We Do That Once Per Day

Cyclical Futures and Institutional Ponderousness in Predictive Policing

13 ‘We do that once per day’

Cyclical futures and institutional ponderousness in predictive policing[1]

Matthias Leese

In recent years, predictive policing has ascended to become a pertinent form of addressing the future in the everyday production of security. Underpinned by the promise of catching a criminal before the crime – or at least to be ‘at the crime scene before the criminal’ (Schweer 2015) – predictive policing seeks to reorganize police work in terms of efficiency and effectiveness through the algorithmic calculation of crime risk. Such risk is usually structured along the dimensions of time and space, so that the presumed occurrence of future crime can be located in specific neighbourhoods and during specific timeframes. Subsequently, so the rationale goes, resources can be reallocated accordingly and preventive efforts can be undertaken, so that the predicted offences will not materialize (e.g. McCue 2007; McCue and Parker 2003; Perry *et al*. 2013). Preventive measures thereby usually consist of a combination of intensified patrols (plain-clothed and/or in uniform), traffic controls, and awareness campaigns in the identified neighbourhoods.

This chapter investigates the precise temporal modalities that emerge in addressing the future through algorithmic analyses of crime data. It argues that there is a considerable rift between the techno-imaginary of seamlessness and continuous flows of live data that result in real-time situational updates and maximum responsiveness on the one hand, and the static ways in which police departments use predictive policing software on the other. Due to the asynchronicity between crime and police work, the police consider it in fact sufficient to analyse crime data only once per day and work with the produced predictions for up to seven days. The daily use of predictive policing software thereby decisively undercuts narratives of real-time analysis and ensuing operational flexibility vis-à-vis a supposedly dynamic threat environment. This practice becomes reinforced and aggravated by limited personnel resources that produce a certain institutional ponderousness when it comes to the street-level enactment of crime prevention measures. Overall, so this chapter puts forward, the temporalities of predictive policing speak closely to the characteristics of the addressed type of crime and to entrenched operational requirements of police work. Predicting the future must in this sense be considered as an iterative, everyday activity that is characterized by a deliberatively short time frame.

Empirical research for this article consisted of multiple ethnographic observations in four German and Swiss police departments that have implemented the software package PRECOBS ('Pre Crime Observation System') by German manufacturer IfmPt,[2] as well as 23 semi-structured expert interviews with involved police officers and software developers, conducted between June 2016 and August 2017. Interview recordings have been transcribed and coded using qualitative data analysis software. All collected material has been anonymized as per agreement with the researched institutions and individuals. Quotations have been translated from German by the author.

The chapter proceeds as follows. First, it provides a brief overview of the distinct empirical approaches to predictive policing, foregrounding the underlying assumptions of prevalent spatio-temporal forms of prediction, and introducing the PRECOBS software package that has been implemented in the researched departments. Working through the empirical material, it then specifies the ways in which predictive policing is practised in everyday police work and analyses the modes in which criminal futures come into being. It concludes by contextualizing everyday predictive policing operations within larger trajectories of prediction and politics, as discussed by the other contributions to this volume.

Predictive policing with PRECOBS

Predictive policing is not one practice, one model, or even one software package (e.g. Bennett Moses and Chan 2016; Kaufmann 2018; Perry *et al*. 2013). Rather, the notion of predictive policing must be understood as a broad label for a variety of ways of bringing criminal futures into being and rendering them actionable. Variance thereby stems from different forms of implementation into everyday police work, as well as from theoretical assumptions, models, and the data that these models are predicated upon. The common denominator of all of them is the managerial aspiration to be able to 'do more with less' (Beck and McCue 2009) through an increase in efficiency and effectiveness. This is supposed to be realized through the underpinning rationale that once an empirically informed prediction of crime-relevant futures has been created, police work on the street level can subsequently be restructured and available resources can be reallocated to areas where crime prevention measures promise to be most successful.

On a more fundamental organizational level, predictive policing in this sense has the capacity to transform the relation that the police build with the future. Unlike earlier manual practices of crime mapping, the promise of predictive policing rests on the combination of digitization, processing power, and the algorithmic exploitation of data. Taken together, these elements present the police with the opportunity to address the future on an unprecedented scale and with unprecedented speed. Criminal futures, at least in theory, are only one mouse-click away, and this novel availability opens up a new set of operational options in terms of actively intervening into these futures as they unfold.

Within the current landscape of predictive policing, two major paradigms can be identified. On the one hand, there are methods that seek to predict *offenders*, thereby creating risk profiles that identify individuals who are more likely to commit crimes or become victims of crime. Such approaches, as for instance used by the Chicago Police Department in its prominent 'strategic subject list' (Saunders *et al*. 2016) have garnered much public attention and critical debate (e.g. Dallke 2017; Gorner 2013; Stanley 2014), as they rely on the collection and combination of data about individuals, possibly including the likes of communication data and social network data. These data are then combined and processed in order to identify individual proximity to crime, for example through algorithmic association rules. Living in a crime-ridden neighbourhood or interaction with known gang members would in this sense serve as indicators that a person could be more likely to either become a victim of crime or an offender, and should thus be targeted through prevention programmes.

The underlying ambition of such wide-ranging data collection and advanced analytics for individualized crime predictions, coupled with a lack of transparency about how risk profiles are in fact calculated, has sparked rather dystopian readings of predictive policing as a form of surveillance and coercion, where state agencies would use an information edge to govern and control populations (e.g. Andrejevic 2017; Hildebrandt 2016; Mantello 2016). Such concerns should not be easily dismissed, as commercial software suppliers and police departments, particularly in the US, are pushing further into this direction. As of today, the majority of regularly implemented predictive policing tools however follow a quite different route into addressing the future. Instead of individuals, they foreground the *place and time* of future criminal activity (Bennett Moses and Chan 2018; Egbert 2017; Gluba 2014; Gluba and Pett 2017; Perry *et al*. 2013).

The most commonly used approach in current predictive policing practices is thereby based on near-repeat modelling. The near-repeat hypothesis rests upon the empirical observation that the best predictor for victimization is in fact victimization itself. In other words, a person or a place that has already experienced crime is more likely to experience further crime than a person or a place that has not (e.g. Farrell 1995; Farrell *et al*. 1995). This observation is particularly pertinent for burglaries, whereby the near-repeat hypothesis presupposes that when within a specific area a burglary has been recorded, there is an increased likelihood for follow-up offences in that area in the following days (e.g. Polvi *et al*. 1991; Townsley *et al*. 2003). Near-repeat models are thereby undergirded by assumptions of rational choice that conceptualize criminal behaviour as conscious decision-making that is guided by opportunities and cost-benefit calculations (e.g. Clarke and Felson 1993; Cohen and Felson 1979; Sidebottom and Wortley 2016), including the repetition of once successful criminal activities (e.g. Farrell and Pease 2014; Johnson *et al*. 2007).

In PRECOBS, future burglaries are predicted through an estimation of individual offender behaviour based on so-called trigger incidents. The functionality

of the software package revolves around the notion that from these trigger incidents, a spatially and temporally connected occurrence of follow-up offences can be predicted. Underpinning here is the assumption that most burglaries are committed by professional criminals who identify profitable target areas, strike multiple times within a short time period, and then move on before the police can react and come up with adequate countermeasures. These professionals, so the rationale goes, can be distinguished from non-professionals through the characteristics of the offence (i.e. the modus operandi). Thus, if a reported burglary is characterized by non-violent and silent ways of gaining access to the dwelling, as well as easily transportable haul with a high resale value, the assumption would be that the offence was committed by professionals and that the same offenders would strike again in the same neighbourhood within a short timeframe.

In order to assess whether a recorded burglary should in fact be regarded as a trigger incident and whether preventive measures should be undertaken in that neighbourhood, PRECOBS processes crime data logged by the police, notably making use of the variables 'time of the incident', 'modus operandi', 'haul', 'type of dwelling', as well as the GIS coordinates (Schweer 2015: 13). If, through the algorithmic analysis of such data, a supposedly professional burglary is identified, the software triggers an alert that specifies the likelihood of follow-up offences within a radius of 400 metres and a timeframe of up to seven days (the highest likelihood for near-repeats falls within the first three days). The software allows for an adjustment of both the spatial dimension (the radius can be reduced or expanded, and manually adapted to fit the topographic characteristics of a neighbourhood) and the duration throughout which the alert is to remain valid. Alerts are double-checked by human operators in order to reduce false positives and are then circulated to operational planning and dispatch divisions within the police department, where increased street patrols and other preventive measures in the identified areas are scheduled.

Predictive policing manufacturers such as IfmPt thereby advertise their commercial software packages in ways that suggest live awareness of any situational changes through continuous and automated analyses 'as new crimes come in'[3] or 'receiving current crime data'.[4] The sales pitch here is that future crime risk can be continuously updated and thereby enable maximum responsivity of police work, so that street patrols can be flexibly reorganized whenever new alerts occur. Predictive policing is in this sense imagined as an uninterrupted process that continuously produces and adjusts criminal futures, in the best case scenario executed in an automated fashion in order to provide as much real-time support for police work as possible – and at the same time requiring as little human input as possible. The narrative that underpins algorithmic security tools more generally is in fact often one of automation and seamlessness, whereby live data goes into the system and is analysed in real-time, so that the results can then be circulated back into the context of application without substantial time lags, thus guaranteeing maximum timeliness of security production (e.g. Amoore 2009, 2011; Leese 2014; Massumi 2007).

What results from such an angle is an imaginary of an always-present relationship with the future, creating minimum response times to whatever security threat might be identified through the ongoing stream of live data. This idea of seamlessness corresponds with a supposedly dynamic and contingent threat environment in which security agencies need to be able to quickly react and adapt, and therefore keep their situational awareness at a maximum level at any time. As Aradau and Blanke (2017: 384) put forward, when it comes to security, algorithmic analytics are indeed 'not primarily about the turn to the future but about near-real-time decision-making'. The assumption here is that on the operational level, flexibility and reactive capacities would crucially rely on continuous situational analyses in order to empower effective interventions. From a technological vantage point, such a seamless and continuous mode of algorithmic prediction would certainly be possible, as there are in fact few limitations when it comes to real-time processing capacities of live data streams. One software developer described how predictive policing software could in theory be implemented into police work:

> You can run that in a fully automated fashion, that's no problem. Technology can do anything. The system can process any kind of data. You can process personal data, you can process different data from different sources – that's no problem from a technical point of view.
>
> (Interview, 9 June 2016)

Such an angle speaks closely to the managerial logic that is inherent in the idea of predictive policing in the first place: Only when the software blends seamlessly into its operational environment and commands no specific attention can the dictum of 'doing more with less' be efficiently realized. And only then can algorithmically generated predictions be translated into street patrols who arrive at the crime scene before the criminal in order to capture the offender – or at least prevent the offence from its materialization. While such a techno-narrative is a compelling one, it must however not be confused with the actual ways in which technological tools become implemented within institutions and work routines. Once rolled out into the 'real world', technologies often become used in unforeseen and creative ways (Pinch and Bijker 1984) that are quite distinct from their developer's original intentions or marketing narratives and unfold unforeseen (side-)effects (e.g. Collingridge 1981; Tenner 1997; Winner 1980). In other words, if we seek to understand the repercussions of new technologies, we must take into account how they become appropriated and used on an everyday basis.

The emergence of cyclical futures

Predictive policing must in this sense not be understood as merely a technological tool, but as a socio-technical assemblage (Law 1991) that requires special attention to its specific forms of implementation and practice. Only through

such contextualization can transformations of policing by means of new algorithmic software packages be adequately addressed (e.g. Bennett Moses and Chan 2016; Kaufmann 2018; Sanders and Condon 2017; Smith *et al*. 2017). The specific modes of bringing criminal futures into being with PRECOBS thus command an empirical perspective on the use of the software package within institutional environments and organizational work routines. In fact, empirical research within multiple police departments revealed that PRECOBS was not used in an automated and continuous fashion, but rather in quite static and non-automated ways. One major reason for this could be found in larger relationships between crime and the organization of police work. As one interviewee explained how the software package was implemented into the work routines of their department:

> Our officers who respond to the call will log the burglary. […] We used to have a little black notebook into which everything was entered, but now they have iPads – we are fully equipped when it comes to that. And there is a simplified reporting form, where the main characteristics are retrieved: what is the exact timeframe of the offense, the specifics of the area, what was stolen, modus operandi? All that goes into the database on-the-fly. And there, you could have automated queries. But in our department, we have to put the data on a flash drive, because we run [PRECOBS] as a stand-alone solution, and we have to load the data into the system.
>
> (Interview, 1 June 2016)

What is striking in this statement, first of all, is that the PRECOBS is used as a stand-alone solution, meaning that the system is not online, or even automatically connected with the central database that police departments use for recording and administering crime data. Even though logging procedures at the crime scene are digitized and central database updates can therefore be realized almost in real-time, the software is installed on a notebook computer with no network connection. This practice speaks to both data protection requirements and maintenance procedures, as the system can through a separation from the police intranet be updated and tweaked easily and without time-consuming bureaucratic procedures (Interviews, 20 March 2017; 16 August 2017).

This separation however produces a situation in which, prior to any actual analysis, crime data has to be transferred to the notebook via flash drive and then manually imported into the software.[5] The operator then runs the program and double-checks any potential alert outputs before producing a brief summary (usually a one-page pdf file per confirmed alert prognosis) of the situational analysis that is subsequently passed on to the operational planning unit. The analysis of crime data is thereby executed only once per day. Once the analysis is finished, the notebook with the PRECOBS software package is stowed away for the rest of the day and only reopened on the following day. Such a once-per-day approach to predictive policing appears puzzling at first sight, as it contradicts the manufacturer's ambitions of seamlessness and real-time situational analysis, and

at the same time seemingly undercuts the reorganization of police work around the principles of efficiency and effectiveness. The once-per-day way of using PRECOBS must however be understood against the backdrop of larger temporal relations between crime and the policing thereof. As one interviewee put it:

> 'That takes place every morning. We log the burglaries of the previous night […] and then we export the past 24 hours or simply the whole dataset, and that goes into the system again.'
>
> Q: 'The dataset is updated every day?'
>
> 'Yes. The system – well it's not exactly 24 hours, but a longer timeframe that we import, but the system checks whether entries have already been processed or not. Because the burglary could have been logged retroactively, from an earlier point in time.'
>
> (Interview, 16 August 2017)

What becomes apparent from this statement is the fundamental and essentially unresolvable predicament that the police face with regard to the asynchronicity of crime and police work. In other words, there will always be a time lag between the occurrence of crime and its detection, reporting, logging, and analysis. All of these consecutive steps however need to take place before, based on the eventual analysis of crime data, preventive measures based on algorithmic calculations can be brought to the street level. This temporal predicament is particularly pertinent for burglaries, as offenders usually strike when residents are not at home. Consequently, many offences will only be detected hours or even days after their occurrence, and even if they are immediately reported and officers are instantly available to log them, substantial time will pass between the actual burglary and the analysis of the ensuing data. Any aspirations of real-time situational awareness and flexibility are therefore undercut by the condition of asynchronicity in the first place, which is why the police in fact consider a once-per-day rhythm of crime prediction sufficient:

> At the moment we have a daily rhythm. We could adjust that, but usually there isn't much dynamic here, so that you would have to do that every hour. If you have the data in the system, you could of course update every minute. But we realized that once per day is enough for situational analysis. In the morning, you have to determine which new burglaries came in, because what happened over night is usually noticed in the morning and then reported. That means you wait until you can include these and analyze them for the daily situational analysis, and that's enough.
>
> (Interview, 1 September 2016)

This is not to say that the police would not make a dedicated effort to log crimes and create crime data as quickly as they possibly could. Quite on the

contrary, among the researched departments, most used digital devices at the crime scene, so that the created data could be automatically transferred to the central database system. This acceleration would, however, not resolve the fundamental asynchronicity inherent in the policing of burglaries. As one interviewee described the time lag dilemma faced against the backdrop of effective crime prevention in their everyday work in detail:

> We have the data in the central system after 15 minutes or half an hour. But getting ahead of the situation more than that, I doubt that this will be possible. Because the current series that happened during the day or during the night – I will only find out about that on the next morning. That I'll be so close to the situation that I log a crime and the burglars are still active in that very same street – I wouldn't say that never happens, but it is very rare. I log a burglary, and then another one, but those happened three hours ago, or four hours. And then I need to get ahead of the situation for the next cycle, when the offender could return, and that's 24 hours.
>
> (Interview, 22 June 2017)

The temporalities of predictive policing, as these accounts demonstrate, must thus be understood in close conjunction with crime itself and the corresponding organization of police work. In the case of PRECOBS and its focus on burglaries, the assumption is that most burglaries are committed by professionals who act rationally and strike within certain timeframes when there is the least risk of being caught, thus leading to the occurrence of offences in cycles of 24 hours. From such considerations, the implementation of PRECOBS in the researched departments has logically emerged as a once-per-day activity that derives from the operational requirements of everyday police work. These cyclical futures cover a comparatively short time horizon that falls in line with the organizational culture and requirements of policing. And even though they could be considered as merely small fragments of foresight, they do in fact constitute a never-ending puzzle that is continuously assembled at the speed of one piece per day.

Limited resources and institutional ponderousness

The empirically diagnosed 24-hour rhythm of crime prediction not only stands in stark contrast to imaginaries of 'live crime data' and 'real-time analysis', but it becomes further reinforced by organizational structures within the police as an institution. Predictive policing must not be reduced to situational analysis, but can unfold an impact on crime prevention only when, in a second step, predictions are put into practice on the street level (e.g. Bennett Moses and Chan 2016; Perry *et al*. 2013). This in turn means that the implementation of criminal futures must fit in with the requirements of different police divisions. Notably, operational planning and dispatch units occupy a central position in practices of predictive policing, as available forces need to be scheduled for street patrols

and other preventive measures according to the produced crime predictions. However, within larger trajectories of limited personnel resources and the need for flexible rescheduling that the use of predictive policing software presupposes, a certain institutional ponderousness can be encountered. Interviewees from different police departments described the problems of work organization and the potential disruptions posed by a continuous use of PRECOBS as follows:

> We pass on the information to the operational planning division who are responsible for operational measures. And they also have to do their scheduling. So if I tell them at 9:00 that we have an alert, and we have these personnel resources available and assign them to the alert – and then at 11:00 I tell them that we have another alert, then that's not an efficient process, because they will have to reschedule. Or they can't react at all. That means there will be no benefits from faster communication of alerts.
>
> (Interview, 22 June 2017)

> The main issue is of course the response time of the operative units. Because let's be honest, […] when we have an alert at 8:00, and another one at 16:00, our forces probably won't be able to react, or only on a limited scale. And that's a problem, of course. We don't have the capacities.
>
> (Interview, 6 July 2017)

These quotes quite aptly illustrate the dilemma that police departments face in the use of predictive policing software: In order to realize the potential of increased efficiency and effectiveness, a certain level of flexibility is required, and such flexibility is in turn tied to the availability of sufficient personnel resources. In other words, whereas the managerial aspiration of predictive policing is to resolve the quandary of shrinking budgets and decreasing numbers of available personnel on the ground through a flexible and target-oriented reallocation of resources, such an implementation would still require sufficient resources in order to enable police departments to be responsive to this newly acquired flexibility.

As put forward by many of the interviewees, particularly in less urban environments, a major obstacle would be the fact that there simply would not be enough forces available to be able to react to potential live situational updates and to adapt preventive measures in new risk areas. From an organizational angle, the once-per-day mode of addressing the future was thus again seen as sufficient, as institutional inertial force would prevent a real-time level of responsiveness anyway. Once more, what becomes apparent here is a discrepancy between the imaginary of algorithmically supported policing through situational awareness, and actual practices that were limited by a set of institutional and organizational constraints. The prospect of having to constantly reallocate personnel resources was thereby regarded as inefficient in itself, as the resources required would outweigh the potential benefits.

Such institutional ponderousness in predictive policing becomes furthermore aggravated when multiple alerts are active at the same time. With each new alert, a new criminal future becomes inscribed in space and time and adds an additional layer to the set of futures that must be reacted to. Predictions created with PRECOBS remain active for a period of up to seven days, during which according to near-repeat theory an increased likelihood of follow-up burglaries can be expected. In the researched police departments, against the backdrop of limited personnel resources, operational planning and dispatch divisions were thus struggling with the amount of simultaneous alerts, even as they were produced only once per day. As one interviewee aptly summarized the situation: 'We have to prioritize. We have three alerts, which one should we prioritize?' (Interview, 6 July 2017)

Predictive policing thus pushes existing organizational structures in police departments to the brink in two closely related ways. First of all, available personnel resources were in the researched departments not fit for flexible rescheduling and short response times to real-time situational updates. Quite on the contrary, the police already struggle with their resources in times of budget cuts. And second, whereas predictive policing starts from the idea of enabling police departments to 'do more with less', notions of efficiency and effectiveness could presumably be mobilized as arguments against budget increases, as an assignment of additional resources would contradict the managerial attractiveness of predictive policing in the first place.

Conclusion

From the analysis of the practices of predictive policing in multiple German and Swiss police departments presented throughout this chapter, several conclusions can be drawn with regard to the modes in which criminal futures are addressed and rendered actionable. First of all, and generally speaking, the time horizon of predictive policing is a comparably short one. Unlike other domains that prescribe mid-term or long-term engagement, such as global health (Jasper 2020), crime can only meaningfully be subjected to predictions on a scale of a few days. Second, practical forms of the implementation of predictive policing software follow entrenched institutional structures and organizational routines of the police as an institution rather than speaking to techno-imaginaries that are predicated upon notions of seamlessness, automation, and real-time. Third, limited personnel resources and ensuing institutional ponderousness further aggravate the static ways in which algorithmic software packages become part of everyday police work.

As near-repeat theory presupposes that the likelihood of follow-up crimes is at the highest within close spatial and temporal proximity of the initial offence, in the researched departments, alerts remained active for a timeframe of up to seven days. The futures that are brought into being within predictive policing are thus kept on a limited time horizon, as their purpose is to enable short-term prevention measures. If analytical foresight follows the operational aspiration to

anticipate and preempt the next move of professional criminals, then this must be done within a couple days or the prediction itself will have been in vain. Criminal futures in the form of spatio-temporal risk alerts are thereby considered as relatively stable and need not be further updated after they have been calculated once. They do however become supplemented by new layers of criminal futures in cycles of 24 hours, so that the short-term horizon of predictive policing is constantly renewed in both time and space.

The idea of short-term futures thereby closely speaks to the temporal characteristics of crime and the corresponding organization and institutionalization of police work. The asynchronicity between crime and police work, as well as the assumption of 24-hour cycles between burglaries that are connected through near-repeat patterns, render it sufficient to address the future in a once-per-day fashion in order to prepare for the ensuing iteration of criminal activity. Moreover, as algorithmic predictions must be enacted through preventive measures on the street level, limited resources and organizational routines of distinct police divisions interfere with ideas of flexibility and responsiveness. Instead, predictive policing becomes characterized by institutional ponderousness that stems from already limited resources. Empirically, predictive policing thus comes into being as a practice that is limited by larger institutional and organizational contexts of police work, thus resulting in the empirically encountered forms of implementation.

It should however be kept in mind that predictive policing is a comparably recent phenomenon. There are still relatively few commercial software packages available, and many police departments that have not yet implemented any of them are running trials in order to figure out how to use algorithmic support most effectively and efficiently. The same is true for the manufacturer side: The PRECOBS software package is regularly revised, and engineers and designers are responsive to the operational needs of the police. At the time of writing (December 2017), IfmPt has announced the roll-out of a new software version that pushes further into automation and integration into police databases through a server-based architecture that allows for networked access and analysis. Other police departments are designing or already implementing custom-built predictive policing tools (Interview, 7 March 2017). And more mobile devices such as smartphones and tablets for street patrols mean that communication between situational analysts and officers on the ground could become quicker and more direct.

It will remain to be seen how such new developments will further alter predictive policing practices, and whether the institutional and organizational constraints sketched out in this chapter will remain in place. After all, what will not change is the asynchronicity of crime and policing, and the organizational routines built around this relationship. As one police officer neatly summed up this fundamental condition:

> It is of course possible that others argue that it makes more sense to run the analysis twice per day, or four times per day, or even continuously. But I think we should not forget that we are speaking about an overall situation.

> […] You must not overexert your people with continuous new alerts. You run your situational analysis in the morning, and that's just like the weather: what will the weather be like for today? You don't want to be constantly updated, and usually that is not necessary either.
>
> (Interview, 1 September 2016)

Notes

1 The research for this chapter was partly funded by the Fritz Thyssen foundation (Grant No. 10.16.2.005SO). Much appreciation goes to Simon Egbert for constructive comments on an earlier version of this chapter.

2 Institut für musterbasierte Prognosetechnik (Institute for Pattern-Based Prediction Technique), www.ifmpt.com (accessed 17 November 2017).

3 PredPol, www.predpol.com/technology (accessed 17 November 2017).

4 PRECOBS, www.ifmpt.com (accessed 17 November 2017).

5 It should be noted here that, although throughout the majority of the researched police departments, this was the standard procedure, one department had established a direct link between PRECOBS and its central database, so that crime data did not have to be imported manually (Interviews, 7 March 2017; 24 July 2017).

References

Amoore, L. (2009) 'Algorithmic War: Everyday Geographies of the War on Terror', *Antipode* 41(1): 49–69.

Amoore, L. (2011) 'Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times', *Theory, Culture and Society* 28(6): 24–43.

Andrejevic, M. (2017) 'To Preempt a Thief', *International Journal of Communication* 11: 879–96.

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): 373–91.

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(11).

Bennett Moses, L. and Chan, J. (2018) 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability', *Policing and Society* 28(7): 806–22.

Clarke, R. V. and Felson, M. (1993) *Routine Activity and Rational Choice*, New Brunswick: Transaction Publishers.

Cohen, L. E. and Felson, M. (1979) 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review* 44(4): 588–608.

Collingridge, D. (1981) *The Social Control of Technology*, London: Palgrave Macmillan.

Dallke, J. (2017) 'Chicago PD Sued over Crime Prediction Algorithm', *ChicagoInno*, 8 June. Online. Available: www.americaninno.com/chicago/chicago-pd-sued-over-crime-prediction-algorithm (accessed 30 November 2017).

Egbert, S. (2017) 'Siegeszug der Algorithmen? Predictive Policing im deutschsprachigen Raum', *Aus Politik und Zeitgeschichte* 67(32–33): 17–23.

Farrell, G. (1995) 'Preventing Repeat Victimization', *Crime and Justice* 19: 469–534.

Farrell, G. and Pease, K. (2014) 'Prediction and Crime Clusters', in G. Bruinsma and D. Weisburd (eds) *Encyclopedia of Criminology and Criminal Justice*, New York, Heidelberg, Dordrecht, London: Springer, 3862–71.

Farrell, G., Phillips, C. and Pease, K. (1995) 'Like Taking Candy: Why does Repeat Victimization Occur?', *British Journal of Criminology* 35(3): 384–99.

Gluba, A. (2014) 'Predictive Policing – eine Bestandsaufnahme: Historie, theoretische Grundlagen, Andwendungsgebiete und Wirkung', *Kriminalistik* (6): 347–52.

Gluba, A. and Pett, A. (2017) 'Predictive Policing: Ein (un)bekannter Ansatz: Definition, Ursprung und Rahmenbedingungen', in M. H. W. Möllers and R. C. van Ooyen (eds) *Jahrbuch Öffentliche Sicherheit 2016/2017*, Frankfurt: Verlag für Polizeiwissenschaft, 431–40.

Gorner, J. (2013) 'Chicago Police Use "Heat List" as Strategy to Prevent Violence', *Chicago Tribune*, 21 August. Online. Available: http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list (accessed 30 November 2017).

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*, London, Thousand Oaks, New Delhi, Singapore: Sage, 406–28.

Jasper, U. (2020) 'The Anticipative Medicalization of Life: Governing Future Risk and Uncertainty in (Global) Health', in A. Wenger, U. Jasper and M. Dunn Cavelty (eds) *Probing and Governing the Future: The Politics and Science of Prevision*, London and New York: Routledge, 122–40.

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(3): 201–19.

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*, London: Routledge, 143–60.

Law, J. (1991) 'Introduction: Monsters, Machines and Sociotechnical Relations', in J. Law (eds) *A Sociology of Monsters: Essays on Power, Technology and Domination*, London, New York: Routledge, 1–23.

Leese, M. (2014) 'The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union', *Security Dialogue* 45(5): 494–511.

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

Mantello, P. (2016) 'The Machine that Ate Bad People: The Ontopolitics of the Precrime Assemblage', *Big Data and Society* 3(2): 1–11.

Massumi, B. (2007) 'Potential Politics and the Primacy of Preemption', *Theory and Event* 10(2): 1–21.

McCue, C. (2007) *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*, Burlington, Oxford: Elsevier.

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): 115–24.

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: RAND Corporation.

Pinch, T. J. and Bijker, W. E. (1984) 'The Social Construction of Facts and Artefacts: Or how the Sociology of Science and the Sociology of Technology Might Benefit Each Other', *Social Studies of Science* 14(3): 399–441.

Polvi, N., Looman, T., Humphries, C. and Pease, K. E. N. (1991) 'The Time Course of Repeat Burglary Victimization', *British Journal of Criminology* 31(4): 411–14.

Sanders, C. and Condon, C. (2017) 'Crime Analysis and Cognitive Effects: The Practice of Policing *through* Flows of Data', *Global Crime* 18(3): 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(3): 347–71.

Schweer, T. (2015) ' "Vor dem Täter am Tatort": Musterbasierte Tatortvorhersagen am Beispiel des Wohnungseinbruchs', *Die Kriminalpolizei* 32(1): 13–16.

Sidebottom, A. and Wortley, R. (2016) 'Environmental Criminology', in A. R. Piquero (eds) *The Handbook of Criminological Theory*, Chichester: Wiley Blackwell, 156–81.

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(2): 259–74.

Stanley, J. (2014) 'Chicago Police "Heat List" Renews Old Fears about Government Flagging and Tagging', *ACLU*, 25 February. Online. Available: www.aclu.org/blog/privacy-technology/chicago-police-heat-list-renews-old-fears-about-government-flagging-and (accessed 30 November 2017).

Tenner, E. (1997) *Why Things Bite Back: Technology and the Revenge Effect*, London: Fourth Estate.

Townsley, M., Homel, R. and Chaseling, J. (2003) 'Infectious Burglaries: A Test of the Near Repeat Hypothesis', *British Journal of Criminology* 43(3): 615–33.

Winner, L. (1980) 'Do Artifacts Have Politics?', *Daedalus* 109(1): 121–36.