Technology and Agency in International Relations

Edited by Marijn Hoijtink and Matthias Leese

First published 2019

ISBN: 978-1-138-61539-7 (hbk)
ISBN: 978-0-429-46314-3 (ebk)

Chapter 7

Who connects the dots?

Agents and agency in predictive policing

Mareile Kaufmann

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

7 Who connects the dots?

Agents and agency in predictive policing

Mareile Kaufmann

Who acts? A journey to the center of humanities

Singularity (Kurzweil, 2005), tech addiction (Kleinman, 2015), fake news (Tufekci, 2018), echo chambers (Barberá et al., 2015), algorithmic bias (Miller, 2015), superintelligence (Bostrom, 2014); as different as they seem at first, these are some of the many signal words in the language of popular science literature and tech-news that express that technology is no longer just a means to an end. Technology is not simply a material solution designed by humans for problems identified by humans, but it is increasingly discussed as matter that matters. The fact that digital technology is leaving its traces on human behavior and social life is no longer an insight highlighted by intellectual niches (cf. early writings on technology and society by MacKenzie and Wajcman, 1985; Bijker et al., 1987). The above concepts illustrate that the discussion of technology's intended and unintended workings in society has made its way into mainstream news coverage, political debate, and dedicated research projects. Such a focus on the way in which technology changes society implies an appreciation of technology and the idea that technology itself has risen to be an important actor in most of today's settings, whether in news reporting, crime control, or nature conservation.

Though, not everyone who writes about, studies, or deals with technology in nature and culture explicitly acknowledges the character of technology's agency. In fact, most commentators stick to the more careful vocabulary of technology's effects or its consequences for society, which also chimes with the attempt to find solutions for related challenges within technology itself. This is one of the reasons why a more profound engagement with the matter of technology, the way in which we understand it, and the role it plays within social, cultural, and natural settings is due. In this chapter, I want to draw attention to the collaborative processes and the many kinds of agencies involved in predictive analytics, more specifically predictive policing. Based on an empirical study of seven prediction software models and 11 interviews[1] with experts, police staff, software developers, and programmers,[2] I want to sketch out an answer to the question: who connects the dots in technology-supported predictive policing? Even though the sources of my empirical study, i.e. informants and actual software models, vary in terms of orientation and national settings, the questions and issues that emerge when they collaborate, build, and implement prediction algorithms for policing are comparable. At a more general level, I want to explore how agency comes about and can be conceptualized, especially in contexts in which technology moves center stage.

The context in which I look at these trends appears to be a rather localized one: in predictive policing, officers use data-driven analyses to prioritize crimes, hotspots, and offender groups in their districts. Policing with crime maps may be nothing new (Chamard, 2006), but it is a field subject to rapid innovation as software begins to manage the various aspects of policing and algorithms co-produce the actual predictions (Chan, 2003; Crawford, 2006). Despite the outspoken focus on the local (the development of prediction algorithms for crime situations in specific cities is a case in point), the more overarching, international dimensions of these practices are evident. Predictive policing software stands for a shift from after-the-fact to rule-based law enforcement (Hildebrandt, 2016b) that prioritizes pattern detection as a mode of understanding the world (Kaufmann, 2018). Policing software and crime prediction algorithms contribute to the making of profiles and based on that, they produce “digital prophecies” (Esposito, 2013) or automated recommendations. The automation of recommendations, in turn, has begun to re-determine global fields as diverse as media usage, commercial practices, and political decision-making. In that sense, predictive policing illustrates one aspect of a development that Sheptycki (2007: 391) already recognized in 2007, namely that “issues (…) of crime control have become central to the transnational condition.” Or, to put it differently, the automation of control that found its way into police practice is not so different from control technologies in other societal areas. Further, predictive policing is an instance of a more global trend towards private (and increasingly digital) security activities that cut across disciplines as different as criminology and International Relations (IR) (Abrahamsen and Williams, 2010: 12f.). Especially Research in the field of security, so some scholars argue, would profit from a more “in-depth conversation between International Relations (IR) and criminology” to better grasp differentiated “practices of (in)security (…) that are nevertheless connected along a Mobius strip” (Bigo, 2016: 1068). This interdisciplinary perspective is indeed the vantage point for this article. Most importantly, the case of predictive policing software exemplifies how human and non-human factors and forms of arguing collaborate in the process of decision-making. As such, the study of these technologies places emphasis on the very local and specific relations that we need to analyze in order to conceptualize the agency of technology and understand the more global trends of algorithmic security at work.

Conceptualizing the role of technological agency is not a simple task. Some have claimed that it leads us to nothing less than questions about life and death. Intelligent technologies, in particular, make us (re-)consider whether they eventually emancipate us from our bodies, our minds, our decision-making, or from biology altogether (cf. O'Connell, 2017). One does not have to follow new materialist perspectives all the way to the transhumanist acme (that is the deliverance from our bodies and the uploading of our minds into machines) to theorize the relationship between technology and society, politics, and IR. Yet, the question as to whether technology has agency will at least prompt us to re-think the neat world of binary categories (for example of structure vs. agency). It blurs the boundaries between matter and that which it represents, and it moves us from readily available and generated matter to generative and creative matter (van der Tuin and Dolphijn, 2010). Ultimately, technological agency and its related premises de-center human cognition. Drawing the focus away from anthropogenic agency does shake a few foundations of the humanities. It challenges our understandings of sociality and the political. If matter can be an agent, then technology is not a static object or a mere means in the hands of humans, but processual in nature. Some new materialists would claim that matter has self-organizing capacities (van der Tuin and Dolphijn, 2010) – an assumption that is unexpectedly reflected in public policy, for example in the European Network and Information Security Agency's (ENISA) portrayal of the Internet as an "interconnection ecosystem" (ENISA, 2011). Understood as an active force, matter is not only sculpted by, but also co-productive in conditioning and enabling social worlds, human life, and experience. As a result of its formative impetus (van der Tuin and Dolphijn, 2010), matter or technology would then be part of shaping nature and culture, the social and the political. Such an analytical starting point also requires a specific set of methodological commitments.

Studying the life of technologies

To study the everyday life of objects as well as the social and political dimensions of technology requires a view that is broader and more transversal than a sole view on the object itself. Studying agency means studying transformation and changes, emergences and development. Such a dynamism is difficult to capture without either focusing on the genealogy of the object or on the web of relations in which it is situated. In the following, I will present a few central approaches and methodologies to trace non-human agency.

The agency of technologies can be studied by using a concrete object, for example a specific digital technology, as a conceptual starting point to *venture into its surroundings* and trace the networks it is situated in. Already in the 1950s and 1960s, Gibson (1966) suggested that objects and the way in which they are perceived, afford specific actions over others. According to his theory of affordances, the shape, or *Gestalt* of objects, gives opportunities to perform some actions with them, but not others, which eventually grants them a certain ability to act.

Much later, Voelkner (2013) offers a slightly different perspective on using the actual object as a starting point to explore its agency: she describes how objects and the many dimensions, decisions, and developments they incorporate can "give form" to a phenomenon. This perspective is loosely based on new materialist ideas: objects not only capture the politics, history, and the many representations ascribed to it, but they do so in a dynamic way. Objects are generative of meaning and representation (van der Tuin and Dolphijn, 2010). Not only do they generate meaning constantly, but Bennett (2010) suggests that objects (in our case digital technologies), actually act quite concretely: they shut down, shape, initiate, burn etc. Objects, she deduces, have constructive and destructive thing-power (Bennett, 2010).

Actor-Network Theory (cf. Callon, 1991; Latour, 2005) focuses even more on the web of relations that objects incorporate. The study of such relations developed over time into an approach to theorize the agency of objects. Actor-Network Theory argues that to appreciate the meaning and agency of objects and subjects we need to look at the networks in which they are situated. It is only through a focus on relations that we can understand how agency comes about and how humans and technologies affect and act on each other, what kind of acts they bring about and what the meaning of these acts are. Objects are then "actants" that mediate between human actors and systems (cf. Mutlu, 2013). The expression of mediation, however, can be misleading as it may suggest reducing the role of objects to the position *in-between* rather than placing them at the center of a network, where they can very well be situated.

A related approach to grasping the agency of objects in a more transversal way is to follow and trace their dynamics through "open-ended assemblages that are always in the process of (un-)becoming, absorbing, discarding, and transforming disparate human and nonhuman elements" (Voelkner, 2013: 204; summarizing Bennett, 2005). Even though Voelkner describes assemblages in her own work on human (in)security as "circumstantial, unstable, and unpredictable" (Voelkner, 2013: 204), it is equally possible to trace the agency of objects within assemblages that are stable in the sense that these assemblages reproduce themselves and therewith the agency of the objects placed within them. In both cases, using assemblages to trace relations between objects or devices, practices, humans, societies, and discourses allows for a deeper understanding of the complexity of a phenomenon. The methodology of assemblages then situates the object and its agency inside a network at the same time as this network can document variability and flows (Voelkner, 2013).

Methodically, studying the participation of an object within a given context requires immersive and in-depth studies. One literally has to follow the object in order to trace its workings. Such mapping exercises can include historical developments to document the life stories of objects, as well as participant observation (Mutlu, 2013) and other (digital) cartographic methods. Here, it is crucial to be aware of the way in which we as researchers and the instruments we use affect affect this very practice of tracing. van der Tuin and Dolphijn (2010) remind us that in fact all of the involved – that is the observer, the observed, and the observing instruments – are agential. They are active parts of the assemblage that is traced. The methodological commitment to mapping then not only requires the active use of reflexivity in the sense of an explanation as to from where a researcher maps a given object and its workings. It also means that the observer, the observed, and the observing instruments can cause new emergences. Such a methodology necessarily leads away from static categorizations and classifications towards mappings and cartographies as only they can capture dynamic developments and translate this dynamism into theory formation. Cartographies of agency aim to transcend narratives, to trace actualizations, adaptations, mutations, co-constitutions, connections, and connectivities, in-betweens, as well as the multiplicity of flows, rather than fixed grids (van der Tuin and Dolphijn, 2010). I will now proceed to explain the standpoint from which I started my cartography of prediction algorithms and the methodological flexibility that I needed to do this mapping exercise.

Surprises in my research on the life of prediction algorithms

When I started studying predictive policing software and their algorithms, I was interested in the way in which they influence the police's understanding of crime. I wanted to trace if and how algorithms co-constitute the way in which police officers react to crime and even what they consider a crime. Since I entered this analytic project knowing studies about algorithmic governance (e.g., Amoore, 2009; Amoore and Piotukh, 2016), the challenges of predictive policing at large (e.g., Harcourt, 2007), and big data policing (Chan and Bennett Moses, 2016), as well as the broader literature on pre-emption, prevention, precaution, and preparedness (e.g., Beck, 1986; Ewald, 2002; O'Malley, 2009), I was inspired to study prediction algorithms without necessarily conducting yet another discursive analysis of temporality and the politics of "*pre.*" The plan was to start a project that would give me in-depth insight into how matter – namely policing algorithms – works and whether these material entities would change and reformulate police work and the police's understanding of crime. I started out studying the actual software products, but soon realized that this would not be sufficient to find out and map how algorithms act in the context of policing. It was more important to trace the *life* of the algorithm: I needed to understand how these algorithms come about, who is part of writing them, what kind of data is fed into them, how algorithms are received and implemented by police officers, how exactly the software products work and present findings, and how these findings would eventually influence police decision-making.

Even if participant observation would have been an ideal way of studying such questions, I figured that observing the software models in action would involve traveling to three continents and at least five different countries. Instead, I chose to conduct in-depth interviews with software developers, programmers, police officers, and experts in the field. They could answer my questions about how they would collaborate in writing an algorithm, who would translate assumptions about crime into variables, which data was used to train the algorithm, how software owners would introduce the algorithms in police stations (sometimes via long-term collaboration), and how police officers would use and interpret the results and take decisions based on them. Together with an insight into the actual software models, I could begin to trace the agencies involved in this process.

While I originally wanted to focus on the agency of the algorithms, and on that alone, the net of relations around the algorithms almost forced itself into my analysis. It was impossible to map the agency of the algorithm without understanding the workings of data, computing practices, attitudes to and histories of technology in police work and much more. Most importantly, I could not take human agency out of the equation. I had to understand and map how humans, technologies, other objects, and their surroundings truly collaborate and constitute each other in the context of technology-based predictive policing. In short, inspired by the material turn in critical security studies, I expected to find and write mainly about the agency of algorithms. But eventually, this mapping exercise taught me to appreciate the role of human agency in relation to the agency of objects.

Algorithms as digital detectives? An analysis of agency in algorithmic predictive policing

INTERVIEWER: "Will people be out of the loop in creating predictions?"
INTERVIEWEE K: "Well, someone needs to push that 'On' button."

The general premise for prediction software technologies to be developed in the first place is that they will make a difference in policing. In terms of the change that predictive policing software would bring, most interviewees mentioned the expectable growth in efficiency and effectiveness of police work (Int. C, E, G, I, K).[3] For some interviewees this was limited to the idea that the software would assist police officers in making "a better guess" (Int. K) as to where and when to place police staff. The expectation of others was much higher. They wouldn't, for example, rule out that the sheer calculatory power of computers would eventually "outperform a skilled police officer" (Int. B) in strategic planning. These divergent anticipations illustrate the many roles that software or algorithms can play in predictive policing. They also give us a first glimpse into the differing ideas about algorithmic agency in the predictive policing assemblage.

If predictive policing is all about connecting the dots within vast amounts of data in order to recognize crime patterns, the rise of prediction software prompts a few questions: if algorithms search information for particular constellations of parameters, who actually, connects the dots? Who detects the pattern? And who even makes data dots appear in the first place? In this context, the popularized fear of data skeptics is that intelligent algorithms may "connect the dots without any human analyst oversight" (Lindsey, 2018: n.p.). In fact, such statements are uttered by skeptics and optimists alike. They imply the idea that either human or algorithmic intelligence may be better or worse for ensuring the identification of the *right* results – whether these are the correct results, the politically correct results, or the efficient results. However, if one describes agency via assemblages or networks, then it will become clear that there is no such thing as either/or. There is not just one kind of agency or one kind of oversight within predictive policing practices.

Where and when different agencies emerge and unfold may be best told in the form of the life story of the algorithm. Even though such a story is not necessarily linear – as it really consists of multiple stories that intersect and change over time, the scaffolding of a life story[4] may be helpful to illustrate the many points at which agency of humans and technology occur in the process of predictive policing.

Pre-conceptions: preparing (inputs) for the algorithm to be conceived

The computation of crime does not start with the birth of the algorithm. Computing crime ties in with a long-standing history of police bureaucratization, the use of technology within the police, and the many reforms that sought to increase police efficiency (cf. Wilson, 2006). Eventually, the computation of crime intersected with the larger societal shifts from analogue to digital computational means (Int. H.; Wilson, 2018a, 2018b). Keeping this broader historical context of predictive policing in mind, this chapter jumps straight to more recent efforts in digital computation. Nonetheless, the simplified life story that I assembled from the insights gained during my project equally begins before the algorithm. It starts with an intention. Every algorithm is developed for a specific purpose. A software developer explains: "Before we even start looking at the data we have to start working with the stakeholders to find out what it is they want to forecast. They decide that" (Int. I). The question of purpose is tightly entangled with the kind of ingredients or information that software developers would use to build the algorithm. This is an early phase that includes data collection and editing as well as the cleaning or pre-processing of databases to help building and fine-tuning the algorithm at a later stage. In short, "without historic data you can't train an algorithm" (Int. B; similar point mentioned by Int. I). At this stage, agency already appears in multiple shapes, for example with regard to the question of how information – the smallest unit of what will eventually make up the algorithms body – is understood, how it is collected, cleaned, assembled, and translated involves many human and non-human actors. Together, they determine how the algorithm will be implemented and what the algorithm can find.

How information is thought of and conceptualized already makes a critical difference for the algorithm to be conceived. Some software developers plan their algorithm with the assumption that data collection should be "opportunistic" (Int. C) and "greedy" (Int. I). In order to train an algorithm, one should "connect all databases so that we get one answer: this is what we know." (Int. D). Since "the more you know, the better system you can make" (Int. C). However, such databases and archives – no matter how big and connected they are – already act within the algorithmic project as they constitute the data that is available for the algorithm's training. Any dataset only ever reflects that which has at some point been chosen to be registered and stored. One interviewee suggests that the "number of people buying headache medicine" (Int. C) could be relevant for police algorithms, but he also mentions that this data is not registered in most countries – and probably shouldn't be for reasons of data protection (Int. C). With that, he acknowledges that databases, even if they would include any available piece of digital information today, influence knowledge production. They do so through the very information about social life that they do and do not contain. More importantly, such ideas express that any data – if only collected – could be of relevance to a policing algorithm.

Other software developers would not agree with such an all-encompassing attitude towards data. They work with more select and small datasets, for example with information about "what kind of crime occurred, where it occurred and when it occurred." (Int. F). Some algorithms focus only on burglaries and add the stolen goods to the relevant information (Int. J). Advocates of selective approaches to data argue that everything else makes it harder to manage the software (Int. C). Often, the latter developers are also more aware about the way in which data is and is not registered, or collected, and what that actually means for the algorithm. A related, yet slightly different discussion among software developers is whether the data they use is enough or not. Some argue that in "these days, digital data is capturing most things that we would be interested in using. (…) I haven't seen a case where there was a type of data that we wanted to use (and) it just does not exist anywhere" (Int. G). Others find that "We don't have all the important data. (…) It's noisy, it's not perfectly measured, we would have preferred other data, which we don't have. We do the best what we can with whatever we got" (Int. K; similar point made by Int. D).

The different opinions as to what kind of data can make an algorithm and how a dataset literally acts on the algorithm as it determines what the algorithm can do, becomes even more evident when interviewees explained how datasets are pre-structured or cleaned. When interviewee I mentions the pre-structured dataset that they receive about prison inmates, it becomes clear that the police's, magistrates', and prison guards' incarceration practices fully determine the dataset that they receive, which will also influence the algorithms' results. Other software developers mention that datasets obviously vary across cities, which is why algorithms have to be built specifically for the geographies they will be used in (Int. F). Police practice to a large extent structures the data that is available for the algorithm's training. When it comes to the way in which police officers themselves generate datasets, a known challenge is underreporting and other thresholds for reporting. Software developers consider these a "caveat" (Int. A):

> The computer program is only using crime incidents that resulted in a formal incident report that's been created. It's not using information when an officer stops on the street talking to a lady sitting on her stoop (...) The individual officers have their own kind of perceptive of what crime is.
>
> (Int. A)

Another police officer problematizes that "approximately 20% of the police population are registering 80% of the information in the database" (Int. D). This is a fact that constitutes the algorithm's workings. Effectively, a multitude of decisions influence the generation of datasets, as for example, the decisions taken by officers on the crime scene. One interviewee reflects about the semantics of when, for instance, police response officially stops: "Because getting control over the scene, when is that? When you handcuff him? Is that when you provided first aid because someone's shot?" (Int. H). Such semantics influence the writing of reports that will eventually be turned into digital information to be analyzed by algorithms. In a similar vein, another officer (Int. D) deliberates about the way in which data collection by the police has to follow the standards of police law, which are, in his opinion, subjective and often checked manually. Others mention that the analogue technology of the police form prestructures and determines data collection. It only affords the collection of information that the form asks of officers. In addition, such forms only ever represent the information that "is reported or only the information that the officers find" (Int. A). Within the context of data collection, all of these decisions that are either taken by police officers or that are enabled through the bureaucratic technologies of law and form-filling is a form of acting that influences the data available for the training of algorithms.

Not only the original production of information, but also its translation into digital data is a moment where the agency of both, humans and technologies are relevant. Much information does not appear digitally, so it has to be translated into digital formats in order to make it readable and possible to process for a computer (Int. A; E; H). While some argue that nothing gets lost in this process *in principle*,

> (...) *in practice* you may lose some precision because there are limits in how many sources you are prepared to invest in let's say digitizing a picture. Same thing is true with everything else. You may not be able to reproduce the same precision that is in the information unless you take the effort.
>
> (Int. I)

Others are more outspoken about the fact that translating analogue into digital information is always an incidence in which human mistakes can be made (Int. A). With digitalization, social context may also get lost (Int. I). However, since social context is relevant for the processing of digital data at a later stage, some police stations have developed procedures to preserve this context. Such procedures are again highly dependent on the police officer that registers the information:

> So they were obliged to fill in a short story. They had to present in written text what is the story here? What is the suspicion? Why do you think this is suspicious? You have to put it in words. Because we can't really tell that from the data you provided.
>
> (Int. D)

This goes to show that human and machinic forms of writing and reading, of compressing and decompressing information are not necessarily compatible and always a moment of decision-making and interpretation (cf. Hildebrandt, 2016a: 26; Kaufmann, 2018).

Yet another set of technologies that afford and structure the data available for training algorithms are automated systems that remove specific variables from datasets (Int. I) or indexing systems that lead programmers through written text (Int. D). All of these make certain variables and texts visible, but also render others invisible within given datasets – even for the algorithm programmers. Software developers furthermore actively clean datasets of what they consider "errors" (Int. C). They structure datasets by categorizing the type of information "and at some point, you have this challenge: who decides if this is black or white?" (Int. H). Some developers need to do this cleaning and structuring work manually: "We have all this data, all this information, but we don't have procedures, we don't have any systems that help us decide which data to keep, which to delete. The data-management itself is manual." (Int. D).

Not only the cleaning procedures – whether done by technologies or humans – determine the available data for the training of algorithms. Many developers actually add and combine different databases to train their algorithm, some of which they find available in the public domain. For example, Twitter data are used to infer information about relevant events and crime locations (Int. G). Other databases are professionally sold to programmers and developers (Int. H), while some data providers only make parts of the database available for use (Int. C, G). As explained above, all these additional datasets are again built according to the specific assumptions and rules of those who collect and organize the data in the first place (Int. D). All of these databases are pre-structured, which often leads to additional manual or digital cleaning-procedures to prepare them for, and attune them to, the algorithm's purpose.

It has become evident, how much a database and the way in which it is built, cleaned and combined has affordances. Each dataset allows for certain types of usages over others. More importantly, each database allows for certain kinds of analytics over others. The rules according to which databases are built, the data collection methods that determine which data is being registered, as well as the practices of human and non-human indexing and data-cleaning not only make up the complex assemblage of the database, but all of them involve different forms of agency within the process of building an algorithm and of predictive policing at large. Human and non-human influences are already at play in the phase that *precedes* the actual programming of the algorithm. One software developer mentions that these processes have at least one political dimension for him:

> If you want to clean up the data, clean up the algorithm, I'm gonna remove some predictive accuracy, I'm gonna make everybody worse off. There is gonna be more injustice in those decisions, but I'm gonna make everybody equally worse off. The question for policy makers is: is that a good trade?
>
> (Int. I)

When and how specific datasets actually stand for *accuracy* and *justice* is debatable. More importantly, even though the developer is deeply embedded in this assemblage of agency and decision-making, this particular interviewee does not see a role for himself to engage with this dimension: "I don't make that decision – that's up to the policy makers" (Int. I).

An algorithm is born

In fact, decisions about data are crucial to the algorithm's makeup. Data is a basic part of creating an algorithm, or to put it differently, algorithms emerge from a set of formal instructions that scan and learn from specific datasets. Anything that an algorithm finds and presents as results, it knows because it either sits in its formal instructions or the datasets it analyzes. An algorithm needs to be taught how to think. This also includes training on which rationalities to follow. These do not need to be mathematic rationalities, but basically include any theorizations or logics that its developers want to embed in the algorithm (Int. B). The algorithm learns correlative as well causal reasoning, while both correlations and causalities are as multiple as the theories we can find about crime. This means that any decision about what to include in the original setup of the algorithm, e.g. definitions of crime patterns, of what variables count as *correct*, are taken by a team of developers and translated into forms by programmers. The algorithm learns from specific datasets that are "found to be most valuable for each type of crime" (Int. G), for each pattern or logic. From that data, it learns at what point a result is considered a result. Whether the result is relevant, however, still varies.

When it comes to prediction algorithms, the teaching period has two phases. First, the algorithm tries to find patterns that it has been taught to find via parameters in a dataset where the relevant incidents (here, the reported crimes) are unknown to the algorithm, but known to the programmers. It scans this dataset, tries to predict,

> … and gets it wrong. You change parameters and it predicts wrong again. Millions of times. Some predictions were better than others (…) the computer tries to remember the parameter settings that made its predictions better than others (…) It keeps on varying other parameters that didn't have an effect to find.
>
> (Int. B)

The training is considered complete when the algorithm has become good enough at identifying the reported crimes. Thereafter, the algorithm is deployed on one computer where it identifies patterns as it is set up to do, and on another computer where it continues the self-learning process. Here, the computer holds information that the algorithm doesn't know already and the algorithm is still allowed to adjust parameters in order to get even better at predicting. (Int. B). To train an algorithm to become fit for its purpose is both time- and resource-intensive (Int. E, Int. D). Most importantly, any control-measure and any interaction with the algorithm in the training phase is highly dependent on the affordances of each dataset and the algorithm's teachers. One interviewee stated: "whoever works on algorithms and sets them up, they will become powerful people" (Int. H). In its training phase the algorithm is highly dependent on the machine-learning expertise, policing insights, the anecdotal, and criminological knowledge of its trainers (Int. G, J).

Most of these trainers, however, need to work in a team. Here, collaboration is reduced to the specific fields of expertise: for example, criminologists develop the base parameters and contents, programmers translate these into forms and police officers rubber stamp the algorithms (Int. C; Int. J). Each act of translation between these steps is also an act of interpretation. Thus, an algorithm never simply emerges out of itself as a neutrally mathematic entity (Int. B). The agency of each expert and each translation tool is playing into the algorithm. Most algorithms never stop learning, which means that there will be an ongoing interaction with its teachers – at least in the way in which the teachers feed it new information via pre-structured datasets and control the algorithm (Int. D). However, the actual act of testing new parameters is fully automated once the algorithm is set up (Int. F). As we see from the above and the following descriptions, humans and technologies can collaborate at any stage in the creation of predictions. Keeping that in mind, the next step describes one of the moments where human agency moves more into the background and the algorithm's own agency moves to the foreground as it begins to combine parameters in a (semi-) automated fashion.

Algorithms' adolescence

Algorithms are eager learners. Their calculative capacity is their strength, which means that the way in which algorithms eventually outperform human brains is a *calculative* one. While this outperformance is intended by humans (most developers actually consider its calculative strength the software's selling point), algorithms can still provoke quarrels with their teachers and develop their own characteristics. For example, a typical point for algorithms to cause trouble is during their testing-phase with police officers: "a lot of police officers were frustrated with the program" (Int. A). The interviewee mimics officers: "The program shouldn't be predicting this spot, it should be predicting this spot over here. (…) They're like: 'I am smarter than this program is, I know where the crime should be and it's not finding it'" (Int. A). As such, algorithms may cause actual debates about policing identities. Interviewee A argues that police officers can physically interact with the people they intend to police. They have both informal and social information available to understand what drives crime and judge where to patrol. An algorithm, however, simply "knows" where to patrol (Int. A).

This is why some developers actually consider that the informal (and non-mathematic) information police officers have, could in fact change the algorithms' views (Int. A), i.e. what they do and do not find. The opposite argument is made by other developers who say that the skepticism towards the algorithm is surprising (Int. E): Police officers are biased. Algorithms may be, too, but at least algorithms are quicker in making decisions (Int. E). Here, the algorithms' talent has to do with the computer's talent: they are good at computing (Int. B). Algorithms may suffer – some argue – from over-representations of specific populations and types of crime. But generally speaking, once they are programmed, algorithms do have a specific task – and they can concentrate on these tasks better than humans (Int. G). The problem is that while their concentration skills are excellent, algorithms' deliberation skills are limited to keeping or deleting specific parameters with the aim to reach more and better crime matches. At this stage, the human interaction with the vehemently working algorithm would be to keep algorithms from *bubbling*, from ending up in a filter bubble of self-amplified social information (Int. B).[5] More basic interaction with such algorithmic effects is to write policing algorithms that are based on expert knowledge before society is "taken hostage" (Int. C) by more mainstream and generalist companies' algorithms.

Algorithms don't only have concentration skills that are superior to that of humans, but they are believed to be better at considering complex information. This, so some developers argue, can give police officers new perspectives on crime:

> I think police officers don't necessarily have a handle […] of how macro-level or community level factors influence individual behavior.

> That's obviously something the […] software picks up. […] it might change how officers view why crime is happening in particular locations. Why is crime happening here, but not there?
>
> (Int. A)

In providing such selected macro-perspectives, algorithms have agency in the policing process. Further, they have quite a concrete analytic influence: even though their actions are originally based on a programmer's setup, algorithms start deleting parameters out of crime analyses (Int. B) or decide when police officers should stop mapping networks (Int. D). They do that in an automated fashion and – strictly speaking – for, and instead of, the human analysts. At the same time, they also discover new insights or parameters for the analysts:

INTERVIEWER: Did the algorithms come across new insights that didn't exist in the literature before?

INTERVIEWEE G: Some cases seemed unusual at first. […] For example, the phases of the moon. […] There is no literature about why that is the case, but with full moon you may be seeing more outside, what seems brighter etc. [The algorithm] is not building a model that is saying: the moon is explaining the crime.

Besides the identification of new and seemingly relevant parameters for the prediction of crime, the algorithm also makes networks and priorities visible that officers can otherwise not see (Int. D; Int. F). Interviewee D mentions, for example, that their networking algorithm could show that someone may be connected to a group of criminals without showing up in any databases as convicted or suspicious (Int. D). Algorithms can identify such connections, because applying the same rules manually would be too complex for police officers. In fact, algorithms are meant to reveal insights beyond that which police officers know. The software actively creates new knowledge based on the inputs that its teachers have been giving it.

This idea that the algorithm's outputs derive from a "kind of higher knowledge base" (Int. D) also creates a sense of accountability that is co-produced by the algorithm. A police officer argues: "So when we do something to any of our citizens, it's based on a higher level of knowledge" (Int. D). That this higher level of knowledge is not a given and not a purely mathematic process, but dependent on human and non-human collaboration including the many decisions and acts of pre-structuring the knowledge-base, is often not reflected on.

Algorithms' graduation

To be considered mature, algorithms need to be more efficient than humans. They need to outperform them in order to increase police efficiency (Int. B).

While many software developers argue that algorithms are "not meant to replace human ingenuity" (Int. F), algorithms develop capabilities that humans can no longer perform. They produce knowledge in a way that the average human being can no longer understand. A developer said: "Even if you were to say you were to publish the algorithm, it wouldn't make any sense to the people reading it" (Int. C).

In addition to the level of complexity at which algorithms combine different sets of information with each other, algorithms tend not to disclose the arguments about how they have reached a specific result. They only provide the result. Humans without advanced digital literacy can no longer know how exactly the algorithm combines the datasets. In some cases, the same datasets actually led to different results. While Interviewee E argues here that humans also don't *need* to know how the algorithm got to its result, as long as the result is a good one, others argue that an explanation for the results' *why* and *how* is necessary as it would help police officers in the implementation of counter-activities, so that officers "can decide whether these reasons are relevant or not" (Int. A). Interviewee H agrees: "if you could have software that suggests why this is happening, you could guide the officer into the problem-solving on scene […] give better advice to the woman who had a burglar in their apartment" (Int. H). He continues to argue that if algorithms don't explain how and why they got to a certain result, they are less transparent than an officer's decision strategy: "it's harder for people then to question those patterns if these parameters are not visible or accessible" (Int. H).

Algorithms at work

Once a software's prediction algorithm has graduated and is actually implemented, the collaboration between algorithms and police officers moves even more into focus. Some developers and users argue that the algorithm actually does not predict anything, but basically provides police officers with the status quo (Int. D). This status quo is a baseline that is "not gonna change basic human interaction, I think, but it's mostly a tool to make our time a little more efficient, both, the policemen's time for which society pays a whole lot of money" (Int. C).

The algorithm, then, has an impact on the policing process, but does not take decisions *for* police officers, not least because the interpretation of an algorithm's result still needs to be done by those who implement crime control:

> We don't know if there is a police agency out there who would download the (software) and simply just send saturation patrols to all the hot spot areas. And if they did that – really – they would be policing the poor minority communities, which is not what the software is intended for. We wrote the software to identify the highest risk. […] We didn't want police officers to interpret this output too literally.
>
> (Int. A)

This means that a true collaboration between police officers and algorithms is still necessary. Software owners argue that humans are needed to make "judgment calls" (Int. C) and "take decisions" (Int. F; Int. A). What the algorithm adds is efficiency, but it does not replace the officer or human reasoning about crime. In fact, the algorithm should not be too fast and professional. Not only would the replacement of human judgment by algorithms cause unease and surprise, but it would re-determine the collaborative practice of policing for the worse. One interviewee sees the problem in the lack of the officers' media competence:

INTERVIEWEE F: Doing predictions in real time creates distractions for police officers.

INTERVIEWER: How so?

INTERVIEWEE F: Well, if they constantly have to ask the question: "Where are my predictions now?," then they spend more time on their iPhones looking through where the predictions are rather than policing the environment. So it actually is counterproductive to do predictions in perfect real-time.

Software owners argue that the algorithm is meant to empower, and not take agency away from police officers. Some developers would even see the potential in empowering vigilantes or reserve-police officers. Interviewee C, here, sees different outcomes depending on the way in which predictive policing tools would be implemented in the general society. An overreliance on prediction algorithms could cause negative effects by lowering the potential for natural surveillance that sits in neighborhoods. This problem of overreliance could be summarized in the attitude: "the computer will take care of it and the police will fix it" (Int. C). On the other hand, some developers see that the general citizen could be empowered by their own digital device and assist in neighborhood patrol. Here, however, the problem of over-reporting and discriminatory bias in neighborhood policing could easily grow out of proportion.

Algorithmic agency and police agency do not necessarily stand in competition with each other. Rather, it is expectable that both forms of agency will continue to be relevant in policing efforts. And yet, the impact of algorithmic predictions is expected to supersede police agency in some domains. Such expectations are *already argued about.* Interviewee K sees the need for collaboration between officers and algorithms by acting as each other's supervisory authority in terms of investigating and alter each other's prediction results:

> So if the computer says low and you think high risk, you should probably do the assessment once more – and the other way around. The danger is if you trust the computer too much, you might overlook very important information that will lead you to do a sensible decision. But you can also distrust the computer too much and these algorithms using information. You should pay attention to it.
>
> (Int. K)

In such collaborations, police officers would also have to check whether algorithms work lawfully and according to the different national standards on “civil liberties or human rights” (Int. C). Especially this last statement implies that the standards for using prediction technology in the context of law enforcement vary. If taken a bit further, it is a statement about the fact that any of the collaborative efforts of humans and technologies to predict crime are also embedded or situated in specific societal contexts.

Yet, not just the police and the societal contexts in which the prediction technology is implemented influence the algorithm’s results, but the software or algorithm also influences the police and policing practices. Many interviewees agree that algorithms will change policing behavior at large – not just via recommendations. Rather, predictive policing could change key performance indicators in the police – i.e. how the police’s efficiency and effectiveness is measured (Int. G). Interviewee J, too, expects a change in police culture: “Predictive policing will be standard police procedure in 10 years’ time. […] It will change policing culture. It will generate new functionalities and new tasks” (Int. J).

Much can be said about how algorithms may make policing more efficient and effective, but the assemblage of agency described above has shown that algorithms also have the power to render decision-logics invisible and less transparent. Yet, the discourse in the software developer community focuses on the way in which algorithms create new insights and generate new interests.[6] Interviewee D argues that this new knowledge already has an effect on policing (Int. D), but it is hard to understand how actual arrests will impact the algorithm’s formula again (Int. D).

Now, do algorithms die?

When and if algorithms die – that means whether an algorithm will actually stop computing – is in fact a popular debate in the philosophy of science. It is currently seen as the ultimate unknown, not least because the answer to this question is not computable. In order to answer this question, the algorithm has to be run (Int. B). However, whether the algorithm stops computing or not, is not necessarily tied to its ability to act. As we have seen from the above descriptions, algorithms, and technologies that precede algorithms, act and collaborate with humans from the moment the algorithm is pre-conceived. Interviewee C summarized this in relation to computation at large and its relevance in the police’s future: “One thing is sure: they’re gonna be using computers much more than now.” With that, one could assume that as long as algorithms’ results are structuring police work – even after they may be gone or are replaced – their agency remains.

What can prediction algorithms tell us about technology and agency? Some conclusions

One interviewee pondered upon the role that digital technologies would have in predictive policing: "Is there a difference in who tells the story, officers or algorithms?" (Int. H) The analysis above illustrates that the agency of identifying patterns is not a question of either/or. In the process of predicting crime a whole network of police officers, software developers, programmers, digital and analogue forms, manual as well as technical procedures for data collection and cleaning, datasets and not least algorithms co-constitute the results. Within this network or assemblage we find many moments where agencies occur and where humans and non-humans influence each other. And yet, choosing the standpoint of the algorithm to explore predictive policing was done with the intent of placing the focus from human agency onto collaborations. The flourishing materialist approaches in IR and critical security studies tend to explore the newness of matter or technologies as actors. This chapter adds to this debate, but it wants to remind us that agency is not a binary concept, but that it is truly co-constitutive as humans and technologies interact.[7] Indeed, we can say that algorithms have risen to be actors in digitized bureaucracies across the globe. Yet, even if they are deployed as seemingly autonomous detectives with "artificial intelligence," algorithms always collaborate with humans in both, international but also more local contexts.

Amongst other things, this chapter has described how these are *collaborations of influence*: such collaborations between algorithms and humans already have an impact on the local level, for example on specific security domains (as Int. D says about the field of policing). At an international scale, they prioritize patterns as a way to grasp social developments and relations and co-create concrete recommendations and predictions based on pattern analysis. Such predictions have become relevant in various domains of international importance, reaching from economic spheres, the creation of law and order or the consumption of information via media. A closer look at the use of prediction software in the domain of policing, then, gave us an insight into the kinds and stages of collaboration as well as the co-constitutive forces that we need to investigate when we want to understand the politics of automated recommendation that emerge globally in different contexts.

This perspective of co-constitution still prompts a few conceptual questions that are relevant when we want to study the relations between technologies, agency, and the international at large. For example, is technology social? Incidentally, a specific subset of technologies, namely media, have actually adopted the *social* into their name. Admittedly, the *social* in social media rather stands for the idea that they connect people to each other, that they facilitate networks and inter-action. However, this chapter went further in arguing that technologies are more than just means; they exist and act through a group or a network. Due to that, technologies are social in the sense that they relate or have active, interdependent relationships with others. They relate to other technologies, humans, and society. The analysis has foregrounded how technologies cooperate and interact with these networks.

Further, it has become clear that technologies can become an ally, which is the Latin origin of the word social, but also involves the idea of political alliances. In that sense, prediction algorithms are allies for certain forms of crime prevention and the related views on crime. In debates about whether technologies play a role in policing (see the section *Algorithms at work*), we have seen that, for example, software developers and algorithms can be allied. This does not mean that they are always of the same opinion, but we have seen examples where algorithms and police officers stand for specific arguments within the debate and together, they rise as important actors in the technology-supported prediction and prevention of crime. Whether this social character of technologies actually ties in with awareness, reflexivity, voluntariness, and intentionality of algorithms could not be answered with this study, but such questions would be promising material for further research.

A question related to the notion of agency and sociality is whether technology is animate. Choosing the model of the algorithm's life story to explore the relationship between technology and agency is already a partial answer to that question. Algorithms are not alive in the sense that they are made of organic mass. Yet, they are tightly entangled with human life or *bios* at large and have already become co-constitutive parts in biological assemblages. In addition to that, algorithms do have a "body" that is made up of processing instructions, which grows as it works on and with data material. Thus, algorithms may not be alive with respect to all the characteristics of organic life, but this chapter has illustrated that they do have a life cycle. Algorithms can organize, adapt, grow, and evolve in an automated fashion. They may not do so in a self-sustained fashion, since the chapter focused on the way in which agency comes about in networks and relationships. Algorithms do not exist out of themselves. If agency is about the ability to act, then algorithms also need to act on something. Thus, algorithms need an environment to emerge from, but also to engage with in the sense that they – again – contribute to emergences and developments within their environments.

Such "intra-actions" (i.e. the "mutual constitution of entangled agencies," cf. Barad, 2007: 33) also includes the ongoing creation of knowledge, which brings us to the question: can algorithms know? And if so, what kind of intelligence is this? Algorithms are active contributors to the production of knowledge. They *know*, but their knowledge is not based on deliberation, but on instruction. Algorithms receive instructions by developers, police officers, researchers, and ultimately programmers, which the algorithms then implement in environments that are too complex for human minds to grasp.

As we have seen, they can combine parameters in a fashion that is impossible for humans to perform and they can concentrate on this task with machinic rigor. Bowker (no date: n.p.) describes this rigor as knowledge production with a *normative temporality*: "Thou shalt learn at the maximum rate you can (be the best you can be) without hesitation or disruption" (online), without stopping and without a chance "to drop out for a while, to tank the odd subject" (Bowker, no date: n.p.).

Most algorithms then work in a deterministic fashion, namely in order to provide knowledge that is guided by a certain telos, i.e. to make police officers more efficient in preventing specific crimes. Yet, the researcher's view on the algorithm's epistemic work is rather to observe how algorithms influence knowledge production at large (van der Tuin and Dolphijn, 2010). This latter view on algorithmic knowledge production is different from how some software developers look at the algorithm, who understand the algorithmic workings as positive and negative effects,[8] all of which can be solved with newer or better algorithms. Instead of seeing algorithmic knowledge production as mere effects of technological means that can become better at what they do, an argument that sees the algorithms' agencies appear also acknowledges that biases or effects are necessary constituents of algorithmic knowledge production. It is a view that sees being and knowing as entangled: If the algorithm *is* and *acts*, it also *knows* in a specific way. The question then becomes whether there are mechanisms in place to make algorithmic knowledge production comprehensible.

This last part has illustrated how much seeing and studying agency is intimately tied to methodological, ontological, and epistemological questions. Just like in IR, *relations* are indeed in focus when agency is studied. Yet, relations are not just a methodological entry point, but they are the ontological core of agency. They are the place from where human and nonhuman actors and acting emerges. This method of tracing agency via relations is then not deployed to create reproducible knowledge, but to broach the issue of what counts as knowledge. In this process, matter or technologies become a transformative force rather than an object to be studied (van der Tuin and Dolphijn, 2010), which is how, and why, technological agency fundamentally challenges and changes the humanities.

Notes

1 The project and all of its interviews have been subject to ethical evaluations by the Norwegian Center for Research Data (NSD), which formally approved the use of the data in anonymized form.
2 The term software developers relates to those who stand for the final product and are part of the software project at large, also with ideas, planning and inputs. The term software programmers relates to those who write and train the software's algorithm. Sometimes, but not always, these roles overlap.
3 All interviewees are anonymized via alphabetic code. In the following, all references to interviewees will be indicated via the abbreviation Int. & letter.
4 I apologize here for using a rather standard model of a life story.

5 The bubble or so-called early voter problem is now countered by big companies like Google with so-called Google love: "If a new page is instituted, Google actually counters this problem with extra love points: they wait and see whether people will click on it. To see if that changes interest in a person or subject – counter the information bubble" (Int. B).
6 for exceptions see ACM Conference on Fairness, Accountability, and Transparency (ACM FAT) https://fatconference.org (Accessed 28. February 2019)
7 Some have argued that the role of humans in studying non-human agency is again very central as they measure impacts of non-human agents on their surroundings. This, again, leaves the role to decide on what counts as agency, to humans and their agency (Mutlu, 2013). This chapter does not try to identify a solution to this problem, but simply suggests that agency is not reducible to one (i.e. technology) or the other (i.e. humans). It foregrounds co-constitution.
8 These could be challenges to the presumption of innocence, the right to non-discrimination, the proportional use of data.

References

Abrahamsen R and Williams M C (2010) *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press.

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

Amoore L and Piotukh V (eds.) (2016) *Algorithmic Life: Calculative Devices in the Age of Big Data*. Milton Park/New York: Routledge.

Barad K (2007) *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Durham/London: Duke University Press.

Barberá P, Jost J T, Nagler J, Tucker J A and Bonneau R (2015) Tweeting from Left to Right: Is Online Political Communication More than an Echo Chamber? *Psychological Science* 26(10): 1531–1542.

Beck U (1986) *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp.

Bennett J (2005) The Agency of Assemblages and the North American Blackout. *Public Culture* 17(3): 445–465.

Bennett J (2010) *Vibrant Matter: A Political Ecology of Things*. Durham: Duke University Press.

Bigo D (2016) Rethinking Security at the Crossroad of International Relations and Criminology. *British Journal of Criminology* 56(6): 1068–1086.

Bijker W E, Hughes T P and Pinch T J (eds.) (1987) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology.* Cambridge/London: MIT Press.

Bostrom N (2014) *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.

Bowker G C (no date) I Don't Wish to Know That. Department of Arts and Cultural Studies, University of Copenhagen. Available at https://artsandculturalstudies.ku.dk/research/focus/uncertainarchives/activities/archivaluncertaintyunknown/bowker/ (accessed 31 October 2018).

Callon M (1991) Techno-Economic Networks and Irreversibility. In Law J (ed.) *A Sociology of Monsters: Essays on Power, Technology and Domination*. London: Routledge, 132–161.

Chamard S (2006) The History of Crime Mapping and Its Use by American Police Departments. *Alaska Justice Forum* 23(3): 1–8.

Chan J (2003) Police and New Technologies. In Newburn T (ed.) *Handbook of Policing*. Cullompton: Willan Publishing, 655–679.

Chan J and Bennett Moses L (2016) Is Big Data Challenging Criminology? *Theoretical Criminology* 20(1): 21–39.

Crawford A (2006) Policing and Security as ‘Club Goods’: The New Enclosures? In Wood J & Dupont B (eds.) *Democracy, Society and the Governance of Security.* Cambridge: Cambridge Univ. Press, 111–138.

ENISA (2011) Inter-X: Resilience of the Internet Interconnection Ecosystem. Available at www.enisa.europa.eu/publications/interx-report/at_download/fullReport (accessed 31 October 2018).

Esposito E (2013) Digital Prophecies and Web Intelligence. In Hildebrandt M & de Vries K (eds.) *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology.* London/New York: Routledge, 121–142.

Ewald F (2002) The Return of Descartes’s Malicious Demon: An Outline of a Philosophy of Precaution. In Baker T & Simon J (eds.) *Embracing Risk: The Changing Culture of Insurance and Responsibility.* Chicago/London: The University of Chicago Press, 273–301.

Gibson J J (1966) *The Senses Considered as Perceptual Systems.* Boston: Houghton Mifflin.

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

Hildebrandt M (2016a) Law as Information in the Era of Data-Driven Agency. *The Modern Law Review* 79(1): 1–30.

Hildebrandt M (2016b) New Animism in Policing: Re-Animating the Rule of Law? In Bradford B, Jauregui B, Loader I & Steinberg J (eds.) *The SAGE Handbook of Global Policing*. London/Thousand Oaks/New Delhi/Singapore: Sage, 406–428.

Kaufmann M (2018) The Co-Construction of Crime Predictions: Dynamics Between Digital Data, Software and Human Beings. In Gundhus H O, Rønn K V & Fyfe N R (eds.) *Moral Issues in Intelligence-Led Policing*. London: Routledge, 143–160.

Kleinman Z (2015) Are We Addicted to Technology? *BBC News*, 31 August. Available at www.bbc.com/news/technology-33976695 (accessed 31 October 2018).

Kurzweil R (2005) *The Singularity Is Near: When Humans Transcend Biology.* New York: Penguin Books.

Latour B (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory.* Oxford: Oxford University Press.

Lindsey N (2018) Does Predictive Policing Really Result in Biased Arrests? *CPO Magazine*, 9 April. Available at www.cpomagazine.com/2018/04/09/does-predictive-policing-really-result-in-biased-arrests/ (accessed 31 October 2018).

MacKenzie D and Wajcman J (1985) *Social Shaping of Technology: How the Refrigerator Got Its Hum*. Milton Keynes: Open University Press.

Miller C C (2015) Algorithms and Bias: Q. and A. with Cynthia Dwork. *New York Times*, 10 August. Available at www.nytimes.com/2015/08/11/upshot/algorithms-and-bias-q-and-a-with-cynthia-dwork.html (accessed 31 October 2018).

Mutlu C E (2013) The Material Turn: Introduction. In Salter M B & Mutlu C E (eds.) *Research Methods in Critical Security Studies: An Introduction*. Milton Park/New York: Routledge, 173–179.

O’Connell M (2017) *To Be a Machine*. London: Granta Publications.

O'Malley P (2009) "Uncertainty Makes Us Free": Liberalism, Risk and Individual Security. *BEHEMOTH – A Journal on Civilisation* 2(3): 24–38.

Sheptycki J (2007) Criminology and the Transnational Condition: A Contribution to International Political Sociology. *International Political Sociology* 1(4): 391–406.

Tufekci Z (2018) It's the (Demoracy-Poisoning) Golden Age of Free Speech. *Wired*, 16 January. Available at www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/ (accessed 31 October 2018).

van der Tuin I and Dolphijn R (2010) The Transversality of New Materialism. *Women: A Cultural Review* 21(2): 153–171.

Voelkner N (2013) Tracing Human Security Assemblages. In Salter M B & Mutlu C E (eds.) *Research Methods in Critical Security Studies: An Introduction*. London and New York: Routledge, 203–206.

Wilson D (2006) Biometrics, Borders and the Ideal Suspect. In Pickering S & Weber L (eds.) *Borders, Mobility and Technologies of Control*. Dordrecht: Springer, 87–109.

Wilson D (2018a) The Instant Cop: Time, Surveillance and Policing. Paper presented at the 8th Biannual Conference of the Surveillance Studies Network, Århus, Denmark, 8 June.

Wilson D (2018b) The Real-Time Cop: Imaginaries of Technology, Speed and Policing. Paper presented at the EURIAS Conference "Automated Justice: Algorithms, Big Data and Criminal Justice Systems" Zurich, Switzerland, 20 April.