized, whether in the form of geographical coordinates or in the form of network-relations, all of which seem to make their insights actionable for crime analysts and officers. As such, patterns embody the spirit of efficient law enforcement (Int. A; Beck and McCue 2009). This spirit could also be observed throughout our empirical material: following the desired progress of beat officers of moving from hotdogs to hotspots (Int. E), the reduction of complexity was considered necessary to identify those areas where police activity would be needed the most (Int. X; Int. P; Int. Y).

Patterns are thus not only a seductive key to the analysis of offenses as they promise to produce actionable knowledge, but they also unfold considerable epistemological authority. Challenging this authority is difficult, as 'anything that is not based on patterns cannot forecasted, and has to be excluded a priori' (Int. J). Indeed, without the identification of patterns, there would only be random information. Patterns are thus not just an argument that informs the idea of prediction, but they are its basic epistemological condition. What our analysis has demonstrated, however, is that even though the pattern is a condition to 'know' and predict crime, patterns neither follow a singular logic or reasoning, nor a singular style of identification. They give form to and formalize different understandings about crime, which are in turn based on specific ideas of governing crime. This makes patterns *political*. However, due to their reductive nature, patterns do not necessarily reveal these ideas. They do not disclose the assumptions and decisions that inform the design of algorithms. Rather, patterns have become emblematic for an advanced bureaucratization of the governance of crime. They speak to the increased collection of information just as much as they speak to digital methods of analysis and the promise of efficiency. Patterns are the shape that predictive knowledge about crime takes, and their epistemological status seems incontestable—at least in the context of forecasting.

Patterns in Perspective: How Patterns Interact with Policing Practices and Cultures

In this final part, we seek to put the epistemological authority of the pattern into perspective. The discussion elaborates on our key finding that—beyond the logic of forecast that any pattern is tied to—different patterns rise from different rationalities and understandings about crime. In other words: we see the authority of patterns, but show that patterns vary with regards to their informative value, their significance and the different stories about crime they tell. This finding needs discussion since patterns steer policing practices. They structure decisions, actions and foster different understandings about crime. We now reflect about the implications of patterned knowledge within policing and policing cultures, which we summarize in four pointed issues.

First, *patterns can only capture offenses that follow rules*. It does not take an outsider critic's role to understand and reflect about the implications of this. In fact, designers and programmers acknowledge (to their regret) that any behaviour that does not follow a pattern cannot be detected (Int. J). Thus, while offender rationality and vulnerability may be subjected to prediction models, some crimes of violence are often considered off the limits of reasonable modelling due to their emotional and spontaneous nature:

Most of the crimes that we really care about - the crimes of violence - those are by and large impulsive crimes, they are not well thought-out and it's not as if there is some plan that the offender is putting

together on how to beat the system. These are much more emotional and impulsive acts -so that [the rational planning] you are talking about really doesn't come into play. (Int. I)

Furthermore, if only offenses that follow rules and statistically identifiable clusters or cumulations can be identified, a sufficient number of crimes is needed to make predictions possible in the first place. In the words of one interviewee: if there is 'not enough crime' (Int. M)—prediction is ironically impossible. '[W]ith […] small numbers I cannot extrapolate a pattern' (Int. M). For example, case numbers in rural areas are often not high enough to generate statistically robust predictions. And even when predictions are based on large enough data sets, geographic patterns translate into generic predictions and focus on broader trends rather than generating specific predictions. Even when done at individual level (see Style 4), predictions are still based on rules and patterned epistemologies. Accordingly, predictions only ever say something about regularities and general trends. More customized or accurate statements are, however, not considered necessary. For policing purposes, it is generally considered sufficient to identify the 'main' patterns in order to push crime prevention to the next level: 'Quantitatively speaking, we do not have to uncover every mini-series. In fact, we are quite happy when we keep track of the main patterns' (Int. L).

However, identifying these main patterns is not easy. The spurious or irrelevant patterns found by algorithms outnumber the actionable ones. Distinguishing whether patterns are spurious or relevant is not only laborious, but when the amount of insignificant patterns is too high, attempts to predict future offenses ironically raise uncertainty rather than help handling it. On the other hand, the number of significant patterns should not be too high for predictive policing to work, since a too large risk area is not actionable for police forces (Int. O).

In addition, there is a difference between patterns of actual criminal activity and crimes that the general population worries about. Police departments are also starting to think about the latter category:

We tend to use crime data to identify hotspots or patterns or high-volume crime. But how do we use open social data to understand: what do [people] worry about, where do they feel unsafe, what kinds of crime do they worry about? (Int. H)

Second, *pattern-based predictions tend to be conservative and address symptoms.* Their premise is 'that the past is prologue' (Perry et al. 2013: 8). Patterns usually do not emerge from live data, but from historic data, and only through retrospective analysis can criminal behaviour be made visible. One interviewee describes a surprise in that respect: 'We knew that burglaries are not uniformly distributed across space. But we were in fact surprised that they are concentrated in such small areas' (Int. N). Due to its primarily historic focus, pattern-based prediction is mostly reactionary. It is a technology based on past data and designed for the identification of effects, sequences and correlations. Nonetheless, it is applied to future developments and ex-ante interventions, aiming to dispatch of police officers to places *before* crime happens. These leaps in temporality (i.e. from past data to future offense) and rationality (i.e. from effects to ex-ante interventions) are not only systematic gaps, but also confront practitioners with several challenges. For example, short-term situational factors will remain a problem. Even though the use of data has become accelerated with digitization, there will inevitably remain an unbridgeable gap with regards to the use of the most recent data. Especially crime

Downloaded from https://academic.oup.com/bjc/article-abstract/59/3/674/5233371 by University of Oslo Library, Library of Medicine and Health Sciences user on 10 January 2020

data tend to be less useful for prediction the more recently they have been collected, as they might still be subject to updates and changes due to ongoing investigations and data cleaning procedures (Int. P; Int. Q). Interviewee I agrees that analysing the most recent data is '[…] not the limit of the algorithm. The algorithm will do it. It's just that we haven't enough data about these immediate settings to forecast accurately' (Int. I).

A related organizational challenge is that once data are fed into the software and patterns are recognized by the algorithm, they also need to be 'recognized' by the practitioners. This is where patterns require interpretation:

There are so many changing patterns in society and I think that data obviously can assist in understanding society better and that they are a valuable input to the police. Next question is what to do with them? (Int. E)

This speaks to a problem pointed out by Perry *et al.* (2013: 12), namely that predictive policing is not about the predictions alone, but also about their correct implementation on the street. Patterns do signal *that* intervention may be needed, some patterns even provide information about the *kind* of intervention needed, but their explanatory power remains limited as contextual information is reduced. Patterns are mainly about form, not content. Even though some styles of pattern detection include causal reasoning about crime and thus provide the police with insights into the kind of offense addressed, the ambition of most predictive policing software is to handle symptoms, not root causes. Crime may be dealt with efficiently, but only at the surface (Bennett Moses and Chan 2016: 813; Andrejevic 2018: 102f). Interviewee F confirms:

And just to be clear: we're only focused on predicting where and when crime is most likely to occur. We don't predict why or how and who? Those are all things that our particular process doesn't focus on.

Such an understanding is further underlined by other interviewees, whose primary interests concern a decline of crime statistics within their assigned territory, thus favouring strategies of displacement over the presumably more difficult prevention or deterrence of crime (Int. P; Int. R).

Third, *the assumptions about offenses that are expressed in patterns feed back into cultures of policing.* Patterns have some aspects in common: they capture developments that follow rules and they address symptoms. As such, they are expressive of the larger trend to rationalize police work and render police forces more efficient. Patterns thus reinforce specific ways of thinking about crime and policing that are captured in the pattern's logic. Beyond that, however, the rise of patterns integrates more specific conceptualizations of crime and offenses in police cultures. At first sight, monitoring groups or places via patterns seems more acceptable than monitoring individuals, since patterned predictions take place on an aggregate and abstract level. One interviewee in fact wonders: 'If you actually use it to […] monitor patterns – is there any disturbance?' (Int. H). The answer is yes. Applying generic predictions and general trends to specific neighbourhoods easily results, via ecological fallacies and self-fulfilling prophecies, in the stigmatization of neighbourhoods and the people who live in them (Harcourt 2007).

Beyond that, some patterns can in fact be tied to actual individuals, as we have seen, for example, in Style 4 of pattern detection. With increasing technological development, analysing the data traces of specific people and tying predictions to individuals is likely to increase. In addition to the difficulty of applying general trends to particular

situations, areas or individuals, our analysis has illustrated that patterns follow different styles of identification. They vary according to axioms, data and focus objects—all of which express different underlying assumptions about crime. Yet, patterns tend to mask these assumptions. Their simplified and glossy surface hides underlying rationales and biases. It is easy to overlook the decisions, stories and assumptions that the clean visual surface of a pattern obscures. With patterns, assumptions about crime are concealed rather than rendered transparent to those who need to act on predictions. What careful designers of algorithms apprehend is that the ideas that inform patterns feed back into the police officers' learning processes—without the necessary reflection (Int. A). Such 'biases' within patterns are then indeed 'productive' (Hildebrandt 2016): what may look at first sight like police efficiency, may in fact be the result of patterned nudging of officers to police specific neighbourhoods and then—of course— also encounter the expected criminal activity in these areas. In turn, these offences become part of the updated data set that future predictions are based upon. Through this self-reinforcing logic, both the identified patterns are affirmed and police work is turned efficient, because they follow their own assumptions or biases (Int. A). The main challenge is then not to eliminate biases, as at times suggested (Johndrow and Lum 2017). 'Bias' cannot be removed, since the many conceptualizations about offenders and offense determine the pattern in the first place. Instead, the challenge is to render the concepts that determine pattern identification more transparent in order to let police officers reflect about the results they get to see. The suggestion to include stories (about how data are collected and interpreted) into software models is here a promising development.

Yet, databases and algorithms that produce predictions are notoriously hard to examine for non-professionals, because they are technically advanced and complex. They are, after all, the result of a collaboration of programmers, researchers, police officers and technologies. Even for software programmers it is at a certain stage no longer comprehensible how algorithms combine enormous amounts of data over time (Int. B). This further raises problems of accountability and transparency (Bennett Moses and Chan 2016: 817f). And if officers actually would like to trace the logics of pattern identification used in a prediction software, the police are not necessarily given insight into the commercial software models that they use, because they may be classified or proprietary (Int. Q; Int. O; Int. T). For several police departments, this was one reason to develop their own creation, as they refuse to work with such 'black boxes' (Int. S; Gluba 2016: 55).

Finally, besides the effects patterns have on understandings of actual offenses, *patterns are part of shaping a specific understanding of crime at large*. Patterns redefine the relationship between crime and the norm in a way that also informs policing cultures. The logics inherent in clusters, categories and cumulations emphasize the normality of crime. In other words, (criminal) behaviour must be a regularity, otherwise it is not graspable by patterns. One interviewee put it like this:

Most people when they think about criminals they think about the Hollywood portrayals of Hannibal Lecter. The criminal insane people. The vast, vast, vast majority of criminal people aren't like that. They are just regular people going about regular routines and crime just fits in here and there. 99.99999% of the time they're not doing anything criminal at all. They're just being human. (Int. F)

Another interviewee made a similar point in relation to patterns:

People inherently follow patterns. There are enough theories that explain this relationship. […] We have to follow patterns, otherwise we would not be able to deal with our everyday life. […] You only need to identify these patterns! Criminals, they are normal people like us – they are not from a different planet. That's often the idea- that they are totally different from us. I always say: we are all small criminals. It's only that our forms of crime do not enter the focus as much. (Int. J)

Even though both interviewees claim that crime—just as any other form of human behaviour—is normal, they do refer to normality still as something that stands out, that can be identified as particular and that can be moved into and out of focus. It is through the varying conceptualizations of normality that criminal behaviour can be identified and targeted. Thus, we put forward here that patterns do not recast criminal behaviour as *the* norm (as Routine Activity-Approaches would suggest), but as *a* norm amongst many others. Our analysis has demonstrated that the variations in styles of pattern identification bring out the many normativities and rationalities that can guide criminal behaviour as well as its control. Further, these normativities are reflected in the constant negotiation between a significant stability and the dynamics of new developments in patterns. This interplay between behaviour that stands out as distinct from other behaviour on the one hand, but follows a specific norm or rule on the other, may thus be captured as the different *normativities of crime* (cf. Kaufmann 2018). The many assumptions that inform pattern identification lead to a dispersion and multiplication of normativities of crime, which feed back into local policing cultures and the idea of societies that related policing activities engender.

Conclusions

Amoore and Raley (2017: 6) have argued that algorithms produce 'new forms of political authority', as they 'authorize what or whom is surfaced for the attention of a security analyst who, in turn, cannot meaningfully access this process of authorizing and surfacing'. Even though Amoore and Raley write about *non*-rule-based machine learning, our empirical data show that the same is also true for pattern-based crime predictions. Even more so, predictive policing brings rules back even into self-learning algorithms through the notion of the pattern. Patterns form the epistemic core of predictive analytics in general, and of policing software or algorithms more specifically. They give form to information hidden in data sets, which grants them considerable epistemological authority—not only in the context of policing. Moreover, patterns do act in their role as authorities, since they guide police action—whether in everyday practices of dispatching officers or in intelligence mapping activities.

What this article has put to the fore is the politics inherent in assigning form to information. We did this by tracing four styles pattern detection, which we organized from general to specific: on the one end of the spectrum we find correlative and spatial reasoning that is based on broad data sets and that targets potentially anyone in society. On the other end of the spectrum we find styles of pattern identification that are informed by complex theories and highly select data, and that target specific individuals. The intention of presenting and discussing this spectrum of pattern identification was to show that crime patterns are not the result of singular logics and simplistic rational choice or routine activity reasoning. Each style of pattern identification expresses a different argument about crime, depending on the theory involved in programming

the algorithm, the data that the algorithm evaluates and the overall objective or target of the algorithm. As such, any pattern is the result of a highly collaborative analytic effort. For a pattern to be identified, it needs the work of data collectors, data selectors, programmers, researchers, police staff, databases and algorithms, each of which play a part in assigning meaning to patterns. With that, crime is neither deviance nor normal. What this article has shown is that digital prediction analytics recast crime in light of different normativities, since every pattern follows specific narratives of how crimes are committed, where to find crime and where to send police patrols.

A general argument often cited in favour of predictive policing tools is that patterns may render problematic assumptions about crime and policing decisions more easily detectable than in the police officers' heads, which is why some consider algorithms a step forward in the debate on transparency. By pointing to the complex networks of decisions, programming efforts, ideas, theories and algorithmic workings that make each pattern, this article serves as a reminder that the pattern itself conceals the assumptions and the decisions that inform its identification. Unless patterns are accompanied and contextualized by explanatory material, they render policing decisions opaque. Not only for most police operators, but also for those affected by pattern-based policing it is barely achievable to reveal and interrogate the parameters that inform the suggested interventions. The clean surface of the pattern makes it impossible to defend oneself against their results. This article discloses only a minor part of the steps that need to be taken to render pattern-based policing more transparent and to invite the continuous reflection of its operators.

Despite their epistemic productivity, patterns themselves do not invite reflections about how they came into being, but they feed into requirements and ideals of efficient policing. They nurture the goal to reduce crime by being faster and smarter than offenders—rather than understanding motives and motivations. Patterns will continue to hold their position as authorities in digital predictive policing efforts. However, without further explanation and without an awareness about the stories each pattern tells about crime, they will feed back into policing cultures without the necessary reflection.

Funding

References

Amoore, L. and Raley, R. (2017), 'Securing with Algorithms: Knowledge, Decision, Sovereignty', *Security Dialogue*, 48: 3–10.

Anderson, C. (2008), 'The End of Theory: The Data Deluge Makes the Scientific Method Obsolete', *Wired*, 23 June.

Andrejevic, M. (2017), 'To Preempt a Thief', *International Journal of Communication*, 11: 879–96. https://www.wired.com/2008/06/pb-theory (accessed 19 November 2018).

—— (2018), 'Data Collection without Limits: Automated Policing and the Politics of Framelessness', in A. Završnik, ed., *Big Data, Crime and Social Control*, 93–107. Routledge.

Andrejevic, M. and Gates, K. (2014), 'Big Data Surveillance: Introduction', *Surveillance & Society*, 12: 185–96.

Ayres, I. (2007), *Super Crunchers: Why Thinking-by-Numbers Is the New Way to be Smart*. Bantam Books.

Babuta, A. (2017), *Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities*. Royal United Services Institute for Defence and Security Studies.

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*, 76: 20–29.

Bennett Moses, L. and Chan, J. (2018), 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability', *Policing and Society*, 28: 806–822.

Bowers, K. and Johnson, S. D. (2014), 'Crime Mapping as a Tool for Security and Crime Prevention', in M. Gill, ed., *The Handbook of Security*, 566–87. Palgrave Macmillan.

Boyd, D. and Crawford, K. (2012), 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon', *Information, Communication & Society*, 15: 662–79.

Brayne, S. (2017), 'Big Data Surveillance: The Case of Policing', *American Sociological Review*, 82: 977–1008.

Chainey, S. and Ratcliffe, J. (2005), *GIS and Crime Mapping*. John Wiley & Sons.

Chan, J. and Bennett Moses, L. (2017), 'Making Sense of Big Data for Security', *British Journal of Criminology*, 57: 299–319.

Dalton, C. and Thatcher, J. (2014), 'What Does a Critical Data Studies Look Like, and Why Do We Care?', available online at http://societyandspace.org/2014/05/12/what-does-a-critical-data-studies-look-like-and-why-do-we-care-craig-dalton-and-jim-thatcher/ (accessed 18 April 2018).

Ericson, R. V. and Shearing, C. (1986), 'The Scientification of Police Work', in G. Böhme and N. Stehr, eds, *The Knowledge Society: The Growing Impact of Scientific Knowledge on Social Relations*, 129–59. Reidel.

Ericson, R. V. and Haggerty, K. D. (1997), *Policing the Risk Society*. Clarendon Press.

Farrell, G. and Pease, K. (2014), 'Predictive Policing', in G. Bruinsma and D. Weisburd, eds, *Encyclopedia of Criminology and Criminal Justice*, 3862–71. Springer.

Ferguson, A. G. (2017), *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York University Press.

Fyfe, N. R., Gundhus, H. O. and Rønn, K. V. (2018), 'Introduction', in H. O. Gundhus, K. V. Rønn and N. R. Fyfe, eds, *Moral Issues in Intelligence-led Policing*, 1–22. Routledge.

Gill, P. (2000), *Rounding Up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence*. Ashgate.

Gluba, A. (2016), 'Mehr offene Fragen als Antworten: Was für eine Bewertung des Nutzens von Predictive Policing noch zu klären ist', *Die Polizei*, 107: 53–7.

Harcourt, B. E. (2007), *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. The University of Chicago Press.

Heidegger, M. (1997 [1957]), *Gesamtausgabe. I. Abteilung: Veröffentlichte Schriften 1910–1976. Band 10: Der Satz vom Grund*. Vittorio Klostermann.

Hildebrandt, M. (2016), 'New Animism in Policing: Re-animating the Rule of Law?', in B. Bradford, B. Jauregui, I. Loader and J. Steinberg, eds, *The SAGE Handbook of Global Policing*, 406–28. Sage.

JOHNDROW, J. E. and LUM, K. (2017), 'Al Algorithm for Removing Sensitive Information: Application to Race-Independent Recidivism Prediction', available online at https://arxiv.org/pdf/1703.04957.pdf (accessed 2 May 2018).

JOHNSON, S. D. (2008), 'Repeat Burglary Victimisation: A Tale of Two Theories', *Journal of Experimental Criminology*, 4: 215–40.

JOHNSON, S. D., BERNASCO, W., BOWERS, K. J., ELFFERS, H., RATCLIFFE, J., RENGERT, G. and TOWNSLEY, M. (2007), 'Space–Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization', *Journal of Quantitative Criminology*, 23: 201–19.

JOHNSON, S. D., SUMMERS, L. and PEASE, K. (2009), 'Offender as Forager? A Direct Test of the Boost Account of Victimization, *Journal of Quantitative Criminology*, 25: 181–200.

KAUFMANN, M. (2018), 'The Co-Construction of Crime Predictions: Dynamics Between Digital Data, Software and Human Beings', in H. O. Gundhus, K. V. Rønn and N. R. Fyfe, eds, *Moral Issues in Intelligence-led Policing*, 143–60. Routledge.

KAUFMANN, M. and JEANDESBOZ, J. (2017), 'Politics and "the Digital": From Singularity to Specificity', *European Journal of Social Theory*, 20: 309–28.

KENNEDY, L. W., CAPLAN, J. M. and PIZA, E. (2011), 'Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies', *Journal of Quantitative Criminology*, 27: 339–62.

KITCHIN, R. (2014a), 'Big Data, New Epistemologies and Paradigm Shifts', *Big Data & Society*, 1: 1–12.

—— (2014b), *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. Sage.

LATOUR, B. (2004), 'Why Has Critique Run Out of Steam? From Matters of Fact to Matters of Concern', *Critical Inquiry*, 30: 225–48.

MAGUIRE, M. and McVIE, S. (2017), 'Crime Data and Criminal Statistics: A Critical Reflection', in M. Maguire, R. Morgan and R. Reiner, eds, *The Oxford Handbook of Criminology*, 163–89. Oxford University Press.

MANNING, P. K. (1992), 'Information Technologies and the Police', *Crime and Justice*, 15: 349–98.

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

MANTELLO, P. (2016), 'The Machine That Ate Bad People: The Ontopolitics of the Precrime Assemblage', *Big Data & Society*, July–December: 1–11.

MARTIGNON, L. (2001), 'Algorithms', in N. J. Smelser and P. B. Baltes, eds, *International Encyclopedia of the Social & Behavioral Sciences*, 382–85. Elsevier.

McCUE, C. (2015), *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. Butterworth-Heinemann.

MIDDENDORF, R. and SCHWEER, T. (2016), *Musterbasierte Prognosetechnik in der Kriminalitätsbekämpfung: Vorstellung der aktuellen PRECOBS-Version und der Entwicklungsschwerpunkte für das Jahr 2016*. Presentation given at 1st PRECOBS-user meeting 2016 in Aarau (on file with authors).

PERRY, W. L., McINNIS, B., PRICE, C. C., SMITH, S. C. and HOLLYWOOD, J. S. (2013), *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation.

SANDERS, C. and CONDON, C. (2017), 'Crime Analysis and Cognitive Effects: The Practice of Policing Through Flows of Data', *Global Crime*, 18: 237–55.

Saunders, J., Hunt, P. and Hollywood, J. S. (2016), 'Predictions Put into Practice: A Quasi-experimental Evaluation of Chicago's Predictive Policing Pilot', *Journal of Experimental Criminology*, 12: 347–71.

Schinkel, W. (2011), 'Prepression: The Actuarial Archive and New Technologies of Security', *Theoretical Criminology*, 15: 365–80.

Schweer, T. (2018), 'Predictive Policing mit Precobs', in Institut für Versicherungswirtschaft der Universität St. Gallen, ed., *St. Galler Trendmonitor für Risiko- und Finanzmärkte. Produkt- und Serviceinformationen*, Vol. 40, 12–4. Universität St. Gallen.

Smith, G. J. D., Bennett Moses, L. and Chan, J. (2017), 'The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-Driven Approach', *British Journal of Criminology*, 57: 259–74.

Townsley, M., Homel, R. and Chaseling, J. (2003), 'Infectious Burglaries: A Test of the Near Repeat Hypothesis', *British Journal of Criminology*, 43: 615–33.

Waske, B. and Beneditksson, J. A. (2014), 'Pattern Recognition and Classification', in E. G. Bjoku, ed., *Encyclopedia of Remote Sensing*, 503–23. Springer.

Weisburd, D., Bernasco, W. and Bruinsma, G. (eds) (2009), *Putting Crime in its Place: Units of Analysis in Geographic Criminology*. Springer.

Wilson, D. (2018), 'Algorithmic Patrol: The Futures of Predictive Policing', in A. Završnik, ed., *Big Data, Crime and Social Control*, 108–27. Routledge.

Zedner, L. (2007), 'Pre-crime and Post-criminology?', *Theoretical Criminology*, 11: 261–81.

Ziewitz, M. (2016), 'Governing Algorithms: Myth, Mess, and Methods', *Science, Technology, & Human Values*, 41: 3–16.