

INTELLIGENT JUSTICE?

A discussion paper on the use of police intelligence data to inform offender management decisions

Rick Muir
Director
The Police Foundation
October 2020

THE
POLICE
FOUNDATION

The UK's policing think tank

1. Introduction

In July 2018 the then Justice Secretary David Gauke MP announced that new technology would be introduced to help tackle crime in prisons. Specifically, a digital categorisation tool would be developed by the Ministry of Justice that would draw on a wider pool of law enforcement data to inform the allocation of offenders to prisons. In a speech in November 2018 Mr Gauke framed this new use of big data in the prison system as part of a wider push to tackle organised criminal networks operating throughout the prison estate, saying:

“Crime not only affects prison staff and fellow prisoners, but reaches far beyond the prison gate. While offenders are rightly separated from society, prisons exist within communities. There is a direct link between crime on the wings and landings and crime in our towns and cities. Ensuring there is less crime in our prisons means less crime in communities.” (Gov.uk, 2018)

The digital categorisation tool, now known as the Digital Categorisation Service, received £1 million in investment as part of a wider package of £30 million to crack down on crime in prison. Although there is not a lot of information in the public domain about how the tool is currently operating, according to the Prison Reform Trust it was operating in nine prisons by March 2020 and was expected to be rolled out to the rest of the estate over the summer of this year (Harman, 2020).

The tool takes data from a range of (publicly unspecified) law enforcement databases to create a central “risk rating” for each prisoner. The old system that this technology replaces relies purely on offence type and sentence length to inform categorisation decisions, whereas the new tool should bring data such as police intelligence into consideration. According to the government this means that the risk a prisoner poses in terms of escape, violence or involvement in organised crime should be taken into account when deciding where they should be held. The Ministry of Justice press statement at the time of the launch suggested that 12 prolific criminals had been moved as a result of use of the tool in the pilot areas, disrupting their control over prison-based criminal networks (Ministry of Justice, 2018).

Since the launch of the tool, little has been published in the public domain regarding its operation. We do not know, for example, what sources of data are used

to inform categorisation decisions, nor the numbers of prisoners moved as a result. An investigation by the Bureau of Investigative Journalism has however raised concerns about how the tool may unfairly discriminate against Black and Minority Ethnic (BAME) prisoners (Black, 2019). According to Crofton Black the preliminary evaluation by the Ministry of Justice, obtained following a Freedom of Information request, concluded that there was no evidence that prisoners from BAME backgrounds were more likely than white prisoners to have their risk category raised. However, based on an analysis of the same figures, Black reports that 16 per cent of the non-white prisoners had their risk category raised, while just seven per cent of the white prisoners did.

Linked to this finding, there has been criticism of the use of police intelligence data to inform prisoner categorisation. Patrick Williams, a senior lecturer at Manchester Metropolitan University, told Black that *“Intelligence-informed categorisation will simply take police intelligence into the prison environment and may result in presenting BAME people as more risky to prison staff. This in turn will increase surveillance and offender management.”* (Black, 2019). As will be discussed below, in other contexts the police have been criticised for using intelligence data to inform risk assessments of suspects because of concerns about accuracy and bias.

The Police Foundation was asked by the Barrow Cadbury Trust to undertake a short study into the implications of using police intelligence data for these purposes. This short discussion paper is the result of that work. The paper is based on a review of relevant literature, alongside interviews with five police officers, one prison officer and a Ministry of Justice official. We were unsuccessful in our efforts to specifically discuss the digital categorisation tool with relevant government officials and so, as regards the operation and roll out of the tool, what is said below is based on what has already been put into the public domain.

The paper does three things. First, it puts this discussion in context by sketching out some of the wider considerations that are pertinent to the use of data analytics in the criminal justice system. Second, it focuses in detail on police intelligence, which it is assumed is a key data source for the prison categorisation tool. It describes what police intelligence data is, how it is collected, how it is assessed and the rules that exist around its wider dissemination. Third, it identifies three concerns that the Ministry of Justice

ought to address if it is to build confidence in the operation of the Digital Categorisation Service. Indeed, these are concerns that are relevant to any use of police intelligence data to inform offender management decisions.¹

2. Big data policing

The application of data analytics to policing means the acquisition, analysis and use of large volumes of digital data for policing purposes, such as the prevention and detection of crime. It holds out the prospect of the police becoming smarter at targeting their resources and more effective at managing suspects and offenders. In a 2018 report the Police Foundation demonstrated the real public value that could be generated across a range of public safety outcomes through the use of data-driven technology (Kearns and Muir 2018).

For example, data analytics can help the police better understand the risks posed by particular suspects so that they can make more informed decisions. It can also help to highlight crime hotspots and guide proactive police resource towards those areas with the highest levels of crime and harm. It holds out the prospect of more targeted and therefore more efficient and effective policing, which, it is hoped, will make communities safer.

However, police forces have also been criticised for their use of big data. The human rights advocacy group Liberty has highlighted four concerns:

- **Bias:** there is a concern that police data contains biases that, if worked upon by machine learning, will result in biased decision-making. Police data reflects police activity. Because members of BAME groups are disproportionately likely to be stopped or arrested by the police, relative to their presence in the general population, they are likely to be over-represented in police databases. Data analytics based on that source material will only reinforce those biases.
- **Privacy:** police acquisition, analysis and use of large volumes of personal data may mean an excessive degree of surveillance of individuals that breaches their right to privacy.

- **Human oversight:** the use of big data programmes can lead to “decision making by machine”, whereby even if a final decision is made by a police officer or other agent, those making such decisions come to rely on an algorithm and do not question its conclusions. This means that decisions which may have a very significant impact on an individual, such as whether they ought to be bailed or charged, may be made without the ethical and “common sense” checks that only a human decision-maker can provide.
- **Transparency:** reliance on artificial intelligence to inform decision-making can lack transparency, simply because those making decisions may not understand the basis on which automated systems are making their recommendations. Both technical complexity and proprietary considerations mean that the inner workings of algorithms are generally not accessible or subject to public scrutiny.

A number of police agencies have been criticised for their use of data to support “predictive policing”, both in the UK and internationally. Predictive policing software uses historic data to allocate police resource to areas where crimes are likely to take place, with the aim of preventing them. For example, in 2016 the Human Rights Data Analysis Group artificially reconstructed an existing predictive policing programme and applied it to drugs offences in the city of Oakland, California (Lum and Isaac, 2016). Using drugs crime data to direct police resources they found that the software would have sent officers almost exclusively to low income minority neighbourhoods. This was despite the fact that drug use was known from health data to be much more widespread across the city.

Outcomes like this arise because police data is not an objective reflection of crime and harm in society. Many crimes are not reported to the police. Many of the incidents logged on police systems reflect police decisions to prioritise certain types of crime or particular geographic areas. There is a significant risk of a crime data “feedback loop” whereby people and places become ever more disproportionately policed based on data that simply reflects existing practices.

Police agencies have also been using big data analytics to help assess the risks posed by individual suspects and here too they have been subject to criticism. For example, Durham Police has been criticised for its use of the Harm Assessment Risk Tool

¹ The paper focuses on the digital categorisation tool being rolled out in prisons, but of course police intelligence data may be used by other agencies. While the focus of this paper is the prison service some of its conclusions will have a wider relevance to the probation service and other agencies who may have some access to police intelligence data.

(HART), one of the first algorithmic models deployed in an operational capacity in UK policing. Developed in partnership with statistics experts at Cambridge University, it was designed to help custody officers make decisions when assessing an offender's risk of future offending and to do so shortly after an offender has been arrested by the police and while they sit at the initial gateway to the criminal justice system. The aim was to achieve more effective offender triage, get offenders on to the most effective path to desistance from committing crime, and therefore to help keep the public safe. The HART's use has been aimed specifically at offenders who were considered at moderate risk of re-offending and who were being considered for possible inclusion in the force's Checkpoint programme, an initiative designed to consider the root causes of offending associated with health and community issues and to offer a way of dealing with those offences out of court rather than by prosecution (Kearns and Muir, 2018).

Critics have argued that the data upon which these decisions are made is likely to contain biases and may therefore intensify disproportionate treatment for minority groups. For example, the model uses 34 predictors, with 29 taken from the detained person's offending behaviour plus age, gender, two forms of post code and "a count of intelligence reports related to the detained person". Liberty argues that the use of postcodes and socio-demographic data may simply reflect and then reinforce pre-existing biases in police data, particularly around race. The use of police intelligence data may be similarly problematic, because it will reflect existing police activity, which may itself be biased towards policing certain crime types and communities. Liberty also expressed concerns about accuracy, pointing out in an independent evaluation that the model's predictive accuracy was assessed to be just 63 per cent (Couchman, 2019).

Another example of police intelligence data being used to inform risk assessment decisions is the Metropolitan Police Service's Gangs Violence Matrix. The so-called Gangs Matrix is a database which contains information on suspected gang members, launched in 2012 following the riots across England the previous summer. It has been used as a risk assessment tool by the police to assess suspected gang members and grade them according to the risk of violence they pose.

In October 2017 there were 3,806 people on the database, with only five per cent of these rated as the highest risk and most marked as low risk. The Mayor's Office for Policing and Crime, in a 2018 review of the Gangs Matrix, found that 80 per cent of those on the Matrix were of Black African-Caribbean ethnicity. These levels are disproportionate not only of course to the proportion of black people in the London population but also of those who offend and are victimised. MOPAC found that people of Black African-Caribbean ethnicity made up 80 per cent of those on the Matrix but only (all London figures) 16 per cent of the population, 27 per cent of those under the age of 25, 32 per cent of violent offenders, 46 per cent of those committing knife crime offences, 63 per cent of those flagged as involved in gang violence and 71 per cent of those committing knife homicide (MOPAC 2018). Similarly, for victimisation those of Black African-Caribbean ethnicity make up 23 per cent of victims and 30 per cent of victims of serious youth violence.

Amnesty International criticised the Gangs Matrix for using an ill-defined concept of "gangs", which has been applied inconsistently and for including and ranking individuals in inconsistent ways and with little oversight. This is important because of the implications for a young person of being included on a database which can be shared with other statutory agencies, including housing and education providers. Amnesty also argued that, at a conceptual level, the way in which the matrix is framed conflates elements of urban youth culture with a propensity to commit violent crime and that this conflation is heavily racialised (Amnesty International 2018).

Following this report, the Information Commissioners Office (ICO) conducted an investigation which led it to conclude that the MPS had breached data protection legislation in its operation of the Gangs Matrix. Specifically, the ICO concluded that the Matrix does not clearly distinguish between victims and perpetrators and is inconsistently managed across London boroughs. "Blanket sharing" of names with third parties was also criticised, particularly where there is a lack of distinction between high and low risk, potentially leading to disproportionate actions by third parties who include other public service providers. The ICO also concluded that data protection laws had been breached by the MPS and it issued an enforcement notice, to which the MPS has since been responding.

In December 2019 the Mayor's Office for Policing and Crime completed a review of the Gangs Matrix and concluded that *"the representation of young, black males on the Matrix is disproportionate to their likelihood of criminality"* (MOPAC, 2018). It did however also find that inclusion on the Matrix did result in less offending and victimisation and concluded that, subject to an overhaul of how it works, it remained a legitimate policing tool (ibid).

So, we know that while the era of big data creates opportunities for policing to better prevent and detect crime, it also creates risk and challenge, in particular with regard to bias, privacy, oversight and transparency. In the next section we explore in greater detail the nature, acquisition, analysis and use of police intelligence data, so that we can then move on in the final section to discuss what all of this means for the potential use of this data to inform offender management decisions.

3. Police intelligence data

3.1 What is police intelligence?

For use within a law enforcement context Innes and Sheptycki (2004) define intelligence as:

"information that has been subjected to some form of analysis and evaluation with the intention of informing future acts of social control."

Within that broad concept of intelligence, it is important to distinguish between a number of sub-categories. First, intelligence is not the same thing as information. As Innes and Sheptycki (2004) point out, information consists of the raw data from which intelligence can then be produced.

Second, intelligence does not just mean information gleaned by covert means, whether by undercover police work or work by the security services. While in those contexts all information gleaned by covert means tends to be described as intelligence, police intelligence encompasses information taken from open sources as well.

Third, following the introduction of the National Intelligence Model in the English and Welsh police service in 2000, a distinction was made operationally between tactical and strategic intelligence. According to Innes and Sheptycki (2004):

"Tactical intelligence refers to the use of data to inform specific, bounded, and targeted interventions against a nominated problem, whereas strategic intelligence consists of data providing a longer-term vision of the contexts and problems relevant to police practice."

Innes and Sheptycki (2004) conclude by distinguishing between four types of intelligence that are typically used within modern policing:

- Criminal intelligence is data that provide some understanding about the identity and activities of a particular nominated individual or group of individuals. This data is sourced from informants embedded in the "criminal milieu" or from members of the public. It is this form of intelligence that is most relevant to our discussion of the new digital categorisation tool.
- Crime intelligence is data which provides insight in relation to particular types of crime, crime hot spots, or crime series, which is most often based upon analysis of police and partner agency data.
- Community intelligence is information provided by "ordinary" members of the public and tends to refer to the "local" problems that they view as significant.
- Contextual intelligence is information about the wider social forces that shape the context in which the police are operating. This is gathered from large data sets so that the police can plan for the future.

3.2 Intelligence-led policing

While the police have always used intelligence to tackle crime, at the turn of the century "intelligence-led policing" was adopted as a proactive approach to crime prevention and detection in England and Wales. Intelligence-led policing has been characterised as an effort, alongside other approaches such as problem oriented policing and community policing, to move beyond reactive "fire brigade policing", in which the police simply respond to and attempt to cope with the "here and now" (Tilley 2008). As Tilley (2008) states:

"Intelligence-led policing draws on the notion that the police can and do know a great deal about offending patterns. Intelligence-led policing involves effectively sourcing, assembling and analysing 'intelligence' about criminals and their activities better to disrupt their offending, by targeting enforcement and patrol where it can be expected to yield the highest dividends."

This more proactive approach became police service policy with the adoption of the National Intelligence Model (NIM) in 2000. The NIM was developed by the National Criminal Intelligence Service (NCIS) on behalf of the then Association of Chief Police Officers (ACPO). It is still supported by the Home Office, HMICFRS and the College of Policing and continues to operate across all 43 territorial police forces.

The NIM was associated with efforts to make policing more efficient and effective, which dovetailed with the wider New Public Management (NPM) agenda of the 1990s and 2000s and was facilitated with the roll out of improved police IT systems. It has also been associated, as Innes and Sheptycki (2004) point out, with a move away from prosecution-oriented policing towards the notion of disruption as a key outcome of investigative work. So, rather than seeing the aim as necessarily to get a suspect before the courts, intelligence-led policing particularly in the serious and organised crime space has come to support the on-going disruption of criminal enterprises, so as to make it difficult for criminals to operate.

The adoption of the NIM led to major changes to police decision-making structures, organised around the distinction made above between tactical and strategic intelligence. According to the College of Policing Authorised Professional Practice in Intelligence Management (College of Policing, 2019), intelligence is mainstreamed into police decision-making within a police force in the following way. Each force should have a chief officer responsible for delivering intelligence-led policing and for developing the force's intelligence capability. A Strategic Tasking and Coordination Group of senior managers sets the Control Strategy for the force containing the operational priorities for crime prevention, intelligence collection and enforcement. It also sets the Strategic Intelligence Requirement which identifies the gaps in knowledge that intelligence collection should aim to fill. Its decisions are informed by the Strategic Assessment, which is an intelligence product setting out the current and long-term issues facing a police force or Basic Command Unit (BCU) (College of Policing, 2019).

The strategic priorities in the Control Strategy are then operationalised by the Tactical Tasking and Coordination Group made up of operational managers, normally at Basic Command Unit (BCU) level or in smaller forces at force level. This group develops the tactical plans to implement the priorities set in the Control Strategy, based on the recommendations of their Intelligence Unit. Its deliberations are informed by the following intelligence products: 1) tactical assessments which

define problems and identify subjects, recommend tactical options, review intelligence requirements, review performance and identify emerging patterns and trends; 2) subject profiles which set out intelligence on a particular suspect or victim and 3) problem profiles, which provide a greater understanding of established and emerging crime or incident series, priority locations or other identified high-risk issues.

3.3 Criminal intelligence data

Criminal intelligence on individual suspects and victims is collected routinely by the police. The legal basis for its collection is that it "contributes to a policing purpose", which includes protecting life and property, preserving order, preventing the commission of offences and bringing offenders to justice (College of Policing, 2019).

This information is collected by police officers in the course of their work, by members of the public volunteering information or by "tasked information". This latter channel involves the proactive collection of intelligence via a mixture of open and closed sources, including internal or external databases, CCTV, covert human intelligence sources (CHIS) and automated number plate recognition (ANPR) systems.

New information is submitted by police officers as an Intelligence Report to their force Intelligence Unit. In submitting this report officers are asked to make an assessment as to the reliability of the source, which is important for an assessment of the credibility of the information and in determining what tactical options might follow.

The source is graded as reliable where the source is thought to be competent and veracious; it is graded as untested when the source is new and where reliability cannot be assumed; and it is graded as unreliable where there are reasons to question the competence, authenticity, trustworthiness or motive of the source. The information's reliability is assessed based on whether the information was gleaned first-hand or indirectly, whether it can be corroborated by information from other sources and indeed whether the information is suspected to be false (College of Policing 2019).

When an Intelligence Report is received by the force Intelligence Unit it is then further assessed by specialist intelligence officers. They will assess for any risks and duty of care issues, the value of the piece of intelligence, how accurate it is, any considerations regarding further research, whether it meets data standards and whether it can be shared more widely and with what conditions.

Intelligence data on individual suspects is shared with other police forces via the Police National Database (PND), which was brought in following the Richard Inquiry into the Soham murders. The then Sir Michael (now Lord) Richard found that police intelligence was not being properly shared between forces and the PND was established to fill this gap, supplementing the Police National Computer which houses criminal record information, with links to fingerprints and DNA data, driver and vehicle records and information on lost and stolen property. The Home Office is in the process of combining both databases and others into the single National Law Enforcement Data Service (NLEDS).

Police criminal intelligence data can be shared outside of the police service on the following grounds: if this sharing serves a policing purpose (as described above), if local protocols are in place and if the person to which it is sent has a legitimate need to receive it. Sharing with other European Economic Area law enforcement agencies does not require any additional Intelligence Report assessment. Sharing with non-EEA law enforcement bodies must be subject to an individual risk assessment. In some cases, sharing is only permitted if certain conditions are met. The intelligence is often sanitised, in particular to protect the identity of sources (College of Policing, 2019).

3.4 Intelligence sharing with prisons

The Prison Service has its own intelligence framework, issued in October 2019 (HMPPS, 2019). It states that intelligence is collected by the prison service for a variety of purposes, including:

“to support offender management, for the prevention and detection of crime, preserving order and discipline in establishments, management of risk and prevention of harm, and any duty or responsibility arising from common or statute law.”

As with police intelligence, intelligence collected in prisons goes through a process of assessment by specialist Prison Intelligence Units before being entered on the national intelligence system, Mercury.² Each prison must complete a monthly tactical assessment,

² Intelligence may also be entered on ViSOR the Dangerous Persons Database. This is a management tool used by UK law enforcement, the National Offender Management Service (including the Prison Service) along with a wide range of other agencies, to manage, Registerable Sexual Offenders, Other Sexual Offenders, Violent Offenders, Dangerous Offenders, Registerable Terrorist Offenders, Registerable Violent Offenders and Potentially Dangerous Persons as part of MAPPA (Multi-Agency Public Protection Arrangements).

identifying threat priorities, emerging and developing threats, persons of interest and concern, and intelligence gaps. This is submitted to the Regional Intelligence Unit within HM Prison and Probation Service (HMPPS).

HMPPS is able to share intelligence with law enforcement agencies under the Offender Management Act 2007 and the Data Protection Act 2018. Direct requests by the police for information regarding named individuals is managed through the HMPPS Operational Partnership Team (OPT).

Prison Intelligence Officers (PIOs) are police officers embedded within prisons and responsible for managing prison intelligence collection by the police. They act as a single point of contact for the police into the prison security unit. They oversee intelligence requests from law enforcement agencies and liaise with the prison security unit to facilitate access to information on prisoners.

Among other things PIOs can provide police forces with information on offender sentence planning, movement and release information, updates on organised crime networks in prison and prison intelligence that can form part of a subject profile.

4. The implications of using police intelligence data to inform prisoner allocation decisions

As we have seen there is already considerable and routine sharing of intelligence between the police and the prison service, and vice versa. However the roll out of the new digital categorisation tool takes this further by using a wider range of data, including (on the basis of what has been put in the public domain) police intelligence data, to guide decisions as to where prisoners should be located. The aim is to reduce crime by disrupting organised criminal networks operating within prisons.

Given the lack of information about how the tool is operating we cannot come to firm conclusions as to its impact. For example, we do not know:

- What law enforcement data is being fed into the tool.
- If, as has been indicated in the media, police intelligence data is being used, we do not know what thresholds have been set for inclusion. All Intelligence Reports are given handling codes so that the

reliability of the intelligence can be easily understood upon dissemination, but we do not know how this is being applied in the operation of the tool.

- Any systemic outcomes data, such as on how many prisoners have had their risk rating raised, nor the characteristics of those prisoners, beyond what has been published by Crofton Black of the Bureau of Investigative Journalism (see Black, 2019).

With these qualifications in mind, we set out below three concerns about the use of police intelligence data as a source for the digital categorisation tool:

First, there is a concern about the accuracy of intelligence data. If an algorithm is using intelligence data as an input, then the information used will inherently contain inaccuracies. Intelligence is not objective data, impartially submitted. Intelligence databases inevitably contain opinions, lies and error. This information is useful for police investigative purposes, but as our interviewees stressed, the information must always be seen in context. So, for example, a police officer may record information they know to be a lie so long as they record alongside it that it is likely to be a lie. In some cases, the significance of the entry may lie in the contextual information that sits alongside it rather than in the entry itself. Indeed, one of the ICO's concerns about how the London Gangs Matrix operated was the sharing of information with third parties with insufficient contextual information alongside.

The key insight here is that if an algorithm is using intelligence data as an input then its inputs will not reflect proven facts about the world. That is not a problem for police intelligence whose purpose is to help the police in their investigative work. There may however be dangers once that data is disseminated more widely and used for other purposes. This risk can be mitigated to some extent by handling codes which provide an assessment as to the reliability of the intelligence. However, in the case of the categorisation tool we do not know what threshold has been set for the inclusion of data in helping to determine a prisoner's risk rating.

The problem of inaccuracy is compounded by concerns about the quality and consistency of intelligence assessment by the police. One interviewee told us that most of the training that police officers receive on intelligence management comes in the form of

e-learning packages, which tend to be completed in a tick box fashion, without sufficient learner engagement. This interviewee told us that in order to properly understand how to gather intelligence fairly, submit it well and proactively use it to inform your work you have to engage properly and take the time to teach yourself. As a result, we were told, the quality of intelligence submissions is highly variable.

Another police interviewee told us that her training was purely theoretical and left her unsure as to what was intelligence and what was just information. She found herself learning from colleagues as much as from formal training, but she told us *"people have different opinions, some people would put absolutely anything on."*

Second, there is a concern about bias. As we have seen in the aggregate, police intelligence data, and indeed most police collected data, reflects police activity. It is in that context that the question of disproportionality and racial bias arises. Police interviewees told us that intelligence gathering is directed by police priorities which vary over time and are subject to wider public and political pressures. The information held on individual suspects will reflect the areas and crime types the police have decided to focus upon, and this may be one explanation for racial disproportionality (although the causes of disproportionality in police data and activity are complex and much debated).

Third, as with all applications of big data analytics for policing purposes, transparency is key to sustaining public confidence. In this particular case there is far too little in the public domain regarding how the tool is operating. Given its implications for the management of individual suspects, this is far from desirable. The content of the much of the data itself is of course inappropriate for sharing beyond law enforcement agencies. However, it should not put national security or individual sources at risk simply to lay out the types of data being used as inputs into the tool and what safeguards have been introduced to deal with the issues highlighted above.

Transparency ought to extend to regular publication of the outcomes of the new tool to allow for scrutiny (by parliament or the prisons inspectorate) of any emerging patterns of bias, or any evidence relating to the ability of prisoners to progress through the system and ultimately to be released.

5. Conclusion

We do not dispute the desirability of the government's objective in developing the digital categorisation tool. The aim is to disrupt organised criminal networks in prison, whose activities cause harm and suffering way beyond the prison gate. Nor do we dispute the need for a more nuanced assessment of the risk posed by individual prisoners, so that this can be properly taken into account when allocating them to particular prisons.

Nevertheless, the use of an automated categorisation tool which includes police intelligence as a key input raises a number of concerns that the Ministry of Justice ought to address. Police intelligence does not pretend to be an accurate representation of the world and indeed there are concerns about the consistency of collection and assessment around the country. In addition, police intelligence data will reflect police activity and may contain biases that could exacerbate the problem of racial disproportionality in the criminal justice system.

Finally, the lack of transparency around the operation of the tool is concerning. Data analytics has an important role to play in the future of law enforcement, in particular in risk assessments of suspects, offenders and victims. But if there is to be public confidence in the application of such tools it is important that how they operate and the outcomes they generate are subject to public scrutiny.

References

Amnesty International (2018) *Trapped in the Matrix. Secrecy, stigma and bias in the Met's Gangs Database*. London: Amnesty International UK. Available at: <<https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf>>

Black, C. (2019) The Ministry of Justice's prisoner risk algorithm could program in racism. *New Statesman*, [online] 14 November <<https://www.newstatesman.com/politics/uk/2019/11/ministry-justices-prisoner-risk-algorithm-could-program-racism>>

College of Policing (2019) *Authorised Professional Practice: Intelligence Management*. [online]. Available at: <<https://www.app.college.police.uk/app-content/intelligence-management/?s=>>

Couchman, H. (2019) *Policing By Machine*. London: Liberty. Available at: <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf>

Gov.uk (2018) *Safer prisons, safer streets* [online]. Available at: <<https://www.gov.uk/government/speeches/safer-prisons-safer-streets>>

HMPPS (2019) *Intelligence Collection, Analysis and Dissemination Policy Framework*. [pdf]. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/843803/intelligence-collection-management-dissemination-pf-31-oct-2019.pdf>

Harman, R. (2020) Security categorisation. *Inside Time*, [online] 31 March. Available at: <<https://insidetime.org/security-categorisation/>>

Innes, M. and Sheptycki, J.W.E (2004) From Detection To Disruption: Intelligence And The Changing Logic Of Police Crime Control In The United Kingdom. *International Criminal Justice Review* 4(1), pp.1-24.

Kearns, I. and Muir, R. (2018) *Data Driven Policing*. London: The Police Foundation. Available at: <http://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/data_driven_policing_final.pdf>

Lum, K. and Isaac, W. (2016) To predict and serve?. *Significance* 13(5), pp.14-19.

Ministry of Justice (2018) *Justice Secretary launches fresh crackdown on crime in prison* [online]. Available at: <<https://www.gov.uk/government/news/justice-secretary-launches-fresh-crackdown-on-crime-in-prison>>

MOPAC (2018) *Review of the Metropolitan Police Service Gangs Matrix*. London: MOPAC. Available at: <https://www.london.gov.uk/sites/default/files/gangs_matrix_review_-_final.pdf>

Tilley, N. (2008) Modern approaches to policing: community, problem oriented and intelligence led policing in T. Newburn, (ed) *The Handbook of Policing*. London: Willan Publishing.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. New York: The New Press.

© 2020: The Police Foundation

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without the prior permission of The Police Foundation.

Enquiries concerning reproduction should be sent to The Police Foundation.

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE
POLICE
FOUNDATION

The UK's policing think tank