Simon Egbert, Susanne Krasmann

# Predictive policing: not yet, but soon preemptive?



**Citation details**
Egbert, S., Krasmann, S. (2019). Predictive policing: not yet, but soon preemptive? Policing and Society, 30(8), 905–919. https://doi.org/10.1080/10439463.2019.1611821.

This is an Accepted Manuscript of an article published by Taylor Francis in Policing and society on 02 May 2019, available online: https://doi.org/10.1080/10439463.2019.1611821.

# Predictive Policing: not yet, but soon preemptive?

*Simon Egbert, Susanne Krasmann*

Abstract: For several years now, crime prediction software operating on the basis of data analysis and algorithmic pattern detection has been employed by police departments throughout the world. As these technologies aim at forestalling criminal events, they may aptly be understood as elements of preventive strategies. Do they also initiate a logic of preemptive policing, as several authors have suggested? Using the example of crime prediction software that is used in German-speaking countries, the article shows how current forms of predictive policing echo classical modes of risk calculation: usually employed in connection with domestic burglary, they help police to identify potential high-risk areas by extrapolating past crime patterns into the future. However, preemptive elements also emerge, to the extent that the software fosters 'possibilistic' thinking in police operations. Moreover, current advances in crime prediction technologies give us a quite different picture of a probable future of preemptive policing. Following a general trend of data-driven government that draws on self-learning algorithms and heterogeneous data sources, crime prediction software will likely be integrated into assemblages of predictive technologies where criminal events are indeed foreclosed before they can unfold and emerge, implying preemptive police action.

Keywords: predictive policing, prevention, preemption, algorithms, datafication

## From Precogs to PRECOBS

It is no coincidence that 'PRECOBS', the currently leading software product for predictive policing in German-speaking countries, reminds us of the three key figures in Steven

Spielberg's film 'Minority Report'.[1] Here, the 'precogs' (from "precognitives") in the police department of Washington D.C. in 2054 serve as the medium to forestall future crime. And indeed, PRECOBS, which officially translates into 'Pre Crime Observation System', was originally called 'PRECOGS' (Balogh 2016, p. 336). Like similar software programmes that have gradually been implemented in police departments throughout the world, PRECOBS is tied to the promise that a substantial revolution of police work lies ahead – with predictive policing, the future of policing has already begun (see Uchida 2009, p. 1, Police Executive Research Forum 2014: 2).[2] However, the critical literature sees an expansion of a 'preemptive logic', of which technologies of predictive policing will be a crucial part. As van Brakel (2016, p. 118) states, a 'pre-emptive logic […] can be recognized in many new surveillance practices, such as predictive policing, especially in the United States'. And Mantello (2016, p. 2) contends that 'the pervasive growth in predictive analytics for law enforcement signals a paradigm shift in criminal justice [… which] follows along the same axis that the state embraces in its logic of preemptive war and targeted assassination.' Similarly, Andrejevic (2017, p. 879) defines predictive policing 'as the use of data-mining tools to predict and preempt criminal activity'.

Yet, while Minority Report's fiction is that the 'precogs' actually can foresee the future, PRECOBS, to date, operates more like common risk technologies, thus rendering the 'preemption' label inaccurate. With predictive policing, actionable prognostic information is gathered by drawing on (police) data of past crime events that are correlated with present crime scene information and translated into models of algorithmic decision making (see Perry et al. 2013, p. 8, Aradau and Blanke 2017, p. 383). PRECOBS is part of the family of predictive

[1] Based on Philip K. Dick's short story 'The Minority Report' from 1956 (Dick 2000).

[2] In the US, crime prediction software is used in most police departments (see Hess et al. 2013, p. 204, Police Executive Research Forum 2014, p. 2-7). Although it is less common in Europe, the software is being implemented in major cities like Amsterdam (Willems and Doeleman 2014), Milan (see Costanzo et al. 2015, p. 246), Berlin (I16 [see footnote 3]), Munich (Okon 2015) and Zurich (Balogh 2016). As examples from the Global South are rare (e.g. Sao Paulo, Altenhain 2017), predictive policing can currently be understood as a Western phenomenon.

policing technologies that employ algorithmic data processing to identify 'patterns of *probable* future offending and victimization', so as to prevent these materializing (Wilson 2018a, p. 108). Moreover, predictive policing is often confined to helping police officers to identify high-risk crime areas, combined with conventional policing practices such as preventive and intensified patrolling and attendant stop and frisk measures (see Uchida 2014, p. 3876f.), which again calls into question the label of preemptive policing.

Nonetheless, the hype around predictive policing – at least in German-speaking countries, where datafied forms of police work are not that common yet – has created a knock-on effect encouraging police forces to test and implement crime prediction software. Authorities have learned to appreciate the usefulness of (big) data analysis and the currently rather simple and cheap modes of implementing and applying it. But what has the ensuing process of datafication in policing to do with the question of predictive policing as being preemptive or not? First of all, predictive policing indeed follows a trend of predictive knowledge increasingly being employed to guide targeted police actions. The aim is to spot the suspect before any offense might be committed (see Wilson 2018a, p. 109): the intrinsic project of predictive policing thus is preemption. Moreover, while most of the programmes to date are limited in scope (PRECOBS, for example, merely focuses on burglary) and reach (designating areas with different levels of probability that a crime is likely to happen), the technology has a substantial potential to be woven into related predictive models and thus to be employed for a variety of different purposes. It may be upgraded in a way that will give rise to a comprehensive process of datafication of policing. Following a general trend of data-driven government that draws on heterogeneous data sources, predictive policing, we argue, may constitute one element of technological or surveillant assemblages (Haggerty and Ericson 2000). As an integrated module of targeted government, predictive policing thus might well become preemptive: it will enable police forces to foreclose criminal events before they emerge.

Taking PRECOBS as exemplary, in the following we explore the preemptive potential of predictive policing technology in more detail by drawing on empirical data from a larger research project on the implementation and application of crime prediction software in Germany and Switzerland. We conducted 35 interviews with representatives of different police departments: crime analysis units, information technology departments, police headquarters, and beat officers. From the ten police authorities of different regions, five are currently using PRECOBS. Furthermore, we 'shadowed' PRECOBS operators in four police authorities, of which one was already piloting PRECOBS Enterprise, the new version of PRECOBS. We also attended a seminar given by the developers of PRECOBS Enterprise, in which the new features and strategic aims of PRECOBS Enterprise were presented to police representatives. Finally, documents dealing with the properties and rationales of the development of the software from PRECOBS to PRECOBS Enterprise – presentation slides as well as manuals of the software – helped us reconstruct the analytical progress associated with and the epistemic transformation resulting from the development of the new software.[3]

After a brief overview on the software's implementation and application, we take a closer look at what exactly predictive policing enables the police to see and to do. We seek to identify elements of 'near preemptive' policing that are already present in current forms of crime prediction software application. Drawing on the critical literature on preemptive logics of security, we will then assess the future prospects of predictive policing. What becomes apparent is that crime prediction software is currently in a quite dynamic process of development. With

[3] All interviews have been recorded and transcribed, and all collected data been fully anonymized. Quotation follows according to our source code: character 'L' stands for a (field or interview) log, 'I' for interview transcript and 'D' for document. The digits following the codes indicate the cited line numbers. We analysed our data by using coding approaches from grounded theory methodology (Strauss and Corbin 1990) and by processing corresponding data analysis software (MAXQDA). Quotes have been translated into English by the authors.[4] By using the SPSS data mining workbench 'Clementine', the crime analysis unit of the Richmond Police Department utilized predictive analytics for different law enforcement tasks in order to enhance the effectiveness and efficiency of police work, e.g. for smarter deployment decision concerning beat officers, risk-based deployment of tactical units, as well as risk and threat assessment (McCue and Parker 2003). In order to do this, they analysed police crime data as well as operational data such as the distribution of calls for services. (McCue 2012: 139f.).

the data basis increasingly being extended and algorithms becoming more sophisticated in their self-learning procedures, the future of predictive policing may indeed be one of preemptive intervention.

## Predictive Policing: current theory and practice

Digital forecasting instruments are on their way to becoming an integral part of day-to-day policing practices throughout the world. The rise of big data and the fabrication of mathematical algorithms have made predictive policing possible, and these factors might constitute a qualitative difference to previous forms of forecasting and prevention in policing (see Perry et al. 2013, p. 3f.; Hardyns and Rummens 2018, p. 201f.). The first initiatives to implement future-sensitive police work using the techniques of data mining and predictive analytics, though without explicitly referring to 'predictive policing', were identified as early as 2003 (McCue and Parker 2003).[4] Nonetheless, 2011 marks the initial starting point when the Police Departments of Santa Cruz and Los Angeles began to employ the software 'PredPol', a joint product of the Police Department and the University of California in Los Angeles; this remains one of the leading software tools for predictive policing in the US context (Beck n. d.; Mohler et al. 2015). PredPol uses earthquake algorithms to predict future crimes, which are understood as 'aftershocks' (Mohler et al. 2011, p. 100). Since then, predictive policing has signified digital technologies that are designated to locate and prevent future crimes by generating 'operative' crime predictions, meaning that they are directly translatable into police measures (Gluba 2014, p. 347). Apart from reducing crime rates and related harm, predictive policing from the outset was also implemented 'to do more with less' (Beck and McCue 2009). It is designed to allocate

[4] By using the SPSS data mining workbench 'Clementine', the crime analysis unit of the Richmond Police Department utilized predictive analytics for different law enforcement tasks in order to enhance the effectiveness and efficiency of police work, e.g. for smarter deployment decision concerning beat officers, risk-based deployment of tactical units, as well as risk and threat assessment (McCue and Parker 2003). In order to do this, they analysed police crime data as well as operational data such as the distribution of calls for services. (McCue 2012: 139f.).

police forces more effectively in times of limited financial resources, complex policing tasks and an insistent political demand for non-discriminatory police work (see Bratton et al. 2009, p. 1; Ferguson 2017, p. 20-33).

Predictive policing that aims at spotting the local and temporal parameters of future crime fundamentally relies on theories from environmental criminology (Wortley and Townsley 2017). The observation that crime is not distributed homogenously in space but clusters in specific areas is crucial, which is why approaches such as situational crime prevention (Clarke 1980) or designing out crime (Clarke and Mayhew 1980) became pertinent. Nevertheless, the prediction-generating part of predictive policing varies in its analytical complexity, depending on the kind of data gathered and the particular theoretical concepts applied when programming related algorithms.[5] This also means that not all prediction software can be aptly referred to as big data or data-mining technology, as often – for example in the case of PRECOBS – only police crime data are analyzed on the basis of explicitly theory-driven approaches, which tend to just extrapolate past patterns of offenses into the future (Perry et al. 2013, p. 17).

What may sound obvious, namely that predictive policing itself relies on the idea that crime is predictable and that societal phenomena are, in one way or another, statistically and algorithmically calculable, is nonetheless noteworthy. Programming of the relevant algorithms is based on the empirical observation that certain types of crime follow particular patterns (Kaufmann et al. 2018) – an observation that is often undergirded by the simple (criminological) theory that human behavior is largely guided by rational choices and is thus predictable (Becker 1968, Cornish and Clarke 1986). As Brantingham, one of the key developers of the software PredPol and son of well-known environmental criminologists Brantingham and Brantingham (Ferguson 2017, p. 65), states:

[5] For an overview of different analytical approaches and their complexity, see Perry et al. (2013, p. 17-55).

> The naysayers want you to believe that humans are too complex and too random — that this sort of math can't be done (…). But humans are not nearly as random as we think (…). In a sense, crime is just a physical process, and if you can explain how offenders move and how they mix with their victims, you can understand an incredible amount. (Quoted in Rubin 2010)

One of the most common approaches to predicting future localities of crime is the "near repeat" model that feeds, among others, PredPol as well as PRECOBS. The basic idea is that the same type of offense is likely to be committed in the near future and in the close vicinity. This 'near repeat hypothesis' (Townsley et al. 2003) has been elaborated and empirically tested, especially in the case of domestic burglary (Johnson et al. 2007; Farrell and Pease 2014, p. 3863). In line with rational choice theory, the assumption is that a successful offender – figured as the 'optimal forager' (Sidebottom and Wortley 2016, p. 168) – will commit a crime soon again in the neighbourhood of the first offense, as he or she is now familiar with the local particularities and thus able to better calculate the risk of getting caught and the likely gains from the potential theft. A further and related theoretical reference is the 'routine activity approach', suggesting that committing an offense depends on the presence of a motivated perpetrator, the availability of a suitable target and the simultaneous absence of sufficient safeguards. Crime, in other words, is a question of opportunities (e.g., Cohen and Felson 1979) and situational crime prevention is the appropriate approach to policing. From this perspective, crime risk is withdrawn from the environment by technical solutions, architectural arrangements or, as in the case of predictive policing, higher police presence so that the prospective offender, when facing these measures, will abandon his original motivation and opportunities will be reduced (see Bennett Moses and Chan 2018, p. 814f.).

**PRECOBS: a socio-technical prediction assemblage**

PRECOBS, which was developed by the private company 'Institut für musterbasierte Prognosetechnik' (Institute of Pattern-Based Prediction Technology) (Schweer 2015), is being utilized by the police departments in Munich and Middle Franconia as well as in Zurich (municipal police) and two cantons of Switzerland (Basel Country and Aarau). Additionally, it is being tested in Baden-Wurttemberg (Germany) and by the cantonal police of Zug and Zurich. Currently, the software is limited to addressing residence burglaries, though an expansion towards everyday street crimes such as auto theft, robberies, and pickpocketing as well as sex offenses is already envisaged (L28, l. 36-40, L49, l. 490-493).

The implementation procedure at a particular police department runs as follows: the software is fed with past policing data concerning the offense in question in order to start the simulation process for configuring the prediction software (see Schweer 2015, p. 15, Balogh 2016, p. 336). This first and foremost entails the identification of areas that are prone to near repeat series, and thus defined as 'near repeat areas' or 'near repeat affine areas'. This means that near repeats have occurred there in the past in a statistically significant manner. Only these designated areas will be involved in the prediction process (Schweer and Schweer 2015, p. 24). In addition, the burglary pattern characteristics for summer and winter are elaborated. This is especially important in the domain of domestic burglaries, as many breakings are carried out after sunset while the household members are still out – for example, at work – which is easily recognizable from outside ('twilight burglary'). A simulation process then is to test the validity of the predictive configuration. In Zurich, for example, burglary incident data from three past years were used to predict burglaries for a fourth – also past – year, in order to compare the simulated predictions with the real, actually registered burglaries for this period (see Balogh 2016, p. 336).

The near repeat theory only applies to professional burglars that are expected to operate on a serial basis and to proceed in a systematic, rational manner: they are assumed to act calculatingly, which makes it possible to identify a pattern-based, non-contingent mode of operation. With PRECOBS, a near repeat is defined as a follow-up burglary at a maximum distance of 400 meters and within a period of up to seven days after the first incident (see Balogh 2016, p. 336). To assess whether a reported incident is a professional burglary, which might be repeated in the near future and in the close vicinity, PRECOBS operates with 'trigger' and 'anti-trigger criteria' (Schweer 2015, p. 14). A 'true' indicator for professional burglary is, for example, noiseless and swift intrusion through a window entered by using suitable tools (instead of just throwing a stone). Also, the type of haul is an important indicator for characterizing how professional the burglar is. If only cash and/or jewellery is stolen, it is likely that a professional burglar was at work, whereas theft of less easily transportable and/or less or non-valuable goods points to non-professional offenders (I2: 262-271; I7: 1123-1127). Therefore, the prediction software registers and analyses the time of the offense, the type of building where the burglary took place (e.g., single-family house or block of flats), the modus operandi (e.g., entry through the window by drilling or using a jemmy), and the stolen objects (money, jewellery etc.) (see also the listing at the bottom of figure 1).

The PRECOBS operators start their day by feeding the new data of recent domestic burglaries (from the last 24 hours) from the case processing system into PRECOBS. Corrected information of older cases is also integrated. The software then analyses the newly integrated data using existing anti-trigger criteria, thus assessing whether a professionally executed burglary has occurred in one of the near-repeat areas of the city. If this analysis indicates a trigger offence, a prediction is generated and eventually an alarm released to alert the PRECOBS operator (I3, l. 587-590, I19, l. 40-45, L8, l. 1-25). He/she is then required to assess whether the prediction

is reasonable and, if so, to forward the alarm notification to the local police station (see Okon 2015, p. 23, Schweer 2018, p. 14).

The decision on the tactic to be employed in the case of an imminent (follow-up) burglary depends on variables such as the range and the locality of the risk areas that the map indicates, and on the availability of officers at the police station concerned. Although the concept of 'near repeat' requires an instant reaction, acceleration of the intervention procedure is required as the probability of a repeated action decreases drastically after 24 hours (Suckow 2018, p. 354) – to instantly send plain-clothed observation forces into the designated risk area in order to spot a suspect offender or to catch the burglar in the act is surprisingly rare. As police officers told us, this is due to limited resources (e.g., I44, l. 1176). Given that it prevents crime from happening in the first place, predictive policing that amounts to preemptive action, ultimately, may be considered efficient. But in the current state of the art there seems to be some hesitation, due to the fact that cost-intensive targeted intervention requires concerted manpower (I7, l. 1172, I11, l. 1309-1311). Decisions on how to process the 'operational circle' (see figure 2) have therefore, up until now, mostly resulted in intensified preventive patrolling (see Balogh 2016, p. 337). Disposable beat officers are sent to the designated risk areas to show presence, either in a special mission or as part of another operation; this means that, after completing another task, they drive through the risk area on their way back to the department (I9, l. 5-15, I20, l. 110-113).

Not only but especially with PRECOBS, predictive policing is never a fully automated process. Rather, it is per se a multidimensional, iterative and socio-technical practice where human operators are always interposed and different epistemologies are at work (Perry et al. 2013, p. 11-15, Kaufmann 2018). Successful implementation, therefore, is not merely a question of technological superiority but depends first and foremost on how police departments, as complex organizations (Chan 2001), are willing and able to change their practices in accordance with the requirements of the prediction software. Appropriate data quality can only be achieved if

the police officers in charge are sensitive to attentive data input (Bennett Moses and Chan 2018, p. 809-10; Kaufmann 2018, p. 148-152). And indeed, operators are needed in several intermediate steps, first of all to feed the crime data from the case processing system into PRECOBS, as the latter has no direct interface with the first. This is for pragmatic as well as security reasons. PRECOBS is usually installed on a separate computer that is isolated from the police intranet, as integration into the police network would involve massive administrative efforts, especially concerning IT security (L8, l. 3-5, L18, l. 5-10). Furthermore, once corroborating information about potential offenders and/or specific incidents in a designated risk area is at hand, this information needs to be added to the programme which leads to the map automatically being generated anew. This new information is then sent by e-mail to the local police department (I3, l. 1-25, L8, l. 2-7, I19, l. 18-29). Conversely, the prediction process cannot work correctly if essential information is missing. For example, if the burglar has already been caught, the trigger/anti-trigger-filter comes to nothing – and it is the operators' task to detect this and to disable the prediction alarm (I2, l. 214-216).

The involvement of human decision making and assessment is a crucial issue in the German context of the software application and its adoption process. Software engineers as well as chief police officers consider it a question of acceptability within the police as well as of public trust in predictive policing.[6] Notably, beat officers do not wish to be sent to designated risk areas by a machine and crime analysts do not want to see their skills and competencies devalued (I2, l. 87-89, 801-805, I11, l. 1018-1020, see also Wilson 2018a, p. 118). Obviously, the authority of experience (Rouvroy 2012) still prevails.[7] As police officers admit, this also means that evaluation of the reasonability of the automated alerts is more often than not conducted quite

[6] See, for example, Okon (2015, p. 23), Schweer (2016, p. 27), Balogh (2016, p. 337).

[7] This is also true for the assessment of PRECOBS by its proponents, as the leading developer of PRECOBS, Thomas Schweer, is a social scientist who conducted fieldwork on policing practices. He therefore has experience with police work – he knows how the police work – which is important for how the potential of PRECOBS is perceived by police authorities in the first place.

unsystematically, relying on gut feeling and selectively employed practical knowledge (e.g., I19, l. 1068). This attitude might also be read as a form of resistance to everyday work constantly being guided by crime alerts that are just "thrown" out into the world by machines (Rouvroy 2012) (I2, l. 87).

So, what does PRECOBS as an exemplary model of current forms of predictive policing have to do with preemptive policing? Before answering this question, we should take a closer look at how preemption as a rationale of governing security intermingles with algorithmic styles of reasoning.

**Algorithms and the rationality of preemption**

Preemptive intervention has become prominent as a method for combating terrorism in the 21st century (Daase and Kessler 2007). It is considered a suitable response to increasingly incalculable as well as catastrophic threats (see Amoore and de Goede 2008, p. 11). These might be improbable but have the potential to cause intolerable harm, and therefore must be prevented before they have 'a chance to even emerge' (Krasmann 2012, p. 671, see also Anderson 2010, p. 790). Common risk technologies, on the other hand, access the unknown future through 'prospective retro-diction' (Aradau and Blanke 2017, p. 378): they draw on past experiences to calculate future probabilities. In this case, prediction is of relative, statistically controllable certainty. Preemptive action, by contrast, fosters 'possibilistic' thinking (Amoore 2013, p. 12): since the past can no longer be seen as a prologue to future events, speculation about unforeseeable harmful events is required. Here, prediction amounts to 'conjecture' (Aradau and van Munster 2011).

Algorithms make their own contribution to such a preemptive logic. They are preemptive not so much in a negative sense, in that they prevent things from happening, but rather positively, in that they suggest what is to come. Algorithms create reality, they are productive. As Richard

Berk (2012) puts it: “The computer algorithms we do [to forecast criminal activities] invent predictors.” But algorithms are not only productive, they are also reductive. They ‘reduce the relative indeterminacy of the future’ to a computational sequence (Reigeluth 2014, p. 245). And, while doing so, they follow their own style of reasoning. Algorithms do not think in terms of verbal language and hermeneutics, nor do they make up causalities. When mining and parsing data and when automatically selecting incomputable data and seemingly random information, algorithms – pursuing an ‘ontology of association’ (Amoore 2011, p. 27) – operate on the basis of resemblance and analogy (see Aradau 2015, p. 26, Kitchin 2017, p. 17). They deploy their own logic of calculation and build up their own correlates (Aradau 2015, Amoore and Raley 2017). Think of the example of the software applied by the supermarket chain Wal-Mart, which was designed to analyse the consumer choices of its customers in relation to many variables such as time, weather, and location, by using data mining techniques and the self-gathered data from its stores. Among the findings was that in cases of imminent hurricanes the sales figures for strawberry flavour pop-tarts increased significantly (Hays 2004). Even without a reasonable explanation, which would be necessary to determine causation, this information enabled the company to make decisions about stocks as an adequate reaction to changing weather conditions. Similarly, statistician and criminologist Berk states, referring to forecasting criminal behaviour: ‘For example, if other things equal, shoe size is a useful predictor of recidivism, then it can be included as a predictor. Why shoe size matters is immaterial.’ (Berk and Bleich 2013, p. 517) The key rationale of this data-driven (or numbers-driven) approach is that a purely mathematical-algorithmic analysis of huge amounts of data suffices to gain robust, though inscrutable knowledge about the future. As we will see, this correlation-focused style of prospective reasoning has also been introduced in the realm of predictive policing (Beck and McCue 2009).

Although drawing on data that originate from the world outside the digital, self-learning algorithms do not re-present reality and, unlike classical risk calculation, they do not predict the future by projecting past events. Rather, they connect the dots and thus trigger a preemptive logic. When creating person-based or spatiotemporal profiles, for example, such data tell us what *could* be the case tomorrow, of course, with a high probability. And it is up to the users of the respective software application to decide whether to follow such suggestions.

**Predictive policing: nearly preemptive?**

Of course, the increasing implementation of predictive policing software at police departments in Western countries is not a response to the perception of incalculable or ungovernable urban threats. Yet, as we argue, dealing with everyday crimes such as burglary also serves as a test case to further develop the technology. This is not to imply that particular future developments and changing modes of government have already been anticipated. Rather, technological advances are driven by positive expectations, by 'sociotechnical imaginaries' (Jasanoff 2015, p. 19) and a general belief in the potential of the technology and the options the market provides. Hence, to sound out the future potential of predictive policing, one might ask: 'What Can We Learn from Wal-Mart and Amazon'? (Beck and McCue 2009) And as we will see, although they basically follow the rationale of common risk calculation – that is, drawing on past events to gain future-related knowledge – there are indeed preemptive elements in current versions of predictive policing.


Figure 1: PRECOBS-operator screenshot-view from Munich (source: http://www.sueddeutsche.de/digital/polizei-software-zur-vorhersage-von-verbrechen-gesucht-einbrecher-der-zukunft-1.2115086)

As the color-coded PRECOBS map indicates (see figure 1), the red-coloured squares represent a high near-repeat probability while the yellow and green squares designate a middle and low probability of a follow-up burglary (D1, p. 7). These squares result from the statistical method of kernel density estimation that assesses the probability of a future burglary on the basis of police data on past burglaries in a given area (Schweer 2015, p. 16). It could thus appear efficient to focus on near-repeat hot spots, the areas of the highest probability of a near repeat, so as to be in the right place at the right time 'to stop an imminent act before it takes place.' (Andrejevic 2017, p. 883, 2018, p. 102, see also Mantello 2016, p. 4) If this is a tactic that follows a trigger alarm, following Andrejevic (2017, p. 882), we can speak of a strategy of 'near term preemption'. However, if police officers suspect a person who is present in, or close to, the designated risk area to be a burglar, this does not mean that this information was provided by algorithms. Rather, it is the *possibilistic* thinking of the police officers themselves that establishes an *imaginative* connection between the prediction map and the risk potential of a

single person who happens to be in the vicinity – an ecological fallacy with a preemptive outcome, so to speak.[8]

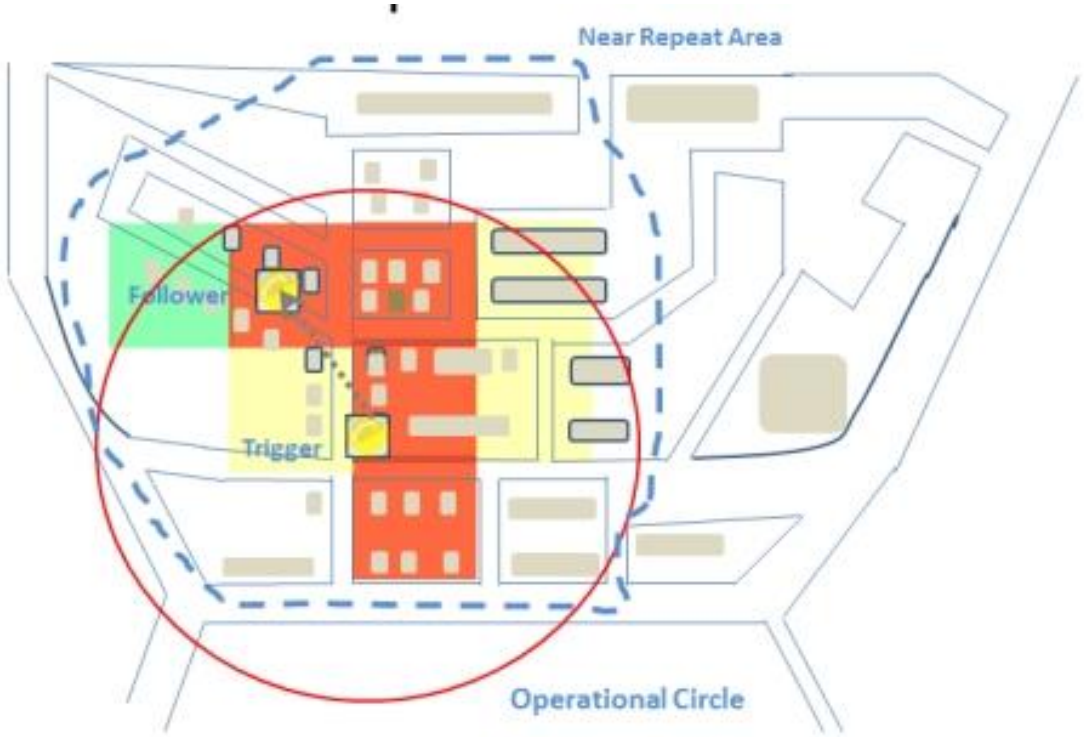


Figure 2: Artwork of PRECOBS map with initial and near-repeat offense, near repeat area and operational circle (source: ifmpt.de)

Currently, most of the crime prediction systems being implemented are, compared to the sociotechnical imaginaries prevailing, quite rudimentary. They do not tap the full potential of predictive policing, and this is especially true for PRECOBS in two respects. For one thing, only police crime data are analysed while other available data sources concerning, for example, the socio-economic or infrastructural conditions of certain areas are not taken into account. Furthermore, PRECOBS is strictly theory-driven in order to identify near-repeat patterns and to detect professional serial offenders, using the dominant strategy of preventive patrolling. The

[8] Interestingly, in Baden-Wurttemberg information about the classification of different risk areas was not passed on to the street forces, as police authorities expected the beat officers to orient their action too much toward the red-coloured squares (see Gerstner 2017, p. 21).

software does not operate autonomously and create future-related knowledge in an inventive manner.

But this is the near future that lies ahead: predictive policing may be applied to a variety of social problems and dangers, from governing the urban poor up to targeting individuals as suspects of terrorist or related violent acts; and alternatively, the technology may be integrated into comprehensive predictive assemblages that, as assemblages, might in effect operate preemptively. It is the technology of algorithms and their logics of association and connectivity itself that allows for predictive policing to be woven into and form part of technological assemblages. Four corresponding trends are worth mentioning here: the use of larger and more heterogeneous data samples; more sophisticated and in particular (non-)supervised learning algorithms; increased use of predictive profiling approaches, that is to say of person-based predictive policing; and, last but not least, a tendency of increasing cross-linkage of different police databases that would make police work increasingly governed by (big) data analysis assemblages. Taken together, we argue, these developments will lead to new forms of predictive policing that will include crucial elements of preemptive action.

Just recently, PRECOBS has developed a new version called PRECOBS Enterprise, which is currently being piloted in several police departments. Once practical and technical problems – among others, concerning the interfaces and their (in)compatibilities – have been solved, the new software will replace the original one in day-to-day business. PRECOBS Enterprise allows for generating predictions at any time – not just, as in the old version, once per day. Predictions may thus be adapted in accordance with the shift structure of the participating police units, a feature that PredPol and Crime Anticipation Software (CAS) already provide for (Hardyns and Rummens 2018, p. 208, 210). Furthermore, in contrast to its predecessor, now known as ‘PRECOBS classic’, PRECOBS Enterprise is designed as a dashboard version that facilitates decentralized use and thus extension of potential users. As a web-based software, it makes local

installations on computers dispensable and, most importantly, creates a technical environment that allows for an easy integration of new data and analytical parameters (Okon 2018, Middendorf and Schweer 2018). Ultimately, it enables PRECOBS operators to be 'Pre-Crime-Analysts' and, in particular, to cover 'up-to-the-minute prediction processes' (Schweer 2018, p. 14). And indeed, one explicit aim of PRECOBS Enterprise is to extend the theoretical basis so as to move away from simply testing near-repeat hypotheses towards the more data-driven approach of risk terrain modelling (L5, l. 33-39, Okon 2018, p. 10). Hence, although it does not operate a-theoretically, and instead of big data still processes small data, that is to say selected crime data, PRECOBS Enterprise shows a preemptive *potential*: being designed as an integrated, modularly constituted platform, it is easily adjustable and expandable and thus fit for data integration (I51, l. 493-512). As one police representative and leading proponent of PRECOBS Enterprise states: 'There is enough information available. But still, we have to connect these sources better with one another.' (I51, l. 231f.) Data-driven assemblages that operate on the basis of information retrieval from data banks and a-theoretical data mining-techniques dispense with linear causalities. By following a logic of 'connecting the dots', they seek to figure out 'hidden patterns and relationships' (McCue and Parker 2003). PRECOBS Enterprise, in other words, is prepared for a shift in focus from 'model is king' to 'data is king' (Aradau and Blanke 2017, p. 379), and thus, ultimately, for preemptive policing practices.

PRECOBS Enterprise is by no means the only software that indicates a preemptive turn in policing. Sophisticated analytical approaches of data mining will increasingly enable the police to individualize crime prediction and to target likely offenders as well as victims. The pilot run of predicting gang crime in London, for example, is based on 'predictive analytics' that create risk scores for the likelihood of persons being linked to gang-related offenses (Accenture 2015, p. 1). The most prominent example in this respect is the 'Strategic Subject List' of the Police Department of Chicago, often referred to as the 'heat list'. By consulting an algorithmically

generated risk score, it targets individuals who are expected to be at high risk of becoming a perpetrator or victim of gun violence (Saunders et al. 2016, Ferguson 2017, p. 37-40). Drawing on Papachristos' (Papachristos 2009, Papachristos et al. 2012) network approach, it analyses the interpersonal connections in incidents of gang violence. As Wernick, mastermind of the 'heat list' from Illinois Institute of Technology, states, it builds on algorithms that are programmed for 'link analysis': 'It's not just shooting somebody, or being shot. It has to do with the person's relationships to other violent people.' (quoted in Biselli 2014) Similarly in Germany, a system called RADAR-iTE (rule-based analysis of potentially destructive offenders for the assessment of the acute risk – Islamist terrorism)[9] has been developed by the Federal Criminal Police Office (Bundeskriminalamt, BKA) in cooperation with psychologists from the University of Konstanz to determine the risk of an attack by 'endangerers' ('Gefährder'). This police term, coined in the context of combating 'politically motivated crime', designates a particular type of persons as *possible* threats to society on the basis of indicators of suspicion that are not necessarily crime-related (BKA 2017; Deutscher Bundestag 2018). Provable (or probable) indicators of being prone to violence are dispensable (Krasmann 2018). Moreover, taking the same line as the Strategic Subject List in Chicago, PRECOBS Enterprise too is now intended to have a feature called 'Pre Crime Monitoring', which includes an 'early-warning system' for places and persons at risk (Middendorf and Schweer 2018, p. 13), for example concerning victims of stalking (L49, l. 159-162). This envisaged extension of PRECOBS Enterprise requires programmers to code more sophisticated risk calculation algorithms and to open them up to more heterogeneous data sources, thus exceeding the limited predictive tools of near-repeat modelling (I2, l. 1929-1941, I51, l. 4-7). This would mean taking a crucial step toward multi- or even a-theoretical data analysis.

[9] The German original: ‚*R*egelbasierte *A*nalyse potentiell *d*estruktiver Täter zur Einschätzung des *a*kuten *R*isikos - *i*slamistischer *Te*rrorismus'.

PRECOBS Enterprise furthermore aims at decentralizing predictive and data analysis operations within police departments, which would imply that all members are able to access the web-based software by using the intranet and which would enable them to search information and/or analyse data more independently (D2, p. 2). This is not only deemed to provide for a better acceptance of predictive systems within the police (Okon 2018, p. 10), but also to substantially extend the use of data analysis within police departments. The dashboard-desktop, in particular, is seen as something that will facilitate 'playing around' with the analytical functions of PRECOBS Enterprise, as it adds a further layer of preemption-like knowledge production: ad hoc analysis is informed not merely by theoretical assumptions, but also by individual experience-based knowledge, intuition and situational parameters, such as providing a time-space for experimental operations and explorative guesswork. Going beyond the previous forms of predictive processing, PRECOBS Enterprise now also covers operations such as 'main offence hours' and 'journey to crime' (L49, l. 502-505), including the peak time of particular offenses (D2, p. 5, L49, l. 577f.) as well as identification of anchor points in the life of offenders, like residence or place of employment, by analysing their routes to and from the crime scene (L49, l. 547-549, Van Daele and Vander Beken 2011). Two functional enhancements compared to the previous PRECOBS version are notable here: PRECOBS Enterprise no longer merely applies to domestic burglary but covers a much broader range of offences, such as sexual assaults (I51, l. 17), and it is no longer restricted to the tactic of predicting, intensified patrolling and deterrence but is also supposed to support police in crime investigations and identifying offenders. Moreover, the new PRECOBS version allows for a further cross-linkage of different police and non-police databases and data pools, fostering what is known as 'platform policing' (Wilson 2018b), which shares essential similarities with cloud computing programs' data linkage (Amoore 2018, p. 5f.). The German federal state of Hesse constitutes a further example of this trend towards a (big) data policing assemblage, or

‘assemblage-ism’, where on the basis of modular and highly integrative platform software information systems and databases are mutually connected and rendered searchable. In Hesse, the in-house programming of the crime prediction software ‘KLB-operativ’ has been combined with developing the ‘investigator app’ (‘Ermittlerapp’) which supports investigations by an advanced sharing of data (I48). The paradigm here is the Palantir software used by the Los Angeles Police Department (LAPD), where numerous data sets on, for example, gangs or from Automatic License Plate Readers are interconnected to generate (not only) predictive knowledge (Brayne 2017, p. 993f.). Unsurprisingly, Palantir’s ‘Gotham’ software was introduced quite recently in Hesse too, and is now being utilized to detect possible terrorists using ‘hessenDATA’ software (Police-IT 2018).

Other sophisticated variants of predictive policing software, such as HunchLab (Azavea 2015), which constantly learns through feedback data fed in by police officers and which strongly intervenes in everyday policing activities with instructions on how to patrol, and holistic prediction approaches such as Risk Terrain Modeling (Caplan and Kennedy 2016) can also be considered soon-to-be preemptive instruments: operating on the basis of self-learning algorithms and heterogeneous ‘data assemblages’ (Jasanoff 2017), they no longer rely (only) on strict theoretical assumptions but are assigned to find new, so far unknown risk correlations from the available data (e.g. between crime incidents and features such as infrastructure or the number of bars and clubs in a certain area) that can be translated into interventive strategies of policing. If these techniques also draw on past data, this is only to identify *new* risk patterns. This is an example of what Amoore and Raley (see 2017, p. 6) suggest with regard to non-rules-based algorithms and non-relational databases (NoSQL databases): ‘the imagination of a horizon of security in which the detection of new events can reject traditional statistical risk criteria and embrace emergent futures.’

Overall, the developments mentioned foster a thorough process of datafication and platformization of police work. In the context of policing, this would not merely mean that more and more aspects of our lives will be turned into computerized data and, transformed into information, obtain a new value (see Mayer-Schönberger and Cukier 2013, p. 78); it would also amount to a fundamental transformation of police work from pencil and paper styles to different forms of data analysis. Moreover, and most importantly, it involves a change in the production of police knowledge, with significant effects on the transparency and accountability of police decision making. It is a shift from model-based, causal knowledge production concerned with explanation to data-based and statistically generated forms of knowledge concerned with correlations between disparate data. This does not automatically lead to data-fetishism, as proponents of the big data-age suspect (e.g. Anderson 2008; Wolf 2010), as theoretical knowledge might still be indispensable (Chan and Bennett Moses 2016, p. 28-31). Nevertheless, once disparate, external data sources are used – such as census data or infrastructure data, partly from private geo-marketing firms – the question of data quality becomes extremely important, as the conditions of their production are in-transparent and much less controllable than data gathering practices by police officers. This circumstance poses a new challenge for the evaluation of predictive policing, an evaluation that is difficult anyway due to its preventive nature (Benbouzid, forthcoming).

Yet, to the extent that processes of knowledge production and decision making in police work will become more technical, they will also tend to become more opaque; and the more sophisticated and complex the algorithm utilized for data crunching is, the more difficult will it be to reconstruct the process of information retrieval, with corresponding effects for police accountability (Bennett Moses and Chan, 2018, p. 817-8). This is the more a serious issue, as person-based as well as place-based predictive policing approaches are on the rise. Practices of ethnic profiling may be reinforced in designated risk areas if intensified controls are targeted at

the ‘usual suspects’ (I9, l. 393-398; I24, l. 176-183; I23, l. 145-150; see also Harcourt 2007; Ferguson 2017). Predictive policing thus may also produce feedback loops: the more intensively certain areas are being policed and the more the ‘usual suspects’ are being controlled and registered, the more will the data base be biased against certain minorities, which in turn leads to these areas likely being considered at high crime risk, thus enhancing the need for intensified patrolling and control, and so on (Kaufmann et al. 2018).

**Conclusion: Predictive Policing and a “datalogical turn” in policing?**

Computerized techniques of predictive policing tend to be either embraced or criticized for opening up a new future for policing, one that is shaped by the rationale of pre-empting crime. As we have demonstrated using the example of the German software PRECOBS, current crime prediction software still strongly echoes the logic of conventional risk technologies. Drawing on past experience and historical crime data, it identifies high-risk areas only to employ conventional policing practices such as intensified patrolling. Preemptive elements are nonetheless involved, for example once the algorithmic output triggers possibilistic thinking, as police officers patrolling in the designated area are guided by the expectation that there must be a burglar around. Any person happening to stroll around thus tends to come under suspicion once police officers establish a speculative connection between the spatiotemporal crime prediction and the risk potential of the people present at that location. And it remains to be seen whether it is the experience and the habits of policing that will be prevalent in the ensuing risk assessment (i.e. the usual suspects) and to what extent the technology itself will bring up a variety of new indicators of suspicion: anomalies or irregularities that come to be identified, either because the technology professes that there *must* be a specific type of offender (e.g. burglar) around or because there is a rather unspecified risk indicated. If nothing in particular constitutes a risk, virtually anything might be considered a potential danger.

The future of ‘datalogical’ policing – police work that is not only datafied but also develops a ‘postprobabilistic’ epistemology (Clough et al. 2015) – lies in the assemblages of (big) data policing. This future has already been initiated where heterogeneous data sets are fed in, numerous information sources are connected with each other, and sophisticated, self-learning algorithms that increasingly dispense with theoretical input are employed. Whether this is to be considered progress in policing depends on a variety of conditions, above all on the quality of the data and on the use to which it is put (Prins and Reich 2018). The future of policing depends on the culture of policing and related rules and (legal) regulations: will there be a systematic but also a supervised process of data collection that is in control of the risk criteria or indicators inscribed into the algorithms to figure out suspicious behaviour, suspicious people or crime hot spots? Will there be enough time and space for careful review of the results of digitalized computing, which tend to be taken for granted as being objective? Will there be time for reflection about the logics, that is to say the pressure to act, that the technology itself deploys (e.g. is there an option of not reacting to a crime that has been predicted, or a way out of ever more fields of risk being discovered)? Will reflection on the purpose of predictive policing, including the logic of efficiency that it fosters, be possible? It is still an open question to what extent algorithmic programming and application will lead to an encompassing process of datafication where the distinction, for example, between police matters and the collection of data for economic purposes will dissolve.

Concerning accountability, predictive policing is also likely to bring about organizational and regulative changes: who is to be addressed when false-positives appear, meaning when people are falsely suspected because of a machine-generated prediction? (Ferguson 2012) Are new forms of accountability necessary, and what should they look like? (L61, l. 37-40) As Hardyns and Rummens (2018: 214) note, this is a particularly serious issue if external software tools of private companies are employed, and especially if the prediction process is completely

outsourced as is the case with PRECOBS: who, within the police, is in control of the relevant criteria of prediction and suspicion? (I48, l. 856-561; I30, l. 115-117; I11, l. 320f.; I48, l. 888-894)

Predictive policing is neither good nor bad in itself. Of course, it may well also contribute to more effectivity and more objectivity in the prevention and prosecution of crime. Nonetheless, much will hinge on how the police – and society – deal with the technology. This might also sometimes involve pausing for a moment and not proceeding with everything that is technologically possible – and, notably, not falling into the trap of believing that crime can be eradicated and that technology is the best way to pursue this aspiration. The fictional precogs in Minority Report had the advantage of *really* being able to read the future. This did not prevent their predictions causing serious calamities and confusion on the part of the prospective offenders, who were not even aware that they might commit a crime but were arrested anyway. Any attempt to forestall the future and any belief in this being possible should therefore be treated with caution: we will never be able to anticipate the vicissitudes of life. No data and no algorithms can predict these.

**References**

Accenture, 2015. London Metropolitan Police Service and Accenture Police Solutions Complete Analytics Pilot Program to Fight Gang Crime [online]. Available from: https://www.accenture.com/t20160415T055944__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_8/Accenture-London-Metropolitan-Police-Service-And-Acn-Police-Solutions-v2.pdf [Accessed 6 December 2018].

Altenhain, C., 2017. *Tropicalizing Surveillance: Implementing big data policing in São Paulo, Brazil* [online]. Available from: https://data-activism.net/2017/11/tropicalizing-surveillance-implementing-big-data-policing-in-sao-paulo-brazil/ [Accessed 6 December 2018).

Amoore, L., 2013. *Politics of Possibility*. Durham: Duke University Press.

Amoore, L., 2018. Cloud Geographies: Computing, Data, Sovereignty. *Progress in Human Geography*, 42 (1), 4–24.

Amoore, L. and Raley, R., 2017. Securing with algorithms: Knowledge, decision, sovereignty. *Security Dialogue*, 48 (1), 3–10.

Anderson, B., 2010. Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography*, 34 (6), 777–798.

Anderson, C. 2008. *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete* [online]. In: Wired, 23.06.2008. Available from: https://www.wired.com/2008/06/pb-theory/ [Accessed 16 February 2019].

Andrejevic, M., 2017. To Preempt a Thief. *International Journal of Communication*, 11, 879–896.

Andrejevic, M., 2018. Data Collection without limits. Automated policing and the politics of framelessness. *In*: A. Završnik, ed. *Big Data, Crime and Social Control*. London, GB: Routledge, 93–107.

Aradau, C., 2015., "The signature of security. Big data, anticipation, surveillance." *Radical Philosophy*, 191 (may/june), 21–28.

Aradau, C. and van Munster, R., 2011. *Politics of catastrophe: genealogies of the unknown*. London: Routledge.

Aradau, C. and Blanke, T., 2017. Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory*, 20 (3), 373–391.

Azavea, 2015. *HunchLab: Under the Hood* [online]. Available from: https://cdn.azavea.com/pdfs/hunchlab/HunchLab-Under-the-Hood.pdf [Accessed 6 December 2018].

Balogh, D. A., 2016. Near Repeat-Prediction mit PRECOBS bei der Stadtpolizei Zürich. *Kriminalistik*, 70 (5), 335–341.

Beck, C. and McCue, C., 2009. Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession? *Police Chief* 76 (11), 18–24.

Beck, C., n. d. *The Los Angeles Predictive Policing Experiment* [online]. Available from: https://cortecs.org/wp-content/uploads/2014/11/CorteX_predpol_rapport_Foothill.pdf [Accessed 6 December 2018].

Becker, G. S., 1968. Crime and punishment: An economic approach. *Journal of Political Economy*, 76 (2), 169–217.

Benbouzid, B. forthcoming. Values and Consequences in Predictive Machine Evaluation. A Sociology of Predictive Policing. *Science & Technology Studies*.

Bennett Moses, L. and Chan, J., 2018. Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society*, 28 (7), 806–822.

Berk, R. A., 2012. Presentation given at Chicago Ideas, 10 October 2012. Available from: https://www.chicagoideas.com/videos/forecasting-criminal-behavior-and-crime-victimization [Accessed 12 December 2018].

Berk, R. A. and Bleich, J., 2013. Statistical Procedures for Forecasting Criminal Behavior. A Comparative Assessment. *Criminology & Public Policy*, 12 (3), 513–544.

Biselli, A., 2014. *How-To Analyze Everyone – Teil IX: Predictive Policing oder wenn Vorurteile Algorithmen füttern* [online]. Available from: https://netzpolitik.org/2014/how-to-analyze-everyone-teil-ix-predictive-policing-oder-wenn-vorurteile-algorithmen-fuettern/ [Accessed 6 December 2018].

BKA, 2017. *Presseinformation: Neues Instrument zur Risikobewertung von potentiellen Gewaltstraftätern* [online]. Available from: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html [Accessed 6 December 2018].

Bratton, W., Morgan, J., and Malinowski, S., 2009. *The need for innovation in policing today.* [online]. Available from: https://info.publicintelligence.net/LAPD-PredictivePolicing.pdf [Accessed 6 December 2018].

Brayne, S., 2017. Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82 (5), 977–1008.

Caplan, J. M. and Kennedy, L. W., 2016. *Risk Terrain Modeling: Crime Prediction and Risk Reduction*. Oakland, CA: University of California Press.

Chan, J. 2001. The technological game: How information technology is transforming police practice. *Criminal Justice* 1 (2), 139–159.

Chan, J. and Bennett Moses, L. 2016. Is Big Data challenging criminology? *Theoretical Criminology* 20 (1), 21-39.

Clarke, R. V. G., 1980. Situational crime prevention: Theory and practice. *British Journal of Criminology*, 20 (1), 136–147.

Clarke, R. V. G. and Mayhew, P. M., 1980. *Designing out crime*. London, GB: H.M.S.O.

Clough, Patricia P. Ticineto T., et al. 2015. The Datalogical Turn. *In*: P. Vannini, ed. *Non-Representational Methodologies*. New York, NY: SAGE, 146–164.

Cohen, L. E. and Felson, M., 1979. Social change and crime rate trends: a routine activity approach. *American Sociological Review*, 44 (4), 588–608.

Cornish, D. B. and Clarke, R. V., eds., 1986. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York, NY: Springer.

Costanzo, P., D'Onofrio, F., and Friedl, J., 2015. Big Data and the Italian Legal Framework: Opportunities for Police Forces. *In*: B. Akhgar, et al., eds.: *Application of Big Data for National Security*. Amsterdam, NL: Elsevier, 238–249.

Daase, C. and Kessler, O., 2007. Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger. *Security Dialogue*, 38 (4), 411-434.

Deutscher Bundestag, 2018. *Instrument des Bundeskriminalamtes zur Risikobewertung potentieller islamistischer Gewalttäter* [online]. Available from: http://dip21.bundestag.de/dip21/btd/18/134/1813422.pdf [Accessed 6 December 2018].

Dick, P. K., 2002. Selected Stories of Philip K. Dick. New York, NY: Pantheon.

Farrell, G. and Pease, K., (2014.): Prediction and Crime Cluster. *In*: G. Bruinsma G and W. Weisburd, W (eds.) *Encyclopedia of Criminology and Criminal Justice*. New York, NY: Springer, pp. 3862–-3871.

Ferguson, A. G., 2012. Predictive Policing and Reasonable Suspicion. *Emory Law Journal*, 62 (2), 259-325.

Ferguson, A. G., 2017. *The Rise of Big Data Policing*. New York, NY: New York University Press.

Gerstner, D., 2017. *Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl. Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4*. Freiburg i. Br.: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Gluba, A., 2014. Predictive Policing – eine Bestandsaufnahme. *Kriminalistik*, 68 (6), 347–352.

Haggerty, D. and Ericson, R. V., 2000. The surveillant assemblage. *British Journal of Sociology*, 51 (4), 605–622.

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

Hardyns, W. and Rummens, A. 2018. Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. *European Journal on Criminal Policy and Research* 24 (3), 201–218.

Hays, C. L., 2004. What Wal-Mart Knows About Customers' Habits. *The New York Times* [online], 14 November. Available from: http://www.nytimes.com/2004/11/14/business/yourmoney/what-walmart-knows-about-customers-habits.html [A(accessed 1.6 December .2018).

Hess, K. M., Orthmann, C. H., and Cho, H. L., 2013. *Police Operations: Theory and Practice*. 6.th Ed. Clifton Park, NY: Delmar Cengage Learning.

Jasanoff, S., 2015. Future Imperfect: Science, Technology, and the Imaginations of Modernity. *In*: S. Jasanoff and S. H. Kim, eds. *Dreamscapes of Modernity*. Chicago, IL: University of Chicago Press, 1–33.

Jasanoff, S., 2017. Virtual, visible and actionable: Data assemblages and the sightlines of justice. *Big Data & Society*, 4 (2), 1–15.

Johnson S. D., et al. 2007. Space–Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization. *Journal of Quantitative Criminology*, 23 (3), 201–219.

Kaufmann, M., 2018. The co-construction of crime predictions. *In*: Fyfe, Nicholas R.; Gundhus, Helene O. I.; Vrist Rønn, Kira, eds. *Moral Issues in Intelligence-led Policing*. London, GB: Routledge, 143-160.

Kaufmann, M., Egbert, S., and Leese, M., 2018. Predictive Policing and the Politics of Patterns. *British Journal of Criminology*, Online First 7 December 2018.

Kitchin, R., 2017. Thinking critically about and researching algorithms. *Information, Communication & Society*, 20 (1), 14–29.

Krasmann, S., 2012. Targeted Killing and Its Law: On a Mutually Constitutive Relationship. *Leiden Journal of International Law*, 25 (3), 665–682.

Krasmann, S., 2018. Enemy Penology. *In*: H.N. Pontell, ed. *The Oxford Research Encyclopedia of Criminology and Criminal Justice* [online]. Available from: http://oxfordre.com/criminology/abstract/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-365?rskey=6dOHrh&result=1 [Accessed 6 December 2018].

Mantello, P., 2016. The machine that ate bad people: The ontopolitics of the precrime assemblage. *Big Data & Society*, 3 (2), 1–11.

Mayer-Schönberger, V. and Cukier, K., 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London, GB: John Murray.

McCue, C. and Parker, A., 2003. Connecting the Dots: Data Mining and Predictive Analytics in Law Enforcement and Intelligence Analysis. *The Police Chief*, 70 (10), 115–122.

McCue, C. McL., 2012. Operational Security Analytics: My Path of Discovery. *In*: M.M. Gaber, ed. *Journeys to Data Mining: Experiences from 15 Renowned Researchers*. Berlin, DE: Springer, 131–146.

Middendorf, R. and Schweer, T., 2018. *Von der Steckkarte zum Dashboard – PRECOBS als integraler Bestandteil moderner Polizeiarbeit*. Presentation given at 2nd PRECOBS-User Symposium on 19 June 2018 in Aarau (on file with authors).

Mohler G. O., et al., 2011. Self-Exciting Point Process Modeling of Crime. *Journal of the American Statistical Association*, 106 (493), 100–108.

Mohler, G. O., et al., 2015. Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association*, 110 (512), 1399–1411.

Okon, G., 2015. Vorhersagen von Straftaten – Vision oder Wirklichkeit? *arcAKTUELL* 4/2015, 22–23.

Okon, G., 2018. *PRECOBS Enterprise – Herausforderung und Chance für die moderne Polizeiarbeit*. Presentation given at 2nd PRECOBS-User Symposium on 19 June 2018 in Aarau (on file with authors).

Papachristos, A., 2009. Murder by structure: dominance relations and the social structure of gang homicide. *American Journal of Sociology*, 115 (1), 74–128.

Papachristos, A., Braga, A., and Hureau, D., 2012. Social networks and the risk of gunshot injury. *Journal of Urban Health*, 89 (6), 992–1003.

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*. Santa Monica, CA: RAND.

Police Executive Research Forum, 2014. *Future Trends in Policing*. Washington, D.C.: Office of Community Oriented Policing Services. Available from: http://www.policeforum.org/assets/docs/Free_Online_Documents/Leadership/future%20trends%20in%20policing%202014.pdf [Accessed 6 December 2018].

Police-IT, 2018. Palantir Gotham alias Hessendata: System und Funktionsweise [online]. Available from: https://police-it.org/palantir-gotham-alias-hessendata-system-und-funktionsweise [Accessed 8 December 2018].

Prins, S. J. and Reich, A. 2018. Can we avoid reductionism in risk reduction?. *Theoretical Criminology* 22(2), 258–278.

Reigeluth, T., 2014. Why data is not enough: Digital traces as control of self and self-control. *Surveillance & Society*, 12 (2), 243–254.

Rouvroy, A., 2012. The end(s) of critique: data-behaviourism vs. due-process. *In*: M. Hildebrandt and K. de Vries, eds. *Privacy, Due Process and the Computational Turn*. New York, NY: Routledge, 143–167.

Rubin, J., 2010. Stopping Crime before it starts. *Los Angeles Times* [online], 21 August 2010. Available from: http://articles.latimes.com/2010/aug/21/local/la-me-predictcrime-20100427-1 [Accessed 6 December 2018].

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 (3), 347–371.

Schweer, T., 2015. „Vor dem Täter am Tatort" – Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs. *Die Kriminalpolizei*, 32 (1), 13–16.

Schweer, T., 2016. Predictive Policing – Straftaten erkennen und verhindern, bevor sie passieren. *Deutsches Polizeiblatt* 34 (1), 25–27.

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 40 (1). St. Gallen: Universität St. Gallen, 12-14.

Schweer, M. and Schweer, T., 2015. Musterbasierte Prognosetechnik bei der Kriminalitätsbekämpfung – Die Methodik der Near Repeat Prediction. *Polizeispiegel* 49 (5), 22–24.

Shapiro, A., 2017. Reform predictive policing. *Nature* 541 (7638), 458–460.

Sidebottom, A. and Wortley, R., 2016. Environmental Criminology. *In*: A.R. Piquero, ed. *The Handbook of Criminological Theory*. Chichester: John Wiley & Sons, 156–181.

Strauss, A. L., Corbin, J. M. 1990. Basics of Qualitative Research. Grounded Theory Procedures and Techniques. Newbury Park: SAGE.

Suckow, O., 2018. Grundlagen des Predictive Policing: Near-Repeat-Victimisation im ländlichen Raum. *Kriminalistik*, 72 (6), 347–356.

Townsley, M., Homel, R., and Chaseling, J., 2003. Infectious Burglaries. *British Journal of Criminology*, 43 (3), 615-633.

Uchida, C. D., 2009. *Predictive Policing in Los Angeles: Planning and Development* [online]. Available from: http://newweb.jssinc.org/wp-content/uploads/2012/01/Predictive-Policing-in-Los-Angeles.pdf [accessed 7 December 2018].

Uchida, C. D., 2014. Predictive Policing. *In*: G. Bruinsma, D. Weisburd, eds. *Encyclopedia of Criminology and Criminal Justice*. New York, NY: Springer, 3871–3880.

van Brakel, R., 2016. Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing. *In*: B. van der Sloot, D. Broeders, and E. Schrijvers, eds. *Exploring the Boundaries of Big Data*. Amsterdam, NL: Amsterdam University Press, 117–141.

Van Daele, S. and Vander Beken, T. 2011. Outbound Offending: The Journey to Crime and Crime Sprees. *Journal of Environmental Psychology* 31 (1), 70–78.

Willems, D. and Doeleman, R. 2014. Predictive Policing – wens of werkeleijkheid? *Het Tijdschrift voor de Politie*, 76 (4/5), 39–42.

Wilson, D., 2018a. Algorithmic Patrol. The futures of predictive policing. *In*: A. Završnik, ed. *Big Data, Crime and Social Control*. London: Routledge, 108–127.

Wilson, D., 2018b. *The Instant Cop: Time, Surveillance and Policing*. Presentation given at 8th Biennial Conference of the Surveillance Studies Network in Aarhus, 8 June 2018 (on file with authors).

Wolf, G. 2010. *The Data-Driven Life* [online]. Available from: http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?_r=0 [Accessed 16. February 2019).

Wortley, R. and Townsley, M., eds., 2017. *Environmental Criminology and Crime Analysis*. 2nd Edition. London: Routledge.