7 Infrastructure shortcuts

The private cloud infrastructure of data-driven policing and its political consequences

Daniel Marciniak

Introduction

A shift occurred during the coronavirus pandemic of 2020: many police forces in the United Kingdom moved their databases online to allow their officers to work from home during the consecutive lockdowns that were imposed. A company representative at a security exhibition in 2021 was cheerful about the future business opportunities this would open. She recounted an extraordinary shift over 18 months during which police went from being very nervous about every little bit of data in the cloud to allowing for the heart of their IT infrastructure – the records management system – to be accessible from anywhere. In fact, the two companies that have cornered 60–70% of the market with competition-limiting practices (Ofcom, 2023), Amazon Web Services (AWS) and Microsoft Azure, are expressly marketing their products to police forces worldwide (Kwet, 2020; AWS, 2023; Microsoft, 2023). What on the surface looks like a boring, mundane change that, at most, cybersecurity experts would be concerned about, may have far-reaching consequences for how police create knowledge and, based on this knowledge, how we will be policed in the future.

Stored on cloud services, police data becomes open to third-party add-on software that seeks to generate insights from this data, routinely analysing it and visualising the results. Amazon and Microsoft offer (two separate and incommensurable) "ecosystems" of second-tier companies that provide these add-ons which run on the same servers and can thus be easily "plugged into" the data. For example, Saadian's Prisoner Intelligence Notification Systems runs on AWS servers and is used by police forces across the UK to track releases from prison (AWS, 2023). Similarly, Microsoft's partners include a full range of big names in policing technology like Accenture, Axon, Genetec, Motorola, and NICE (Microsoft, 2023). A whole new market offers itself up to policing.

Drawing on Srnicek (2016) and Langley and Leyshon's (2017) concept of *platform capitalism*, some authors have referred to this change as the *platformization* of policing, describing a cloud-based infrastructure that integrates data streams from disparate sources, internal and external to policing, allowing new forms of analysis and prediction that are intended to shape

DOI: 10.4324/9781003412908-10

future police action (Egbert, 2019; Gates, 2019; Linder, 2019; Wilson, 2019). Platform capitalism, as Wilson (2021: 51) puts it, is "integrating policing into the circuits of the digital economy through intensive datafication". This chapter develops this perspective by examining police's dependency on a private provision of cloud infrastructure as an *infrastructure shortcut*: a way for police to receive advanced data analysis without the need for developing and maintaining underlying infrastructure. Crucially, this also entails a lack of detailed understanding of the functioning and control over the design of this infrastructure.

Much research has followed Amoore's (2018) call to shift focus from the material question of where "the cloud" is to examining the new epistemologies of automatic pattern and anomaly detection that emerge from cloud computing and related fields of big data, machine learning, and artificial intelligence. Instead, this chapter seeks to illuminate the *interrelation* of materiality and epistemology by asking what the consequences are of who owns and maintains the cloud infrastructure. The tools running on data platforms often seek to structure workflows and ultimately to automate the epistemic work of interpreting the data routinely produced by police – answering questions of which areas police should patrol, which incidents to investigate first, which officers to put under closer supervision, and so on. With commercial solutions, there is no public discussion of the purposes and mechanics of data use because they are often proprietary and outside the purview of democratic decision-making. Moreover, by outsourcing this epistemic work to private companies, thus rendering it an invisible infrastructure, police may be risking not only a technical but also an epistemic lock-in by giving up on their ability to reflect on and revise the epistemic work central to their operation.

The analysis in this chapter centres on the example of place-based predictive policing and is based on semi-structured interviews with 18 members of police forces in analyst or planning positions representing 11 police forces in the United Kingdom and 3 in the United States, 12 employees from five predictive policing companies, and observations made at six security trade shows in the US, the UK, and Germany. Predictive policing refers to the use of data analysis detecting patterns in crime data that are used to identify targets for police intervention. This can be the use of risk scores for prioritising individuals likely to (re-)offend or forecasting the location of crime events. In this chapter, the focus shall be on the latter. It adds to the growing body of research that has extensively dealt with unmasking the "objectivity" of place-based predictive policing, analysing it as a socio-technical assemblage and revealing the risk of biased feedback loops, as well as studying police officers' attitudes towards this technology and its influence on their decision-making (Benbouzid, 2019; Kaufmann, Egbert, and Leese, 2019; Ratcliffe, Taylor and Fisher, 2019; Shapiro, 2019; Egbert and Leese, 2020; Marda and Narayan, 2020; Sandhu and Fussey, 2020; Brayne, 2021; Duarte, 2021; Lally, 2021; Tulumello and Iapaolo, 2021; Waardenburg, Huysman and

Sergeeva, 2022). While predictive policing may have already reached the end of its popularity with some police forces in the UK and the US ending its use and the EU considering an all-out ban, it has been one of the first machine learning-based technologies implemented widely in policing, and the linkages between infrastructure work and political decision-making presented in this chapter are indicative for future data-driven technologies in policing.

The idea for place-based predictive policing has its origins in hotspot mapping, which gained particular popularity with the advent of computerised systems for recording and mapping crime and the management of patrol through the COMPSTAT process, in which mid-level officers are held accountable for the crime statistics within their areas of responsibility (La Vigne and Groff, 2001; Wilson, 2020). Crime is addressed from a rational choice perspective which imagines the offender as more likely to commit crime in a familiar environment – a perspective that Jeffrey Brantingham, one of the main proponents of predictive policing and co-founder of the company PredPol, describes using the analogy of the offender as forager (Brantingham and Tita, 2008; Maguire, 2018). Without further knowledge about the offender, recorded crime patterns become a proxy for this behaviour and areas with higher crime concentration become the problem that needs to be addressed. While there are approaches such as risk terrain modelling which attempt to solve the "problem" by changing the built environment, for example, by changing the lighting conditions in a high-crime area, the primary "solution" to crime patterns in predictive policing is deterrence achieved through the allocation of police patrols (Benbouzid, 2015; Eck and Clarke, 2019).[1] With the problem and its solution thus identified, the predictive problem essentially becomes a management problem of how to produce timely forecasts, distribute them to officers, and ensure that predicted areas are patrolled (Benbouzid, 2019).

The predictive policing software that addresses this management problem exists in a variety of institutional arrangements between police and the private sector including (a) standalone software running on police servers, (b) customisable data analysis employing generalist tools like SPSS Modeller, SAS, or visual programming tools in Microsoft Azure, and (c) dedicated predictive policing tools that run on cloud servers (regularly owned by Amazon or Microsoft). The latter arrangement will be the focus of this chapter.

This chapter contributes an insistence on the minutiae of infrastructure work in laying out a nuanced critique of the platformisation of policing and (well-intentioned) design decisions in the automation of police functions. The chapter begins with a discussion of infrastructure work in terms of setting up and maintaining technical infrastructure as well as designing a process that engages all levels of the police organisation. Having set out the basis for why (some) police forces have opted for commercial products, the chapter then analyses the setting of priority crimes and the issue of feedback loops as examples of the detailed political decision-making that goes into the

development of predictive policing. Finally, it critically discusses police agencies' dependence on private companies for their IT infrastructure.

Commercial infrastructure shortcut

As Star and Ruhleder (1996) have argued, infrastructure is fundamentally relational. While it is transparent to its users, it is the centre of activities for those who build and maintain it. The complexity and cost associated with this usually invisible infrastructure work form a central reason for police to outsource the production and maintenance of software and underlying hardware to private companies. The aim of this section is to provide insight into this complexity before the second part of this chapter explores how this outsourcing means that private companies gain considerable influence over political aspects of policing priorities.

Police data management systems have long been predicated on the logic of the archive; a record of information that is saved for an imagined future use (Derrida, 1995; Waterton, 2010). Police bureaucracies have been built around the archiving and retrieval of criminal records almost since their inception and, in the UK, challenges around territorial police forces recording crime data independently remain more than a century later (Thomas, 2007). These systems were designed to retrieve individual records one at a time. Thus, the underlying infrastructure is poorly adapted to the kinds of analysis required for predictive policing (or other forms of AI/machine learning for that matter). These require retrieving information from all files at the same time. Implementing predictive policing hence presents a major logistical challenge that further includes maintaining servers that are able to run the statistical models at regular intervals. These servers also need to allow for data entry and be able to display maps with predictions. This challenge can be difficult to meet for police forces, whether this is in getting the machines ready for the task or getting machines and humans to cooperate.

An example of this is a predictive policing implementation in West Yorkshire, UK, where technological "teething problems" with maps failing to update led to scepticism and minimal uptake (Hamlin, Ellinger, and Jones, 2019). Before it even gets this far, the technological requirements to regularly update complex statistical models can prove prohibitively expensive. This is why one of the interviewed analysts developing his own predictive models looked enviously towards the technology in the neighbouring police force:

> They were like a test force for the country. So they received quite a lot of investment from Microsoft and from IBM SPSS as well. And not just in terms of training and software but infrastructure: two 40 gigabyte servers to help process their information and stuff like that. So they can download their information every five minutes. We can do it [at] two in the morning.
>
> (UK Police Analyst)

It is this bridging of infrastructural problems by private companies that this chapter seeks to foreground.

Predictive policing is not a private sector innovation. Rather, it has emerged from the academic field of environmental criminology concerned with the spatial concentration of crime. One of the first implementations of the idea of focusing deterrence in specific places at specific times was an experimental study addressing near-repeat burglaries in Manchester (Wilson, 2020). As such, there are not many secrets around the way predictions are produced. One software developer even suggested that the company could make their prediction algorithms public without fearing for their market position as the main challenge would lie in providing the "plumbing" in the background (Software Developer). This section thus first describes the technical "plumbing" associated with maintaining and setting up the predictive policing infrastructure and then discusses the design of the underlying workflow that turns predictive policing from a research project into a product.

Infrastructure work

There are two main areas of infrastructure work that software companies do: maintaining and updating the code base and setting up infrastructure to take in data from new customers. This section describes the two in more detail and reflects on their role in privileging a centralised, commercial provision of the technical infrastructure required for predictive policing.

To begin with updates and maintenance: A software developer described the steps for a new feature update as the following: whenever there is a new feature that is added to the software, software developers first write the necessary code for a version of the software running on their local machines, the development environment. If everything seems to work, the changes move on to the release environment. This is an account with the cloud service provider that is not connected to any of the customers. Only once the updated software is running on these servers without issues, it is rolled out to operational servers, the staging environment. Testing the new features involves running a series of pre-programmed scripts that simulate a user to test comprehensively for errors (Software Developer). A similar approach is taken to check for security vulnerabilities: automated scripts ensure that different types of accounts (admins, analysts, data owners, data viewers) have access only according to set permissions (Software Developer).

There is thus a considerable amount of work that goes into ensuring that new features do not jeopardise the functioning and security of the system when they are rolled out. Quite opposite to the imagination of a fixed black box continuously transforming inputs into outputs, the software is subject to constant adaptation and change. As research on maintenance and repair has highlighted, it takes work to maintain the relations of socio-technical assemblages (Graham and Thrift, 2007; Denis and Pontille, 2019). Here, this applies both to the small adjustments of bug fixes as well as to larger

readjustments of what the software's role is (see the shift from crime prediction to patrol management discussed in the next section).

Police analysts usually have the skills to develop predictive models but are not trained software developers able to maintain everything from data intake to user interface. Without a dedicated team of software developers, it is nearly impossible for a single police force to carry out the work described above and maintain its own computer code. Maintenance work can thus form one of the in-roads for private companies to provide predictive policing solutions. Being part of a cloud infrastructure that allows these continuous changes at a distance further supports the common subscription-based business model for predictive policing.

This is not to say that companies do not struggle with some of the same challenges as police forces – as well as challenges that are unique to them. This is particularly the case for the second type of infrastructure work which relates to the initial setup of links between different elements of the predictive policing assemblage. A central challenge that affects both companies and police is the integration of data from different databases. For instance, one interviewee described how he and his colleagues had to write multiple computer scripts that would regularly copy data from various legacy systems designed without interoperability in mind into a more general database (US Police Head of Analysis). Similarly, companies have to figure out how to retrieve data from a variety of systems. As a data scientist complained, "each department has different CAS [crime administration system] and RMS [record management system] systems" (Data Scientist 2).

A challenge unique to companies is to then apply their general predictive model to data that is subject to a large variety in recording practices. For example, some police departments record an incident with a single time and date referring to when it is recorded, and others record it as a period within which the incident is thought to have occurred (Product Manager and Data Scientist). Examples like this, and more generally the availability of different variables, result in the need for predictive models tailored to each police force. Only once this initial setup is completed, the models become cogs in the bigger machinery of data retrieval, processing, and display.

Apart from these technical challenges, companies face a unique challenge in institutional hurdles as outsiders to police departments. Some police forces would not have the resources to provide a dedicated contact person, or policies on data security would create hurdles for connecting the police's data into the companies' software (Product Manager and Data Scientist). With security guarantees by the big cloud providers (Microsoft and Amazon both offer services tailored to governments) and the recent move to cloud storage to allow working from home during the Covid pandemic, these concerns for data safety and technical issues around interoperability of data storage are becoming less and less of a hurdle.

Putting the challenges of the initial setup aside, hosting the predictive tools on servers in the cloud has the advantage for companies that they can reuse

the same computer code for different customers, whereas police forces have to put things together from scratch. It is difficult to overstate the importance that cloud infrastructure plays in this. This is demonstrated by the case of one company that went from prediction software running on a desktop computer to a web-based interface, and most recently to a cloud-hosted solution. The Product Manager describes how crucial the move to a cloud-based service was for their business model:

> In the second phase of [the software], [its] version one. That was all built in a manner to be installed on a server at a police department's headquarters or in their IT … and so the price doesn't scale up and down very well because setting that up and getting it integrated and install is the same amount of work for a small police department as for a big department. So, when that was kind of ready, we had inelasticity of the price and then the economy wasn't doing well, so budgets were really tight and so we really didn't get a whole lot of traction on that.
>
> (Product Manager and Data Scientist)

With the software hosted in the cloud, smaller departments have access to an infrastructure that the company has built using government grants and investments from other customers when they would not have the budget to develop a predictive policing software themselves (Product Specialist 1). What predictive policing companies offer is the simplicity of boxes on a map accessible to all officers without needing to develop and maintain the infrastructure that automates prediction and delivery.

More generally, the increasing move to cloud services promises easier access to data for analysis rather than solely maintaining the chain of custody for the bureaucratic paper trails of policing. With the data already online, companies can attach their modes of analysis as add-ons. Companies take infrastructure problems that many police forces are ill-equipped to deal with, such as maintaining computer code and integrating data from proprietary databases, and they transform them into the forgotten, boring background of invisible infrastructure (Star, 1999).

Designing patrol management

Apart from the technical challenges described in the previous section, the development of predictive policing poses a design challenge: making the product enticing to a range of actors, or, to use Callon's (1984) phrase, *enrolling* them in the socio-technical assemblage of predictive policing (for a description of this assemblage see Egbert and Heimstädt in this volume). Companies have an institutional focus on making predictive policing work and can adjust their offerings through updates of software running in the cloud. In providing insight into some of the design processes, this section argues that companies employ these advantages to learn in an iterative process how to

enrol various agents from police officers and police management to databases and prediction algorithms.

Predictive policing trials are emblematic of the different lessons that police and companies can take from them. In the UK, there have been multiple trials of predictive policing funded with innovation funding from the Home Office. These trials, as one interlocutor observed, often serve the career of the officer organising them but seldom lead to a stable application and remain at a prototype stage (UK Police Head of Intelligence Analysis). Other trials fail when the money runs out that was used to finance additional patrol time, or they never manage to have enough data to produce predictions. Designing a complete product is also a challenge for the software companies, as one interviewee described,

> The forecasting aspect was like we were building what was available in the academic literature, but it didn't kind of fuse things together enough to actually make it a very operationally useful product […]. We had different features, like we had the [areas to focus on], we had the visualisation of past crimes, we had the near-repeat pattern zones. But it wasn't clear how that all came together to capture and secure workflow.
>
> (Product Manager and Data Scientist)

This highlights the importance of designing the whole workflow rather than just providing predictions. In contrast to police agencies, some companies have benefited from trial funding because it allowed them to refine their product in multiple stages. The outcome is a product that, as Benbouzid (2019) observes, not only provides a map of likely areas of crime but mainly enables the management of police patrols. Accordingly, PredPol has recently embraced patrol management in their rebrand to Geolitica as the product's main feature (PredPol, 2021). Managing patrols is no small feat: Manning (2008), for example, demonstrates the largely performative quality of crime mapping in the CompStat process, a precursor to predictive policing, and its failure in transforming existing patrol practices.

The police officers who are supposed to follow the computer's instructions on where to patrol are sceptics. As research by Sandhu and Fussey (2020) shows, officers question the superiority of the automated analysis over their own judgement and are concerned about biases in the data. Oftentimes, officers question the uniqueness of the insight provided by predictive policing. As one interviewee puts it, "No shit. We're going, 'Oh yeah, what a surprise'" (UK Detective Sergeant). Ratcliffe, Taylor, and Fisher (2019) encountered similar resistance in the Philadelphia predictive policing experiment. In a trial for West Yorkshire police, Hamlin, Ellinger and Jones (2019) found that it was difficult to convince officers of the software's effectiveness when the likelihood of encountering crime in a patrol zone was generally very low. As one of the sergeants they interviewed put it: "If you are wandering around and

nothing's happening, it's hard for people to see that they are doing a good job" (Hamlin, Ellinger and Jones, 2019: 478).

To successfully insert themselves in the patrol management process, the companies studied in this chapter appeal to both the patrol officers on the street and their managers in the back office. Addressing the perceived attack on officers' professional judgement, one strategy is to move predicted areas around so that they are not just those that officers would expect from their own experience:

> We generally have to walk a fine line between telling them things that they agree with and surprising them a little bit. Because we want them to buy into the prediction and believe it and, and say that, 'oh yeah, I, I agree with what it's predicting', but we also want to change it up a little bit so that they, they don't sit there and say like, 'well, this thing isn't telling me anything new'. So, it's kind of the balancing you have to strike.
>
> (Product Manager 1)

Another approach is to reintroduce choice in the form of choosing between multiple predicted areas and choosing what to do in that area. A product manager describes how this is done to give officers a sense of agency,

> We don't give them one box to go to, to sit in all the time. We give them a few boxes and […] we suggest tactics for them to try. And we rather than giving them one tactic, we've since developed the choice to decide what sort of tactic they want to try based on the situation or based on the timing or based on the type of crime. Whatever they think would be most effective. They can choose that. And I think some of that does drive some motivation or at least makes it less about like, "oh, I'm being told exactly what to do". And more about like, "oh, I have some agency in deciding what I can do".
>
> (Product Manager 1)

At the same time, predictive policing companies use GPS sensors from the devices that are used to display the maps to record officer movements and the time they spend in predicted areas (at times circumnavigating police unions' resistance to GPS trackers on police cars). They also provide a tool for officers to report what they do in a predicted area. All this information is then fed back to senior officers in the form of data visualisations "trying to provide agencies with better tools to manage their patrols" (Product Manager 2). This arrangement thus mobilises the authority of senior officers to supervise patrol officers and enables them to exercise control while simultaneously offering patrol officers a sense of professional independence. Evidently, there is more to predictive policing than boxes on a map. It is perhaps not surprising that the approach from some software engineers is this coupling of

workplace surveillance and gamification (for examples outside policing see Whitson, 2013).

Some of the predictive policing providers, like PredPol/Geolitica and Hunchlab/Shotspotter Missions, also offer senior officers the ability to manually assign areas for patrol, moving further away from an "objective" crime reduction tool to a management tool. All these design decisions catering to the requirements of patrol management, rather than solely the production of predictions and their display on maps, depend on further infrastructure in the form of features in the software, some of which require major changes in user interfaces and database models (Software Developer).

The use of a cloud infrastructure and building on experiences in multiple trials with multiple police forces allow companies to build software in an iterative process that not only predicts crime but also creates a "workflow" aligned with the organisational requirements of supervising police patrol. Whether for predictive policing discussed here or more generally for (automated) data analysis and visualisation, the two elements of maintaining technical infrastructure and designing workflows tilt adoption and development towards commercial solutions in the form of plug-ins to data hosted on servers belonging to AWS, Microsoft, or another cloud provider. Not only does this create a problematic oligopoly of cloud ecosystems (Ofcom, 2023), it also comes with the danger of technological lock-in. As the conflict between NYPD and Palantir around moving police data to a different service provided by IBM shows (Iliadis and Acker, 2022), switching providers can come with difficult questions around how to transport not only the raw data but also the insights that have been created in the past.

Deciding priorities

Perhaps oligopolies of cloud providers with significant market power and technological lock-ins are only a nuisance. After all, police forces, as discussed above, are already used to being stuck with legacy systems that do not interoperate and with what Hayes (2012) terms the surveillance–industrial complex, which includes revolving doors between industry and state agencies – not exactly a "healthy" form of a competitive economy. So, what is the concern? Reflecting on the initial wave of computer adoption in US policing in the 1960s, Kent Colton (1979) warned already four decades ago that "the computer may also serve to reinforce the status quo, to lock in and substantiate our present approach, and to indirectly countermand other innovation" (Colton, 1979: 19). The concern is that just as patrol cars have cemented a form of patrol that hinders engagement with people on the streets, policing software may have lasting effects on the way we are policed. Products like predictive policing have a different character from other products police agencies purchase, like cars, guns, and even record management systems. Because they seek to automate knowledge production, they influence not only *how* the police act but also *why* they act.

This section discusses two ways in which the use and design of predictive policing contain normative decisions around what policing should be: it first discusses the (at times only implicit) weighting of police priorities, before then engaging with design responses to the common criticism that predictive policing reinforces existing institutional biases. In outlining the design choices of developers, the argument of this section is not to say that they make poor or dangerous decisions that worsen policing. Quite the opposite, developers are aware of the pitfalls of predictive policing and, with possibly limited success, seek to mitigate these. What this section does problematise is the fact that political decisions about the purpose of policing in terms of how it operates (patrol for deterrence) and what it prioritises (predictable types of crime) become fixed in products without ever being subject to wider political deliberation. Moreover, outlining the complexity of producing crime prediction highlights how the automation aspect of predictive policing outsources and partially replaces the roles of analysts and their intimate familiarity with crime patterns, removing core knowledge required to make strategic decisions. A police force that has automated its crime analysis risks losing the capability to rethink its approach to crime. In this, predictive policing is not much different from the larger trends of governments outsourcing expertise to consulting firms, as described by Mazzucato and Collington (2023).

Companies are involved in highly political decisions around what policing is today. This is particularly true in a context in which arguments from police abolitionists and the "defund the police" movement reverberate internationally (Vitale, 2017; Lum, Koper, and Wu, 2021). The question of how to allocate police resources to different tasks given a multitude of, at times contradictory, expectations from stakeholders like different parts of the community, local politicians, or oversight bodies is part of the day-to-day work in policing. Automating parts of this allocation then brings these tensions to the fore. This is reflected in an interview with a UK police officer in a planning function who was enticed by the idea of prioritising police work by harm as reflected in the Cambridge Harm Index, a simple measure reflecting the sentence length associated with a crime. During the interview, he quickly realised that other aspects such as community perception of crime, confidence in the police, and urgency of incidents would not be adequately reflected in the score. The "wicked problem" (Rittel and Webber, 1973) of policing does not have a singular problem description. There is a multiplicity of goals and therefore no single correct measure: "What is the goal? What are you trying to achieve? Everybody has a different view" (UK Detective Sergeant).

The core idea for predictive policing is that the purpose of police patrol, a central policing task, is to deter crime through police presence. Delivering the right "dosage" at the right time would maximise deterrence and prevent crime. Just as in the case of the Cambridge Harm Index above, this means prioritising some things over others: it assumes that the use of police time for patrol is an adequate measure to address crime and superior to other strategies. Moreover, the spatial location of patrols is optimised for deterrence

rather than, for example, speed of response to emergency calls or fostering community relations. It is optimised for crime that is recorded by police, and it is optimised for crime that occurs in spatio-temporal clusters. When no explicit decision is made, volume and predictability of recorded crime determine priorities – the "politics of patterns", as Kaufmann,Egbert, and Leese (2019) term it, comes into play. However, it would be simplistic to say that the "objectivity" of patterns alone always trumps other concerns. Reflecting the balancing act of prioritisation sketched out above, some companies provide police forces with the option to rank crime types according to their own priorities and assign a likelihood that patrol would affect it (a strategy that surely helps to enrol police managers).

Explicitly or implicitly, decided by companies or police managers, with or without preconfigured values – predictive policing companies influence police priorities. Should this process be a discussion behind closed doors between companies and the police? How meaningful is ranking crime types without an understanding of the underlying data on the one hand and an overview of alternative modes of policing on the other? With technologies like predictive policing, the character of policing as a practice and its accountability to a democratic process are at stake. This is both an opportunity as it can trigger a discussion around priorities in police resource allocation, and a risk when this discussion does not happen because of black-boxed, proprietary software.

Another example of the politics embedded in predictive policing is the issue of feedback loops. The main criticism of predictive policing in academic and public discourse is that, since it is based on police records, it will only reinforce pre-existing patterns of police presence in overpoliced communities and, to make things worse, add a sheen of objectivity that could lead officers to be even more aggressive in their actions (see also Narayan in this volume). This argument can, for example, be found in O'Neill's (2016) popular book *Weapons of Math Destruction* and relates to a growing body of work concerned about discrimination facilitated and amplified by algorithms (Gandy, 1993; Eubanks, 2018; Noble, 2018; Benjamin, 2019). Perhaps the most convincing evidence for the possibility of feedback loops has been provided by Lum and Isaac (2016), who replicated PredPol's algorithm. Applied to drug crimes – typically detected by the police rather than reported by the public – they found a feedback loop further concentrating existing police activity. Predictive policing companies are, of course, aware of this criticism, and PredPol has sought to dispel it with a research paper published by its founders that claims patrol following its predictions would not lead to more biased arrests (Brantingham, 2018; Brantingham, Valasik, and Mohler, 2018).

Independent of whether the predictions affect officer behaviour, there are design decisions that interviewees highlight as mitigation for a feedback loop: First, they suggest the use of call-for-service data rather than crime records for types of crimes that are often recorded through officer-initiated contacts such as traffic stops.

> We like to have a focus on only dealing with, citizen-initiated calls […]. So reports that ended up in the [record management] system that are citizen-initiated types of calls and work towards having less and less or no officer-initiated types of calls.
>
> (Data Scientist 2)

Without officer-initiated contacts in the data, the issue of a feedback loop is largely solved. It brings, however, a new challenge in that one incident may relate to multiple calls-for-service, and the difficulty lies in filtering these out. As the data scientist describes in the example of gunshots, the data retains some messiness as it has not been pre-filtered by the police bureaucracy.

> However, we have to deal with duplicates. A lot of times, especially with gunshots, you have to deal with error in these calls, wrong calls, you know, fake calls, […]. […] there's this sort of, the messiness of that data.
>
> (Data Scientist 2)

Second, following ideas from risk terrain modelling (Caplan and Kennedy, 2011), not all predictor variables need to be from police data; they can also be information about the night-time economy, lighting conditions, footfall, weather, and many more. The developers argued that including these provides further protection from biases in police data (Product Manager 2 and Data Scientist 2). As an added benefit, the Data Scientist at another company argued that it provides more long-term reliability to the models, making them less susceptible to changes in patrol strategies:

> [The] more the model uses things that are not being affected by the use of the model, I think the better, you know, accuracy will remain and the kind of validity of the actions.
>
> (Product Manager and Data Scientist)

Third, one company argued that implementing some randomisation around which of the predicted areas are shown to officers would further help in preventing over-policing. This is simultaneously intended to engage officers more and make following the predictions more interesting, as discussed above.

Notwithstanding these efforts: however advanced the modelling, however carefully selected the variables, area-based predictive policing remains always associated with patrol and all its problems. As Aaron Shapiro puts it,

> Ultimately, [predictive policing] is incapable of resolving two fundamentally incommensurate but concurrent functions of the police patrol. On one hand is a view of police patrols as distributing public safety as a common good […]. On the other is the view from marginalized

> communities, who experience the patrol as an enactment of uneven geographies of legitimacy and authority, risk and danger, harm and abuse.
>
> *(Shapiro, 2019: 469)*

This fundamental contradiction seems to be behind some of the doubts and disillusionment of employees who were not quite sure if the software they were producing was contributing to the public good. This shines through in the statement of one of the Product Specialists:

> Although our product is great because we are moving people around and we're trying to like stop saturation and all of that, they're like, we're changing that up. It doesn't mean that a little kid might not get shot in the box, like, you know, at some point in time. So it's, it's hard.
>
> (Product Specialist 2)

A Product Specialist and a Software Developer expressed their hope that the tracking data gathered through their software could be used to identify factors such as the number and type of calls-for-service answered by an officer or their driving speed to predict and prevent mistakes and shooting incidents caused by high levels of pressure and emotional stress. Yet, these kinds of questions are not the main interest of the customer; "the focus tends to be on crime reduction" (Product Manager 2). Addressing the problems of police patrol is difficult and not a priority, as this Product Manager explained,

> The harm caused by police events […] is probably the less documented or it's not as easy to measure in some way. If we, you know, potentially if you look at survey data of the community in terms of what is your general perception of the police, how has that changed over time in some way? Or a number of looking at the counts of incidents where the police are, you can look at police shootings, you can look at like kind of violent interactions or sort of dangerous interactions with the police. […] We haven't done anything like that yet. It's just kinda been like, 'what's the most, what's the easiest, the lowest hanging fruit', essentially, like in terms of determining effectiveness. Well, we can look at, do we have a reduction in crime? Well, yes, we did. That's a good thing. That's kind of what the police departments are focused on.
>
> (Product Manager 1)

Thus, even when companies are well-intentioned and have ideas for improving policing, their customers, police departments, seem to show little interest in a product that provides more than the promise of crime reduction. The control that predictive policing companies have over police work is either opaquely produced through the way they select and weight variables in their statistical models or is closely aligned with the management goal of

controlling patrol. Predictive policing reduces the multiplicity of goals associated with police patrol (deterrence, proximity to incidents for emergency response, building of community relations, and more) to the goal of deterring street crime through police presence and fixes this strategy in software design. Simultaneously, it automates the processing and interpretation of crime data and thereby poses a risk for police to lose some of their intimate knowledge of their data and an understanding of crime patterns – a knowledge lock-in in addition to the technology lock-in discussed earlier.

Discussion and conclusions

The literature on area-based predictive policing has extensively dealt with unpacking the black box, examining in detail its various elements, and highlighting the risks of bias and discrimination from amplifying existing problematic police practices (Egbert and Leese, 2020; Brayne, 2021). What this chapter contributes is a critical discussion of the role of private companies in this assemblage. Drawing on ideas from science and technology studies literature on infrastructure, innovation, maintenance, and repair (Star, 1999; Graham and Thrift, 2007; Denis and Pontille, 2019), it has highlighted the often invisible maintenance work and iterative change that underpins predictive policing. It has argued that the ability to provide this infrastructure work at a distance through cloud services can privilege private companies when police departments do not have the technical capabilities for this work. Companies can profit from economies of scale and build and maintain infrastructure developed with innovation funding from the state because providing their services through the cloud means they can deal with most of the infrastructure in one place. This also allows them to add extra features to their software that make predictive policing more amenable to patrol management processes that tie into the authority of senior officers by tracking officers' actions and whereabouts. While larger police forces might have the capacity to hire software developers to maintain a similar infrastructure, many police forces do not have the necessary resources.

The backstage, technical work is not just innocent "plumbing" but, as the second part of this chapter has demonstrated, means that private companies become entangled in the politics of policing. This is not to say that the interviewees were not genuinely concerned about the consequences of their software and tried to address common criticisms of predictive policing. But this chapter questions whether these deliberations should be had in opaque interactions between police and companies shielded by claims to intellectual property rights which has been widely criticised (Joh, 2016; Ferguson, 2017; Raso *et al.*, 2018). Political decisions on police priorities become fixed in the infrastructure of predictive policing: the imagined purpose of patrol is deterrence, crime that is predictable because of its spatio-temporal concentration becomes a priority, and so on. It replaces a multifaceted analysis of crime patterns that asks why crime happens with an automated conclusion informed

by rational choice theory that it must be the lack of "capable guardians". One interviewee criticised the superficiality of this form of analysis:

> So, it's all very well, if you send a cop into that red square, red grid at that time and the evidence base shows a five percent reduction; that's not a root cause, dealing with a root cause, it's kind of like being a ready mixed plaster on top.
>
> (UK Police Business Intelligence Manager)

Fixing priorities in infrastructure limits the ability to shift priorities in accordance with the multiplicity of values that are negotiated in police resource allocation – driven, among other factors, by communities, local politics, the news cycle, and shifts in legislation. Moreover, automating the epistemic work of resource allocation means that police departments outsource a central epistemic function of analysing trends and patterns in crime. Without the institutional knowledge of regular engagement with crime numbers, alternative ways of interpreting crime patterns cannot develop.

This chapter is thus a call not to separate the political economy of "boring" infrastructure from the exciting shifts in knowledge production afforded by new technologies variously referred to as AI, machine learning, and big data. The question of who maintains infrastructure has consequences for who makes the political decisions about what this infrastructure does and will do, as highlighted in this chapter. Focusing on infrastructure should further open the door to questions around whether this technology is required considering the natural resources involved in keeping it running (Hogan, 2018; Crawford, 2021; Jue, 2021). Both the market for cloud infrastructure and the market for surveillance technologies are driven by the availability of capacities that are in search of customers. According to Jue (2021), the "data centre industrial complex" perpetuates itself by promoting increasing uses of data. Similarly, Hayes (2012) describes the "surveillance industrial complex" as a market in which lobbyists push the threats that their products, often developed with government funding, are supposed to address. Huang and Tsai (2022) demonstrate in the case of China how capitalist incentives can easily lead to "over-surveillance" with technological capacities exceeding expectations set out in state policy. There is thus a dual concern around, on the one hand, the technological solutionism, as Morozov (2013) calls it, of companies addressing our social problems instead of democratic politics, and, on the other hand, capitalist incentives driving some of this decision-making.

When companies provide the infrastructure for police management and, in some cases, the storage and processing of all data held by police, police agencies become dependent on these companies and are locked in technologically and epistemologically. Certainly, the New York police department's legal battle with Palantir over facilitating the transfer of results from past data analysis to their new provider, IBM, serves as a warning of the kinds of lock-in police forces can be faced with when committing to cloud-based products

(Hockett and Price, 2017). Moreover, while the cost for these systems is not always as egregiously high as news reports make it seem ($35,000–$50,000 for HunchLab and $200,000 for PredPol (Shapiro, 2019: 462), but $3.5 million for Palantir (Hockett and Price, 2017)), these costs are charged annually. Depending on the type of arrangement – analytical tools used by police but hosted in the cloud or analysis provided and automated by companies and hosted on cloud platforms – some share of this is paid to large cloud providers such as Amazon AWS and Microsoft Azure who have simultaneously cornered the market for storing government data online. So far, the commercial provision of cloud infrastructure has gone unquestioned, but as legislation is just catching up to the problem of bias in predictive policing, it is perhaps only a matter of time before we start discussing open-source government software and ways of limiting the environmental footprint of data analysis.

So, given the costs, the contribution to an oligopoly of cloud service providers (Ofcom, 2023), and the opacity of political decisions embedded in the software design, what are the alternatives? As one interviewee from a software company suggests, a product that supposedly has such a public benefit should perhaps not be provided by a private company:

> I have some natural scepticism about [...] companies who are trying to do public benefit and make money doing it. Actually, I feel like anything that has any sufficiently broad public benefit should be regulated as a public utility. And if predictive services have this huge public benefit, then predictive services should be like regulated as a public utility and possibly socialised.
>
> (Software Developer)

As stated in the introduction, predictive policing software is produced in a variety of institutional arrangements, not all of which involve private companies. Large police forces and nationwide efforts can have the technical resources to shoulder the required infrastructure work. An example of this is the development of the National Data Analytics Solution at West Midlands Police, funded with £5 million innovation funding from the Home Office. This project includes an ethics panel consisting of local stakeholders and subject matter experts that publishes regular reports on its work (Oswald, 2022). Public scrutiny is involved from the very beginning of the development process, and the software is developed in the direction of a public purpose rather than with the perspective of making a product that sells. Even if not necessarily a radical approach, this demonstrates the possibility of alternative institutional arrangements.

With public pushback, limited evidence of effectiveness, and the European Union planning an outright ban on predictive policing, this technology may already be on its way out. But the issues discussed in this chapter apply more widely to attempts at outsourcing knowledge production in policing. The technology market for police is awash with data visualisation dashboards,

automatic resource optimisation, and software that enables investigators to identify leads in unstructured data. Microsoft and Amazon advertise their cloud services to police and the wider intelligence and defence sector as secure "eco-systems" in which companies can offer software solutions as plug-ins. Examples in policing are Accenture's Intelligent Public Safety Platform running on Amazon's AWS servers, and Motorola Command Central and Genetec Citigraf running on Microsoft's Azure servers. All of these products contain assumptions about how security services should operate and automate knowledge production, thereby closing off other ways of knowing.

There are fundamental questions about the role of policing that are raised by the need to distribute limited resources, and any attempt at automating these prioritisations shines a light on their complexity. Partial solutions like predictive policing have become viable ways of allocating resources mainly because they attempt to solve the problem of turning patrol allocation into a manageable process, what Sandhu and Fussey (2020) have termed the *uberization of policing*. But the time spent on patrol could be used differently. Particularly with voices from police abolitionists becoming louder, there is a need to rethink what police do, and this should not be decided behind the closed doors of private companies.

Note

1 Note that this epistemology does not include addressing social factors like inequality (see also Narayan, this volume).

References

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

AWS (2023) 'AWS for the UK Justice and Public Safety, Amazon Web Services, Inc'. Available at: https://aws.amazon.com/government-education/worldwide/uk/justice-and-public-safety/ (Accessed: 19 June 2023).

Benbouzid, B. (2015) 'From Situational Crime Prevention to Predictive Policing. Sociology of an Ignored Controversy', *Champ pénal/Penal field* [Preprint], (Vol. XII). https://doi.org/10.4000/champpenal.9066.

Benbouzid, B. (2019) 'To Predict and to Manage. Predictive Policing in the United States', *Big Data & Society*, 6(1), 1–13.

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press.

Brantingham, P.J. (2018) 'The Logic of Data Bias and Its Impact on Place-Based Predictive Policing', *Ohio State Journal of Criminal Law*, 15(2), 473–486.

Brantingham, P.J. and Tita, G. (2008) 'Offender Mobility and Crime Pattern Formation from First Principles', in L. Liu and J. Eck (eds) *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*. Hershey PA: Information Science Reference, 193–208.

Brantingham, P.J., Valasik, M. and Mohler, G.O. (2018) 'Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial', *Statistics and Public Policy*, 5(1), 1–6.

Brayne, S. (2021) *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York, NY: Oxford University Press.
Callon, M. (1984) 'Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay', *The Sociological Review*, 32, 196–233.
Caplan, J.M. and Kennedy, L.W. (2011) *Risk Terrain Modeling Compendium*. Newark, NJ: Rutgers Center on Public Security.
Colton, K.W. (1979) 'The Impact and Use of Computer Technology by the Police', *Communications of the ACM*, 22(1), 10–20.
Crawford, K. (2021) *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press.
Denis, J. and Pontille, D. (2019) 'Why do Maintenance and Repair Matter?', in A. Blok, I. Farías, and C. Roberts (eds) *The Routledge Companion to Actor-Network Theory*. Abingdon; New York: Routledge, 283–293.
Derrida, J. (1995) 'Archive Fever: A Freudian Impression', *Diacritics*. Translated by E. Prenowitz, 25(2), 9.
Duarte, D.E. (2021) 'The Making of Crime Predictions: Sociotechnical Assemblages and the Controversies of Governing Future Crime', *Surveillance & Society*, 19(2), 199–215.
Eck, J.E. and Clarke, R.V. (2019) 'Situational Crime Prevention: Theory, Practice and Evidence', in M.D. Krohn et al. (eds) *Handbook on Crime and Deviance*. Cham: Springer International Publishing (Handbooks of Sociology and Social Research), 355–376.
Egbert, S. (2019) 'Predictive Policing and the Platformization of Police Work', *Surveillance & Society*, 17(1/2), 83–88.
Egbert, S. and Leese, M. (2020) *Criminal Futures: Predictive Policing and Everyday Police Work*. Abingdon; New York: Routledge.
Eubanks, V. (2018) *Automating Inequality*. New York, NY: St Martin's Press.
Ferguson, A.G. (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York, NY: New York University Press.
Gandy, O.H. (1993) *The Panoptic Sort. A Political Economy of Personal Information*. Boulder, CO: Westview.
Gates, K. (2019) 'Policing as Digital Platform', *Surveillance & Society*, 17(1/2), 63–68.
Graham, S. and Thrift, N. (2007) 'Out of Order: Understanding Repair and Maintenance', *Theory, Culture & Society*, 24(3), 1–25.
Hamlin, R.G., Ellinger, A.D. and Jones, J. (eds) (2019) *Evidence-Based Initiatives for Organizational Change and Development:* IGI Global (Advances in Business Strategy and Competitive Advantage). Available at: https://doi.org/10.4018/978-1-5225-6155-2.
Hayes, B. (2012) 'The Surveillance-industrial Complex', in K. Ball, K. Haggerty, and D. Lyon (eds.) *Routledge Handbook of Surveillance Studies*. Hoboken: Taylor & Francis (Routledge International Handbooks), 167–175.
Hockett, E. and Price, M. (2017) 'Palantir Contract Dispute Exposes NYPD's Lack of Transparency', *Just Security*, 20 July. Available at: https://www.justsecurity.org/43397/palantir-contract-dispute-exposes-nypds-lack-transparency/ (Accessed: 24 November 2021).
Hogan, M. (2018) 'Big Data Ecologies. Landscapes of Political Action', *Ephemera. Theory & Politics in Organization*, 18(3), 631–657.
Huang, J. and Tsai, K.S. (2022) 'Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China', *The China Journal*, 88, 2–28.
Iliadis, A. and Acker, A. (2022) 'The Seer and the Seen: Surveying Palantir's Surveillance Platform', *The Information Society*, 38(5), 334–363.

Joh, E.E. (2016) 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing', *Harvard Law & Policy Review*, 10, 15–42.
Jue, M. (2021) 'The Data Centre Industrial Complex', in M. Jue and R. Ruiz (eds.) *Saturation: An Elemental Politics*. Durham: Duke University Press, 283–305.
Kaufmann, M., Egbert, S. and Leese, M. (2019) 'Predictive Policing and the Politics of Patterns', *The British Journal of Criminology*, 59(3), 674–692.
Kwet, M. (2020) 'The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud, The Intercept'. Available at: https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition/ (Accessed: 19 June 2023).
La Vigne, N.G. and Groff, E.R. (2001) 'The Evolution of Crime Mapping in the United States. From the Descriptive to the Analytic', in A. Hirschfield and K. Bowers (eds.) *Mapping and Analysing Crime Data: Lessons from Research and Practice*. London: Taylor & Francis, 203–221.
Lally, N. (2021) '"It Makes Almost no Difference Which Algorithm You Use": On the Modularity of Predictive Policing', *Urban Geography*, 43(9), 1437–1455.
Langley, P. and Leyshon, A. (2017) 'Platform Capitalism: The Intermediation and Capitalization of Digital Economic Circulation', *Finance and Society*, 3(1), 11–31.
Linder, T. (2019) 'Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service', *Surveillance & Society*, 17(1/2), 76–82.
Lum, C., Koper, C.S. and Wu, X. (2021) 'Can We Really Defund the Police? A Nine-Agency Study of Police Response to Calls for Service', *Police Quarterly*, 25(3), 255–280.
Lum, K. and Isaac, W. (2016) 'To Predict and Serve?', *Significance*, 13(5), 14–19.
Maguire, M. (2018) 'Policing Future Crimes', in M. Maguire, U. Rao, and N. Zurawski (eds.) *Bodies as Evidence: Security, Knowledge, and Power*. Durham: Duke University Press, 137–158.
Manning, P.K. (2008) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press (New perspectives in crime, deviance, and law series).
Marda, V. and Narayan, S. (2020) 'Data in New Delhi's Predictive Policing System', in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. New York, NY: Association for Computing Machinery (FAT* '20), 317–324.
Mazzucato, M. and Collington, R. (2023) *The Big Con: How the Consulting Industry Weakens our Businesses, Infantilizes our Governments and Warps our Economies*. London: Allen Lane.
Microsoft (2023) 'Public Safety and Justice Solutions'. Available at: https://www.microsoft.com/en-gb/industry/government/public-safety-and-justice (Accessed: 19 June 2023).
Morozov, E. (2013) *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York, NY: PublicAffairs.
Noble, S.U. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: Combined Academic Publ.
Ofcom (2023) 'Ofcom Proposes to Refer UK Cloud Market for Investigation', *Ofcom*. Available at: https://www.ofcom.org.uk/news-centre/2023/ofcom-proposes-to-refer-uk-cloud-market-for-investigation (Accessed: 13 June 2023).
O'Neil, C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. London: Allen Lane.
Oswald, M. (2022) 'A Three-pillar Approach to Achieving Trustworthy and Accountable Use of AI and Emerging Technology in Policing in England and Wales: Lessons from the West Midlands Data Ethics Model', *European Journal of Law and Technology*, 13(1), 1–27.

PredPol (2021) 'Geolitica: A New Name, A New Focus', *Predictive Policing Blog*, 2 March. Available at: https://blog.predpol.com/geolitica-a-new-name-a-new-focus (Accessed: 18 May 2022).
Raso, F. *et al.* (2018) *Artificial Intelligence & Human Rights: Opportunities & Risks*. Berkman Klein Center for Internet & Society. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:38021439 (Accessed: 11 February 2020).
Ratcliffe, J.H., Taylor, R.B. and Fisher, R. (2019) 'Conflicts and Congruencies between Predictive Policing and the Patrol Officer's Craft', *Policing and Society*, 30(6), 639–655.
Rittel, H.W.J. and Webber, M.M. (1973) 'Dilemmas in a General Theory of Planning', *Policy Sciences*, 4, 155–169.
Sandhu, A. and Fussey, P. (2020) 'The "Uberization of Policing"? How Police Negotiate and Operationalise Predictive Policing Technology', *Policing and Society*, 31(1), 66–81.
Shapiro, A. (2019) 'Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing', *Surveillance & Society*, 17(3/4), 456–472.
Srnicek, N. (2016) *Platform Capitalism*. Cambridge, UK; Malden, MA: Polity Press.
Star, S.L. (1999) 'The Ethnography of Infrastructure', *American Behavioral Scientist*, 43(3), 377–391.
Star, S.L. and Ruhleder, K. (1996) 'Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces', *Information Systems Research*, 7(1), 25.
Thomas, T. (2007) *Criminal Records*. London: Palgrave Macmillan UK.
Tulumello, S. and Iapaolo, F. (2021) 'Policing the Future, Disrupting Urban Policy Today. Predictive Policing, Smart City, and Urban Policy in Memphis (TN)', *Urban Geography*, 43(3), 448–469.
Vitale, A.S. (2017) *The End of Policing*. London: Verso Books.
Waardenburg, L., Huysman, M. and Sergeeva, A.V. (2022) 'In the Land of the Blind, the One-Eyed Man Is King: Knowledge Brokerage in the Age of Learning Algorithms', *Organization Science*, 33(1), 59–82.
Waterton, C. (2010) 'Experimenting with the Archive: STS-ers As Analysts and Co-constructors of Databases and Other Archival Forms', *Science, Technology, & Human Values*, 35(5), 645–676.
Whitson, J.R. (2013) 'Gaming the Quantified Self', *Surveillance & Society*, 11(1/2), 163–176.
Wilson, D. (2019) 'Platform Policing and the Real-Time Cop', *Surveillance & Society*, 17(1/2), 69–75.
Wilson, D. (2020) 'Predictive Policing Management: A Brief History of Patrol Automation', *New Formations: A Journal of Culture/Theory/Politics*, 98(1), 139–155.
Wilson, D. (2021) 'The New Platform Policing', in A. Završnik and V. Badalič (eds.) *Automating Crime Prevention, Surveillance, and Military Operations*. Cham: Springer International Publishing, 47–68.