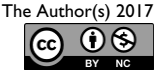
Article

new media & society
2018, Vol. 20(4) 1433–1450



DOI: 10.1177/1461444817697722
journals.sagepub.com/home/nms

Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom

Lina Dencik and Arne Hintz
Cardiff University, UK

Zoe Carey
The New School, USA

Abstract

Social media and big data uses form part of a broader shift from 'reactive' to 'proactive' forms of governance in which state bodies engage in analysis to predict, pre-empt and respond in real time to a range of social problems. Drawing on research with British police, we contextualize these algorithmic processes within actual police practices, focusing on protest policing. Although aspects of algorithmic decision-making have become prominent in police practice, our research shows that they are embedded within a continuous human–computer negotiation that incorporates a rooted claim to 'professional judgement', an integrated intelligence context and a significant level of discretion. This context, we argue, transforms conceptions of threats. We focus particularly on three challenges: the inclusion of pre-existing biases and agendas, the prominence of marketing-driven software, and the interpretation of unpredictability. Such a contextualized analysis of data uses provides important insights for the shifting terrain of possibilities for dissent.

Keywords

Big data, dissent, predictive policing, protest, social media

Corresponding author:
Lina Dencik, School of Journalism, Media and Cultural Studies, Cardiff University, Bute Building, King Edward VII Avenue, Cardiff CF10 3NB, UK.
Email: DencikL@cardiff.ac.uk

The collection and analysis of social media data for the purposes of policing forms part of a broader shift from 'reactive' to 'proactive' forms of governance in which state bodies engage in big data analysis to predict, pre-empt and respond in real time to a range of social problems. The premise is that through the massive collection of data that contemporary technologies allow for, it is possible to identify patterns, outline possible behaviour and predict risk (Mayer-Schönberger and Cukier, 2013). This pursuit has emerged in the context of a broader political climate that has emphasized a proliferation of strategies and mechanisms of government aimed at controlling future events. In particular, a post-9/11 'threat environment' has generated a focus of state conduct on managing uncertainty and the 'indeterminate potentiality' of threats through an operative logic of pre-emption (Massumi, 2015). However, there is a lack of research that accounts for the ways in which different state bodies are making use of big data, and how big data is changing the way states research, prioritize and act in relation to social and political issues. Researching these practices is essential for understanding how and in what context algorithms interplay with key social transformations such as circumstances of protest and the ability to practice dissent. Although big data is often said to promise for more efficient, rational and objective decision-making, the use of big data for governance also introduces fundamental challenges to conceptions of the relationship between state and public and practices of citizenship.

Developments in policing, and protest policing in particular, have been significantly shaped by this wider context, and the incorporation of big data technologies has come to form a central component of decision-making around tactics and strategy. Advances in so-called 'Open Source Intelligence' (OSINT) that seek to collect and analyse data from social media and other sources in order to predict and pre-empt crime and disorder situate current policing practices firmly within the big data-security nexus. This article examines how the British police use social media data for the purposes of policing so-called 'domestic extremism and disorder'.[1] In the United Kingdom, this includes the policing of certain demonstrations and protests. We explore how analysis of social media data comes to inform pre-emptive and real-time police tactics and how 'threats' are defined and understood. In particular, we investigate how algorithmic processes are situated within existing institutional practices and in relation to human decision-making and broader social context. This provides much-needed evidence to the big data-security debate, which remains often speculative and abstract. We start by discussing the emergence of big data-based pre-emption in governance, focusing on protest policing. Based on a presentation of findings from our empirical research, we then argue that data-driven policing introduces significant (re)conceptions of threats that need to be understood in the context of human input and assessment as well as existing social and institutional practices. In particular, connecting our empirical analysis to a growing body of scholarly concerns with algorithmic decision-making, we highlight how the integration of big data into policing introduces questions around bias, marketing-driven analysis and the interpretation of unpredictability. These all speak to a shifting and complex terrain for the expression and enactment of dissent in a datafied 'threat environment'.

Big data and pre-emption as governance

The shift from 'reactive' to 'proactive' forms of policing is closely aligned to a heightened security focus since 9/11 that became particularly pertinent in the United Kingdom

following the 7/7 bombings in 2005 (Gillham, 2011). Massumi (2015) argues that 9/11 has introduced an entirely distinct 'operative logic of power' that has come to define the current political age, namely, one centred on *pre-emption*. That is, actions are carried out on the basis of

> *uncertainty* – and not due to a simple lack of knowledge. There is uncertainty because the threat has not only not yet fully formed but … it has *not yet even emerged*. In other words, the threat is still indeterminately in potential. (Massumi, 2015: 9; italics in original text)

As Massumi points out, this leads to a problem of perception and time: how do you perceive what has not yet emerged? How do you perceive potential? By what mechanisms can the not-yet be operationalized?

The incorporation of big data technologies in modes of governance speaks to this problem. Underpinned by the '4Vs' of big data – increased volume, variety, velocity and veracity of data elements (Amoore and Piotukh, 2016; Mayer-Schönberger and Cukier, 2013) – and centred on the activities of 'capture, curation, and analysis' (Hey et al., 2009: xiii), data-driven processes have come to provide a seemingly 'scientific' method for tackling uncertainty. Threats are rendered perceptible through algorithmic calculative devices, logics and techniques that give this big data 'meaning' (Amoore and Piotukh, 2016). Algorithms – automated instructions to process data and produce outputs – may allow for understanding previous occurrences, predicting future behaviour and facilitating possibilities for pre-emptive action. It is argued that based on scientifically generated and value-neutral information, data may reduce political influences and subjective judgements, and may therefore offer a more rational, impartial, reliable and legitimate way of decision-making (cf. Mayer-Schönberger and Cukier, 2013). In the context of security problems, the promise (and supposed necessity) of big data as a 'game changer' (Hildebrandt, 2013: 8) lies precisely in the perceived 'epistemic capabilities of algorithms' (Aradou and Blanke, 2015: 6) to anticipate, conjecture and speculate on future threats. This logic justifies a need to 'collect it all', and it establishes trust in the 'new' processes, rationalities and techniques of decision-making through which algorithms can unveil the 'unknown' (Aradou and Blanke, 2015). The motivation becomes to trust in probabilistic reasoning as a way to mathematically render uncertainty (Frické, 2014) and thus operationalize the 'not-yet' through mechanisms that do not have to rely on 'feeling' but on 'objective' and 'rational' forms of analysis, secure in the belief that the ability to collect (all) data yields better knowledge.

Following 9/11 and attacks in Madrid in 2004 and London in 2005, the use of big data for predictive policing increased precipitously as the operative logic of pre-emption took root. Amassing data from various surveillance networks, predictive policing has come to incorporate event-based concerns (frequency of arrests, emergency phone calls, incident reports and complaints), place-based concerns (known addresses of criminal suspects, locations of gang activity, places where crime is common), the types of crime that are typically reported (violent, property), information about individuals (suspects, convicted criminals, individuals with links to criminal networks), gang activities, traffic patterns and environmental factors (poor lighting, lack of police surveillance, easy escape routes, infrequent pedestrian traffic, etc.) (Badger, 2012; Howard, 2012; Koehn, 2012). The

programme PredPol, for example, developed collaboratively by California police and academic institutions, was designed to process all of these concerns and deliver predictions about crime hotspots to police on the street in real time (Mohler et al., 2011). Programmes like CompStat (used in New York City) and Palantir (used in Los Angeles) process historical crime records to map the time and location that various types of crime are likely to occur or predict the likelihood that individuals will commit a crime (Kelling and Bratton, 1998; Kelly, 2014). Similar programmes were subsequently introduced in the United Kingdom (Jones, 2014).

Initially focused on deterring criminal activity such as theft and violence, this logic of predictive policing has moved to incorporate a wider sense of public order, including the policing of protests and demonstrations. This coincides with a shift in protest policing strategy from what Gillham (2011) describes as 'negotiated management' in which active cooperation between police and protestors is encouraged through the institutionalization of permits and planning, to a strategy of 'strategic incapacitation' characterized by the goals of 'securitising society' and isolating or neutralizing the sources of potentially disruptive protest actions or events (similar to the practices of the 'Miami model' as outlined by Vitale, 2006 and Elmer and Opel, 2008). These goals are primarily accomplished through (1) the use of surveillance and information sharing as a way to assess and monitor risks, (2) the use of pre-emptive arrests and less-lethal weapons to selectively disrupt or incapacitate protesters who engage in disruptive protest tactics or *might* do so and (3) the extensive control of space in order to isolate and contain disruptive protesters whether actual or *potential* (Gillham, 2011: 637, original emphasis). In the United Kingdom, for example, pre-emptive actions have included disruption of protests by implementing checkpoints and searches that discourage attendees from participating, or the use of pre-emptive arrest and 'kettling' (containing a crowd within a limited area) to upset the network of organizers by removing strategic influencers (Swain, 2013). Social media uses for protest policing have become a more prominent practice as part of this shift, including real-time monitoring of tweets to track the movement of demonstrators (Procter et al., 2013a); infiltrating social media communication to identify rioters (Trottier, 2012); broadcasting information, instructions and available resources to affected communities (Procter et al., 2013b); as well as developing personal profiles on organizers and participants alike, including 'habits, lifestyle, modus operandi, addresses, places frequented, family-tree chart, photographs, risks to public, ability to protect him/herself, and related information' (National Intelligence Model, quoted in Swain, 2013).

These developments in policing are emblematic of the ambition to predict (and control) the future. However, the claims to objectivity, impartiality, reliability and legitimacy of big data and its algorithmic processing have been questioned (Elmer et al., 2015; Gillespie, 2011, 2014) and criticized as 'carefully crafted fictions' (Kitchin, 2017: 17). Rather, as data collection is initiated, and algorithms are developed by humans, a great deal of expertise, judgement and choice is reproduced in the data. This means that big data is not necessarily an accurate representation of offline reality, but it is shaped by the way it is created, collected, stored and interpreted. The social context of data generation is thus crucial for its interpretation (Halford, 2015). Furthermore, the continuing role of human judgement may entrench existing discrimination or produce new forms of discrimination based on staid categories or skewed data sets, while pertaining to a belief in

the accuracy of predictions and the representativeness of decontextualized data (Halford, 2015; Peña Gangadharan et al., 2015).

Significant arguments have been made regarding the ways in which algorithmic processes come to shape understandings of the world, and therefore become 'the new power brokers in society' (Mackenzie, 2007: 93). The 'subtractive methods of understanding reality' – that is, the reduction of information flows into numbers that can be stored and then mined – produce very particular forms of information and computational knowledge (Berry, 2011: 2). Big data thus carries its own specific set of values and logics. As noted by boyd and Crawford (2012), it shapes the reality it measures by staking out new methods of knowing. However, there is still a lack of research that can illuminate these debates by looking at how technologies are incorporated in governance in practice. Below, we explore this by focusing on the uses of 'big data', particularly social media data,[2] by the British police for the policing of protests and demonstrations as a way to illustrate important social and political implications of algorithmic decision-making.

Policing 'domestic extremism and disorder' in the United Kingdom

In terms of British policing, protests and direct actions fall under the remit of the National Domestic Extremism and Disorder Intelligence Unit (NDEDIU). The establishment of domestic extremism units within the police followed a period of militant animal rights campaigning in the late 1990s and 2000s in the United Kingdom, particularly aimed at targeting animal testing laboratories (Lewis et al., 2013). In 2001, a new unit was set up within the National Crime Squad to police 'animal rights extremism'. Additional forms of militant activism were incorporated in the remit of 'domestic extremism' policing in 2004. Further restructuring in the years that followed led to the eventual creation of the NDEDIU that placed stronger emphasis on gathering and understanding intelligence relating to domestic extremism in order to expand prevention and enforcement in the policing of domestic extremism and strategic public order issues in the United Kingdom and was put under the lead of the Metropolitan Police Service's Counter Terrorism Command in 2011 (National Police Chiefs' Council [NPCC], 2016).

The term 'domestic extremism', most frequently described as 'serious criminality', has been controversial and ambiguous from the outset. It is seemingly intended to refer to forms of radical political action that pertain to domestic policy as opposed to, for example, 'extremist' views related to so-called Islamist fundamentalism. However, as the policing of 'domestic extremism' now falls under the remit of counter-terrorism units, these distinctions have become unclear (cf. Quinn, 2015). Moreover, the UK government has in recent years foregrounded concerns with 'extremism' and has expanded definitions and meanings of this term to include non-violent extremist 'ideology', often framed in terms of 'values'.[3] This has created further ambiguity around how 'extremism' is defined and distinguished, expressed also from within the police (cf. Dodd, 2014). The practices of policing protests, activism and disorder in the United Kingdom have therefore developed within a continuously changing context that has raised significant concerns regarding the scope of and possibilities for dissent. This has also extended to the

methods and tactics employed by the police, including recently renewed criticism of the infiltration of activist groups by undercover officers (cf. Lubbers, 2015).

The so-called London Riots that took place in London and elsewhere during the summer of 2011 were significant for developments in police practices, particularly in relation to intelligence gathering. The Inspectorate of Constabulary report *The Rules of Engagement* into the policing of the riots outlined social media as a key area of policing to be developed in order to prevent similar events from happening in the future (Her Majesty's Inspectorate of Constabulary [HMIC], 2011). Reports have suggested that since 2012, the NDEDIU has developed a team of 17 people working with Social Media Intelligence (SOCMINT) specifically (Wrightm, 2013). At the time of research, the collection, engagement and uses of social media for policing purposes fell under the regulatory framework of the Regulation of Investigatory Powers Act (RIPA) from 2000. Within the RIPA policy framework, the Data Retention and Investigatory Powers Act 2014 (DRIPA), and the Data Retention Regulations (DRR) from 2014 provided specific updates on data-based investigations. However, this regulatory framework has been widely criticized for being ill-suited for the contemporary digital age, described by David Anderson QC, who was commissioned to review terrorism legislation in the United Kingdom, as 'incomprehensible and undemocratic' (Anderson, 2015). It provided little governance and oversight in practice for this growing use of social media in policing domestic extremism and disorder, and police have predominantly developed their own guidelines for how to interpret current legislation with regards to uses of social media data for policing.[4]

Researching social media and big data uses

The research project on which this article is based examined how social media data are collected and analysed by police in the United Kingdom for the purposes of policing domestic extremism and disorder and how these analyses come to inform police strategy, particularly around events such as demonstrations and protests. For this article, we are focusing on one particular part of this project: a set of semi-structured interviews with British police involved in the policing of domestic extremism and disorder. The interview sample consisted of five senior members of the British police force identified at the time of interview as

- Head of Open Source and Social Media, National Counter Terrorism Police Functions Command (Interviewee A);
- Head of Digital Engagement at the College of Policing (Interviewee B);
- Previous Head of NDEDIU and the Chief Officer Lead for the National Police Co-ordination Centre (NPoCC) (Interviewee C);
- Head of the Communications Data Investigators team (Interviewee D);
- Regional Prevent Officer leading a social media taskforce (Interviewee E).

All interviews were carried out during August and September 2015, in person, lasting on average around 90 minutes, and aimed at exploring the uses of social media for policing. Using interviews with police as a research method has certain limitations in that it

may not expose all the practices and tools that are applied, especially those that police wish to conceal, and we were not provided with some information. However, these interviews gave us a number of key insights into the operations of the police and the ways in which social media is integrated into police practices. The level of access we were granted to very senior members of the police meant that we were able to explore the broader rationale, visions and challenges in using social media for policing purposes despite the small sample. We were not allowed to record all interviews, and the quotes used in the rest of this text are primarily from those interviews that we were allowed to record and from those interviewees working particularly with the intelligence side of policing. However, all interviews provided us with relevant information about police practices, and note-taking from all interviews helped inform our analysis.[5] In the following section, we present key findings from the interviews.

Social media data collection as police practice

Police collect social media data leading up to any event, such as a protest or demonstration, and they monitor social media activity during the event. As such, social media monitoring is used for both pre-emptive as well as real-time police tactics and responses. Most of the time, police decide to monitor events based on prior information that an event is happening, either through other forms of intelligence or from the media. This could also include knowledge of community tension, or if something has happened that might trigger reactions from certain groups. In addition, police are also considering social media monitoring to identify potential tension surrounding the police, or hostile mentions of the police, which was described in an interview as 'looking for reputational risks for the force' (Interviewee D).

Our interviews highlighted that the use of social media data for British policing is a relatively recent development. Partly attributed to an institutional culture and a demographic make-up 'dominated by 40-plus white males, rightly or wrongly, that haven't grown up on social media' (Interviewee D), integrating social media into broader police practices still operates on a 'learning curve'. Within the operations of NDEDIU, the use of social media as a regular police practice only began to develop in 2012, following the London Riots and criticisms of other forms of intelligence-gathering as mentioned above. According to one of our interviewees, who was leading the domestic extremism unit at the time, this contributed to a reconsideration of tactics within the police:

> [I]t made certainly me and others think, is there another way we can gather information which is more proportional? For me it's always about … recognizing that if you want to have legitimacy amongst the public, you've got to be able to gather information which the public can go, that's not unreasonable. (Interviewee C)

As such, uses of social media for policing domestic extremism and disorder emerged as a response to a combination of events that not only highlighted the potential role of social media in organizing and mobilizing forms of protests and uprisings, but also a perception of social media as a more legitimate resource for intelligence gathering. While part of this legitimacy stems from a perception of these data being 'public' (or

'open' as in 'open source intelligence'), the nature of these data has also been subject to negotiation within the police. Our interviewees recognized that collecting data for policing purposes has implications for understandings of the public and private nature of such data:

> [U]p until a couple of years ago, the joint thinking – not just in the police but across a lot of the organisations – was that if you saw it on social media, it's open to anybody, then there's no privacy issues. We fought for a long time, we fought for more governance and we said that's not right, there are privacy issues here. (Interviewee D)

In recent years, the police have produced guidelines for how social media data can be used for policing purposes that set out parameters for, for example, monitoring individual accounts and profiles, and rules for the length of time data is retained.

Importantly, a prevalent theme that emerged from our interviews is that SOCMINT is not treated as an isolated practice within policing. Rather, it is integrated with other forms of intelligence-gathering practices, exemplified also by the structure of the NDEDIU. As part of this unit, SOCMINT sits under the creation of an 'all source hub', which integrates social media data with other forms of intelligence (human intelligence, undercover work, etc.) and existing databases. In this way, the policing of domestic extremism and disorder comprises three elements: big data, intelligence and databases (Interviewee A). This means that SOCMINT is 'cross-checked' with other forms of intelligence:

> Social media isn't the only tool you'd use to understand the dynamics of large-scale protests which may become unlawful. There'll be other intelligence means. There'll be an understanding of what's happened before, what happened the last time this group protested. So social media, I think, is just one tool in the box of many. (Interviewee C)

The integration of OSINT and SOCMINT into the policing of domestic extremism and disorder has relied on bringing in external programmes and tools. The NDEDIU does not house software developers and engineers who develop software for the police. Nor is there one specific provider of tools catered for police and law enforcement purposes. Rather, the police have bought a host of programmes and tools from different companies. These are a combination of 'off-the-shelf' tools that are already available and programmes that have been purchased through a procurement model (Interviewee A). There is some scope for the police to make suggestions for changes and amendments to these programmes to better suit their needs, but there is no active involvement in the design or development of the actual software. The collection and analysis of data, however, is all done in-house. Software developers or private 'accredited training companies' train police in using the software, as well as in how to use social media data more generally. This means that the police do not design or necessarily have knowledge of the algorithms behind the software they are using for data collection and analysis:

> [W]e're just knowing that we're looking for A if it's associated with B and also has C in it, then we'll write that query and we'll see what comes back and then we'll tweak it and we'll add in exclusions or inclusions. So the actual algorithm [that] sits behind it [is] beyond us. (Interviewee D)

Predominantly, the tools used by the police are commercial tools that have, more often than not, been developed for marketing rather than law enforcement needs and are then adapted for policing purposes:

> A lot of stuff came out of marketing because marketing were using social media to understand what people were saying about their product … We wanted to understand what people were saying so it's almost using it in reverse. (Interviewee C)

Due to sensitivity about revealing police capacity and tactics, we were not provided with names and details of the exact software that the police use, but mainstream tools such as TweetDeck and Hootsuite were mentioned in addition to those acquired through procurement (see also Trottier, 2015).

Uses of social media data for protest policing

Monitoring social media activity for the purposes of policing protests was predominantly described as aiding 'situation awareness' for any given event (Interviewee A). Mostly, the focus of policing protests as expressed in the interviews concerns potential disruption or violence at protests: 'what we're looking for is somebody that's going to go there, either to cause disruption against the protest or use the protest as cover for further activity' (Interviewee D). Below we outline prominent big data uses and types of analyses that inform predictive policing of protests as outlined in our interviews.

Keywords and threat words

Keyword searching is the most dominant practice. Large data sets relating to a particular event are filtered by a list of keywords, in order to search for potential threats. 'Threats' in this context would be, for example, particular words associated with violence or disruption ('threat words'), and would be followed by an assessment as to whether further action is needed to identify individuals. Lists of keywords and threat words are context-specific, and different lists are developed depending on the nature of the event, the location and the people it is likely to attract (particularly to include sensibilities of language and dual meaning words, for example, 'flared trousers as opposed to a flare being set off' [Interviewee D]). As such, algorithms are used to 'filter the noise' in terms of particular words that allow police to assess only highlighted data:

> We'll look for people talking about guns or whatever at protests and it'll produce a PDF document to say all these posts have got all the criteria you're looking for, and we'll look through them and then there's one in there that actually is of interest to us. We'll take that and we'll put that into an intelligence report. (Interviewee D)

Risk assessment and resourcing

Furthermore, social media data allow police to gather a sense of who and how many people will be attending an event and how militant it might be. As such, 'threats' might

be identified in this context by ascertaining whether certain groups and individuals are attending the event, and what their intent of going there might be:

> Lots of events are organized on Facebook publicly and that gives you a good feeling for how many people are going, and I don't think that's unreasonable for the police to understand how many people are coming to an event, and whether or not the words they're saying, the symbols they're using suggest violence or otherwise. (Interviewee C)

The interest in whether 'risk' individuals or groups are planning to attend an event is frequently informed by prior knowledge about those people. In other words, many activist groups are well known to the police based on previous intelligence: 'you can work out there are some groups that come and protest and they don't protest peacefully and they never have' (Interviewee C). Monitoring the social media activity of these groups, in particular in the lead up to an event that could be of interest to them, will be part of police planning for that event.

Influencers/organizers

Linked to that, social media data analysis is used to identify what was referred to in interviews as 'influencers'. One of the outcomes of the investigation into the London Riots was the perceived need to identify individuals who may be influential in certain contexts (e.g. DJs proved to be influential during the London Riots) (Interviewee A). In several instances, the notion of 'influencers' was intertwined with 'organisers' in interviews and it is not entirely clear how distinct these categories are. However, influencers would typically be characterized by online reach and following, rather than involvement in the event. Software tools such as Klout may help police identify influential individuals or groups, in which the amount of tweets, re-tweets and followers will highlight particular accounts. This may be of interest to the police in terms of 'engaging' with such individuals and groups before an event or for identifying potential criminal activity resulting from the nature of influencer communication:

> There are some really influential people on Twitter, who have thousands and thousands of followers and they say something and it gets repeated a thousand times and that word or that feeling's been repeated 10 or 20,000 times. That's quite powerful and quite fast … If you've got someone who is saying lots of things that suggest let's be violent and that's been retweeted by lots of other people, that person, you could argue, is starting to influence the people who are coming, you're starting to plant seeds in their minds. (Interviewee C)

However, there is also recognition that definitions of 'threats' in terms of influencers (or organizers) on these terms can be problematic:

> I think you have to be careful with that one because being an influencer, does that make you a bad person? Does that make you someone the police should be interested in? If you're influencing a crowd to do something that's unlawful, absolutely but if you're just an influencer, then I think you have to be careful. (Interviewee D)

Sentiment analysis

Even though marketing-driven software has placed much emphasis on sentiment analysis of big data, it remains a marginal aspect of police social media practices. It may serve as a source of information for more long-term developments, but the level of sophistication of sentiment analysis, at the time of research, was not high enough to inform real-time police tactics (described as 'over-rated' in one interview). Furthermore, it may require contextual knowledge that can account for different demographics, places and cultures. However, basic analysis of the mood of a crowd might help signal any potential tension with the police:

> I suppose things like if you're dealing with a large event and you've got crowds, is this crowd happy or are they cross or are they angry? Are they saying things that the language is really angry and really cross and they're not happy with the police, or is it really positive about the police because you'd argue if the sentiment was really negative about the police, we might change our tactics. (Interviewee C)

Geo-location

Despite the uses of some software by the police that is particularly concerned with geo-location, the limited availability of geo-location on major social media platforms such as Twitter and Facebook makes it a marginal aspect of big data analysis. Less than 2% of tweets are geo-tagged (Interviewee A), making it problematic to rely on this to gather information about the location of crowds or individuals. Instead, potential locations for gatherings of crowds are identified through keyword searches as mentioned above. However, as with sentiment analysis, this practice is set to develop further along with technological developments.

Situating big social media data in the policing of dissent

These types of analyses are part of a significant shift in police practice – from 'reactive' to 'proactive' policing. Although the data produced from these processes are not used in isolation, they do come to inform police strategies in particular ways. For example, they might be used for certain types of pre-emptive tactics, such as pre-emptive arrests and/or interception of actions:

> If someone's discussing something openly online and we've come across it, and they've said, I'm going to go to the protest tomorrow and I'm going to set off flares, then if there's something criminal in that – i.e. is it illegal to possess what he's saying he's going to set off if it's a flare or whatever … Then that might be something that we take action against at his house and arrest him before he actually gets there … Or if actually what he's talking about is, I'm going to go down there and I'm going to cause mayhem and all the rest of it, we actually might go round and say to him, we know you're planning to go and can we suggest another course of action for you. (Interviewee D)

Seeking out certain individuals or groups prior to an event may also include people who are considered to be key figures or potential organizers:

> What we have in the past done is we've identified organisers of a protest and we've gone round and spoken to them, not because we think that they're going to do anything criminal but to say, we know you're going to have a protest, how can we help you make sure that that protest goes off safely? (Interviewee D)

As such, predictive analytics will in some instances lead to pre-emptive tactics such as seeking out or confronting particular groups before any activity has occurred. A key aspect of predictive policing in this respect is to identify potential trigger points that might lead to disorder before it happens. Moreover, data will inform what strategies will be used for policing any given event depending on the size, nature and militancy of the crowd. As mentioned above, this might mean softer or more forceful forms of policing as well as being able to navigate activities as they are about to happen so as to respond in real time with changed tactics. While ambivalence remains around acting upon automation, we can therefore see how algorithmic processes transform understandings of threats that shape the practice of policing in a continued human–computer negotiation. Threats are perceived and identified in a particular context of data-driven analysis carried out in relation to existing social and institutional practices that introduces a number of important questions regarding developments in protest policing. Here, we want to highlight three particular aspects that we argue have significant implications for the limits on dissent.

First, as our findings highlight, police continue to emphasize the role of 'human assessment' in any outcome produced by automated processes such as the analysis of big social media data. This is significant as it highlights the role of human judgement in data processing and responds to concerns regarding the claims to objectivity, impartiality, reliability and legitimacy of big data (Elmer et al., 2015; Gillespie, 2011, 2014). As noted earlier, the algorithms that are at the centre of big data analysis and that categorize people in order to make predictions about their behaviour (as well as recommendations of products, treatments and courses of action) may replicate classic forms of discrimination and establish new categories of differential treatment. Algorithms may create self-fulfilling prophecies whereby the targeting of certain groups in the initial analysis raises their visibility in all future calculations while obscuring other forces at play (Edwards, 2015). In predictive policing, for example, data mining can constitute a form of discrimination if it leads members of protected classes to have disproportionate contact with the police. The spectre of discrimination becomes especially acute if members of these groups find that they have a greater chance of being caught when committing the same crime as others (Barocas, 2014). In protest policing, it may disproportionately highlight those who have attended previous protests as potential threats, regardless of whether they have been involved in unlawful activity or not (cf. Lewis and Evans, 2010).

The 'biases' of any algorithmically produced pattern or identification of networks, groups and individuals are 'corrected' within the police by integrating big data analysis with human intelligence and existing databases. Thus, any action or tactic employed continues to rely on what was described as 'professional judgement'. As such, big data analysis is not an automated process in the way that is frequently assumed in debates on big data. The role of human input, both in terms of designing the algorithms as well as any analysis and interpretation of such data, remains central in data-driven governance.

The notion that big data may absolve human errors and allow for 'objective' or 'efficient' forms of governance, therefore, is largely mythical in the context of this study at least. Rather, big data is predominantly used to identify patterns that are subjectively (humanly) interpreted and assessed, not least in the identification of any anomalies within these patterns. Thus, discretion (and assumptions and ideology) is a key feature in data-driven policing. In particular, pre-existing knowledge, intelligence and broader societal understandings of events continue to shape and determine big data analyses. This points to the significance of understanding the integration of algorithmic processes as part of a set of agendas and interests, contextually shaped and advanced.

Second, our findings highlight the significant role played by private and commercial actors in automated processes in the policing of protests. Most of the tools used by police are commercial tools either obtained 'off-the-shelf' or commissioned through a procurement model. At its most obvious, this introduces significant issues around accountability, as the algorithms used for predictive policing remain obscure to both police and the public. Moreover, the dominance of marketing-driven software development, which informs much of the commercial tools and programmes available for predictive analytics, also produces a particular type of data and, ultimately, knowledge. Debates in the emerging field of 'data science' have indicated the extent to which big data introduces a new epistemology and a new way of categorizing social phenomena (cf. boyd and Crawford, 2012; Fieke, 2014). Our findings illustrate the extent to which the algorithms that are developed and the categories that are used to order data are catered towards marketing needs, integrating terminology and salient categories of subjects and communication derived from the field of marketing. Notions such as 'sentiment' and 'influencers' are predominantly defined and identified by terms that speak to data that are important for marketing purposes. These same categories, and the basis upon which they are defined and identified (whether through reach or through negative or positive language), are being transferred to analyses of data for entirely different purposes, such as law enforcement. Although some of these categories may be informative for police, they shift understandings of 'threats' towards particular communicative practices whose meaning originates in a very different context. This is at its most explicit, perhaps, in the wish to apply big data analysis to monitoring reputational risks for the police. These practices lead to a reinterpretation of 'threats' on quite alien terms that also expand the meaning of (supposedly illegitimate) dissent.

Finally, third, and related to this, notions of predictability and probability remain contentious in the use of big data. As discussed in our interviews, social media data remain inconclusive and will not lead to predictable results. In this sense, ascertaining the probability of something happening (which relies on knowing all information) is not the same as ascertaining the predictability of something happening. Social media users have developed specific cultures in relation to the various platforms, which are often very different from the cultures, interactions and types of communication found offline (or on other platforms), and investigations that are not rooted in these cultures will likely lead to misinterpretations. Social media platforms also contain limitations to expression that may alter the intended meaning of a user. Typically, users do not always represent themselves accurately online, or implement in real life what they announce online, and the characteristics of social network ties do not necessarily translate from social media to

'real' life. The social context of data generation is thus crucial for its interpretation (Halford, 2015). A key question for practices of predictive policing is therefore how to deal with the uncertainty and unpredictability that remains with much (if not most) social media data. If the goals and promises of predictive policing lead officers to interpret unpredictability as 'risk', this can become conducive to an environment of 'over-intervention' by the police. In other words, will what is (and inevitably will remain) 'possible' be interpreted as 'probable' and therefore lead to pre-emptive tactics? If the assumed possibility of predictive policing to pre-empt and therefore eliminate an increasing range of criminality means that a risk becomes interpreted as a possible threat, monitoring of, and intervention into, activity based on social media data is likely to expand.

Conclusion

As our research illustrates, the operationalization of the 'not-yet' with regards to protest policing is increasingly incorporating algorithmically produced intelligence based on social media activity. As argued above, these technologies are part of operationalizing the problem of perception and time that inevitably arises from trying to 'control the future' (Massumi, 2015). Big data, and social media data especially, has been said to provide possibilities to predict, pre-empt and respond to a range of social problems and risks on the basis of mathematical calculation and perceived 'epistemic capabilities of algorithms' (Aradou and Blanke, 2015). At the same time, this perception has also been met with substantial concerns with the ways in which algorithmic decision-making in governance can significantly (re)shape possibilities for social change. Often suffering from a lack of empirical analysis, these debates struggle with situating uses of big data in context and in relation to institutional practices.

In our study of the uses of big social media data for the purposes of protest policing in the United Kingdom, we have illustrated the need for such a contextual perspective in order to understand the complexities of this shift in governance. We have seen how the transformation from 'reactive' to 'proactive' policing combines data analysis with human intelligence and interpretation. Algorithmic processes in police practice are embedded within a continuously negotiated human–computer interaction that incorporates a rooted claim to 'professional judgement' and a significant level of discretion. Rather than a simple transfer from human to algorithmic decision-making, big data analysis involves contextual knowledge and information and leads to complicated negotiations on underlying questions such as the boundaries between public and private data. As more information on analytical programmes and data scores becomes available (cf. Angwin et al., 2016), the dynamics of their institutional application and the exact interactions between data analysis, human intervention and different interests remain under-researched. This project thus points to a crucial research agenda in an increasingly datafied environment.

While the continued role of human discretion may ease some concerns regarding automated decision-making, our research has highlighted three challenges: First, human interventions may insert pre-existing biases and agendas into predictive policing, and a (implicit or explicit) trust in the objective and neutral nature of data analysis may exacerbate and conceal that bias and those agendas. Second, many of the tools used for data collection and processing are commercial programmes, many of which were developed

for marketing purposes. This raises the 'black box' problem (Pasquale, 2015) of police having little understanding of how data output is created, adds difficulty to the interpretation of data and implies that data are attributed meanings which originate in different contexts and are quite alien to questions of law enforcement. Third, most data are likely to remain inconclusive and thus uncertain and un-predictable. In the context of a security-led need to limit uncertainty and render events predictable, this means that 'naturally'-inconclusive human activity comes to be interpreted as a risk and therefore (legitimately) subject to intervention in the form of pre-emptive measures.

These negotiations become significant in our understanding of the possibilities for dissent as interpretations and perceptions of threats become shaped by the dialectics of the big data-security nexus. In other words, policing as a practice is negotiated between the desire to predict future outcomes on a rational mathematical foundation that requires the ability to know all information (and for this information to be correct, representative and unbiased) while being subject to the realities of human input and interpretation at all stages of the policing process. Although we found a level of hesitance towards automated processes and recognition of the limitations of algorithmic decision-making in our interviews with police, these processes are part of shaping an increasingly complex terrain for the possibilities for dissent that needs to be understood within the broader operative logic of pre-emption as well as the context of existing institutional practices.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: The research for this article was made possible through a grant from the Media Democracy Fund, the Ford Foundation and the Open Society Foundations.

Notes

1. This article is based on the project 'Managing "Threats": Uses of Social Media for Policing Domestic Extremism and Disorder in the UK' funded by the Media Democracy Fund, the Ford Foundation and the Open Society Foundations
2. Sometimes referred to as 'big social data' (cf. Manovitch, 2011).
3. See for example Prime Minister David Cameron's speech in July 2015 announcing a new anti-extremism bill: http://www.independent.co.uk/news/uk/politics/david-cameron-extremism-speech-read-the-transcript-in-full-10401948.html
4. Much of this legislation has been replaced by the Investigatory Powers Act. For the police's own interpretation of guidelines at the time of research, see http://www.uk-osint.net/documents/ACPO-OSIW-&-Research.pdf
5. The research project also included a social media data analysis in which we emulated the practices of police to collect Twitter data in the lead up to protests in order to further examine potential challenges of predictive analytics and algorithmic definitions of extremism and threats. Results from that analysis can be reviewed in the project report at http://www.dcssproject.net/managing-threats-project-report/

References

Amoore L and Piotukh V (2016) Introduction. In: Amoore L and Piotukh V (eds) *Algorithmic Life: Calculative Devices in the Age of Big Data*. London; New York: Routledge, pp. 1–18.

Anderson DQC (2015) *A Question of Trust – Report of the Investigatory Powers Review*. Available at: https://terrorismlegislationreviewer.independent.gov.uk

Angwin J, Larson J, Mattu S, et al. (2016) Machine bias. *Propublica*, 23 May. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Aradou C and Blanke T (2015) The (Big) Data-security assemblage: knowledge and critique. *Big Data & Society* 2(2): 1–12.

Badger E (2012) How to catch a criminal with data. *From The Atlantic CityLab*, 14 March. Available at: http://www.citylab.com/tech/2012/03/how-catchcriminal-data/1477/

Barocas S (2014) Data mining and the discourse on discrimination. In: *Proceedings of the data ethics workshop, conference on knowledge discovery and data mining (KDD)*, New York, 24–27 August. Available at: https://dataethics.github.io/proceedings/DataMiningandtheDiscourseOnDiscrimination.pdf

Berry D (2011) The computational turn: Thinking about the digital humanities. *Culture Machine* 12: 1–22

boyd d and Crawford K (2012) Critical questions for big data. *Information, Communication & Society* 15(5): 662–679.

Dodd V (2014) Chief constable warns against 'drift towards police state'. *The Guardian*, 5 December. Available at: http://www.theguardian.com/uk-news/2014/dec/05/peter-fahy-police-state-warning

Edwards A (2015) Big Data, predictive machines and security: enthusiasts, critics and sceptics. *Discover Society*, 28 July. Available at: http://discoversociety.org/2015/07/28/big-data-predictive-machines-and-security-enthusiasts-critics-and-sceptics/

Elmer G and Opel A (2008) *Preempting Dissent: the Politics of an Inevitable Future*. Winnipeg, MB, Canada, ARP Books.

Elmer G, Langlois G and Redden J (eds) (2015) *Compromised Data: From Social Media to Big Data*. New York: Bloomsbury.

Frické M (2014) Big data and its epistemology. *Journal of the Association for Information Science and Technology* 66(4): 651–661.

Gillespie T (2011) Can an algorithm be wrong? Twitter Trends, the specter of censorship, and our faith in the algorithms around us. *Culture Digitally*, 19 October. Available at: http://culturedigitally.org/2011/10/can-an-algorithm-be-wrong/

Gillespie T (2014) The relevance of algorithms. In: Gillespie T, Boczkowski PJ and Foot KA (eds) *Media Technologies: Essays on Communication, Materiality, and Society*. Cambridge: MIT Press, pp. 167–193.

Gillham PF (2011) Securitizing America: strategic incapacitation and the policing of protest since the 11 September 2001 terrorist attacks. *Sociology Compass* 6(7): 636–652.

Halford S (2015) Big data and the politics of discipline. *Discover Society*, 30 July, 2015. Available at: http://discoversociety.org/2015/07/30/big-data-and-the-politics-of-discipline/

Her Majesty's Inspectorate of Constabulary (HMIC) (2011) The rules of engagement: a review of the August 2011 disorders. Available at . https://www.justiceinspectorates.gov.uk/hmic/media/a-review-of-the-august-2011-disorders-20111220.pdf

Hey T, Tansley S and Tolle K (eds.) (2009) *The Fourth Paradigm: Data-Intensive Scientific Discovery*. Redmond, WA: Microsoft Research.

Hildebrandt M (2013) Slaves to big data. Or are we? (IDO. Revista de Internet, Derecho y Politica (17)). Available at: http://journals.uoc.edu/index.php/idp/article/viewFile/n17-hildebrandt/n17-hildebrandt-en

Howard A (2012) Predictive data analytics is saving lives and taxpayer dollars in New York City. *O'Reilly Radar*, 26 June. Available at: http://radar.oreilly.com/2012/06/predictive-data-analytics-big-data-nyc.html

Jones C (2014) Predictive policing: mapping the future of policing? *Open Democracy*. Available at: https://www.opendemocracy.net/opensecurity/chris-jones/predictive-policing-mapping-future-of-policing

Kelling GL and Bratton W (1998) Declining crime rates: insiders' views of the New York City story. *Journal of Criminal Law and Criminology* 88(4): 1217–1232.

Kelly H (2014) Police embracing tech that predicts crimes. *CNN*, 26 May. Available at: http://edition.cnn.com/2012/07/09/tech/innovation/police-tech/

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

Koehn J (2012) Algorithmic crimefighting. *San Jose.com*, 22 February. Available at: http://www.sanjose.com/2012/02/22/sheriffs_office_fights_property_crimes_with_predictive_policing/

Lewis P and Evans R (2010) Peace campaigner, 85, classified by police as 'domestic extremist'. *The Guardian*, 25 June. Available at: https://www.theguardian.com/uk/2010/jun/25/peace-campaigner-classified-domestic-extremist

Lewis P, Evans R and Dodd V (2013) National police unit monitors 9,000 'domestic extremists'. *The Guardian*, 26 June. Available at: http://www.theguardian.com/uk/2013/jun/25/undercover-police-domestic-extremism-unit

Lubbers E (2015) Undercover research: corporate and police spying on activists. An introduction to activist intelligence as a new field of surveillance. *Surveillance & Society* 13(3/4): 338–353.

Mackenzie A (2007) Protocols and the irreducible traces of embodiment: the Viterbi algorithm and the mosaic of machine time. In: Hassan R and Purser RE (eds) *24/7: Time and Temporality in the Network Society*. Stanford, CA: Stanford University Press, pp. 89–106.

Manovitch L (2011) Trending: the promises and the challenges of big social data. In: Gold MK (ed.) *Debates in Digital Humanities*. Minneapolis, MI; London: University of Minnesota Press, pp. 460–475.

Massumi B (2015) *Ontopower: War, Powers, and the State of Perception*. Durham, NC; London: Duke University Press

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

Mohler GO, Short MB, Brantingham PJ, et al. (2011) Self-exciting point process modeling of crime. *Journal of the American Statistical Association* 106(493): 100–108.

National Police Chiefs' Council (NPCC) (2016) National domestic extremism and disorder intelligence unit. Available at: http://www.npcc.police.uk/NationalPolicing/NDEDIU/AboutNDEDIU.aspx

Pasquale F (2015) *The Black Box Society*. Cambridge, MA: Harvard University Press.

Peña Gangadharan SP, Eubanks V and Barocas S (eds) (2015) *Data and Discrimination: Collected Essays*. Open Technology Institute – New America. Available at: http://newamerica.org/downloads/OTI-Data-an-Discrimination-FINALsmall.pdf

Procter R, Crump J, Karstedt S, et al. (2013a) Reading the riots: what were the police doing on Twitter? *Policing and Society* 23(4): 413–436.

Procter R, Vis F and Voss A (2013b) Reading the riots on Twitter: methodological innovation for the analysis of Big Data. *International Journal of Social Research Methodology* 16(3): 197–214.

Quinn B (2015) City of London police put Occupy London on counter-terrorism presentation with al-Qaida. *The Guardian*, 19 July. Available at: http://www.theguardian.com/uk-news/2015/jul/19/occupy-london-counter-terrorism-presentation-al-qaida

Swain V (2013) Disruption policing: surveillance and the right to protest. *Open Democracy*. https://www.opendemocracy.net/opensecurity/val-swain/disruption-policing-surveillance-and-right-to-protest

Trottier D (2012) Policing social media. *Canadian Review of Sociology* 49(4): 411–425.

Trottier D (2015) Open source intelligence, social media and law enforcement: visions, constraints and critiques. *European Journal of Cultural Studies* 18(4–5): 530–547.

Vitale A (2006) From negotiated management to command and control: how the New York police department polices protests. *Policing and Society* 15(3): 283–304.

Wright P (2013) Meet Prism's little brother: Socmint. *Wired*, 26 June. Available at: http://www.wired.co.uk/news/archive/2013–;06/26/socmint

Author biographies

Lina Dencik is senior lecturer at Cardiff University's School of Journalism, Media and Cultural Studies where she serves as Director of MA Journalism, Media and Communication and Co-Director of the Data Justice Lab.

Arne Hintz is senior lecturer at Cardiff University's School of Journalism, Media and Cultural Studies where he serves as Director of MA Digital Media and Society and Co-Director of the Data Justice Lab.

Zoe Carey is a doctoral student in the Department of Sociology at The New School for Social Research.