Machine learning predictive algorithms and the policing of future crimes: governance and oversight

In *Policing and Artificial Intelligence* (Dr John L.M. McDaniel and Prof Ken Pease OBE, eds., Routledge, Forthcoming 2020)

Alexander Babuta* and Marion Oswald**[1]

Both authors have contributed significantly and equally to the writing of this chapter

Abstract: This chapter focuses upon machine learning algorithms within police decision-making in England and Wales, specifically in relation to predictive analytics. It first reviews the state of the art regarding the implementation of algorithmic tools underpinned by machine learning to aid police decision-making, and notes the impact of austerity as a driver for the development of such tools. We discuss how what could be called 'Austerity AI' is often linked to the prevention and public protection common law duties and functions of the police, a broad and imprecise legal base that the ECtHR in *Catt* found less than satisfactory. The potential implications of these tools for appropriate application of discretion within policing, as well as their potential impact on individual rights are then considered. Finally, existing and recommended governance and oversight processes, including those designed to facilitate trials of emerging technologies, are reviewed, and proposals made for statutory clarification of policing functions and duties, thus providing a clearer framework against which proposals for new AI development can be assessed.

Police use of algorithms in England and Wales

UK police forces collect a vast amount of digital data from many different sources, but have historically lacked the technological capabilities needed to analyse this data to improve effectiveness and efficiency (Babuta, 2017). However, as data continues to evolve in volume and complexity, there is increasing interest in the use of data analytics and machine learning tools to improve decision-making and service provision within policing in England Wales (The Law Society of England and Wales, 2019). This follows the trend already seen in the United States, where 'predictive policing' algorithms have been gaining traction for some years (Bachner, 2013; Joh, 2014; Ferguson, 2017). While the statistical methods underpinning these technologies have existed for many years, significant advances in computing power and the availability of large volumes of digital data have now enabled rich insights to be rapidly extracted from large, disparate data sets.

While often presented as novel and futuristic, predictive analytics was first implemented in UK policing more than ten years ago, but traditionally focussed on spatial analysis of past crime data, to predict locations where crime is most likely to occur in the near future (Bowers, Johnson and Pease, 2004; Johnson, 2008; Johnson et al., 2007). While various field trials have shown this technology to be more likely to predict the location of future crime than non-algorithmic methods (Mohler et al., 2015), the use of these tools has so far been limited and localised to individual forces: responses to Freedom of Information requests suggest that 12 (out of 45) UK police forces are currently using, trialling, planning to use or trial predictive mapping software, or have done so in the past few years (Liberty, 2019). Numerous bodies that have scrutinised the police's use of technology have urged forces to make more effective use of such tools to better direct operational activity at the local level (HMIC, 2017; London Assembly, Budget and Performance Committee, 2013; Europol, 2017). Police

[1] *Royal United Services Institute **University of Northumbria

forces' apparent disinclination to deploy this technology on a wider scale could be partly due to an absence of authorised professional guidance, leading to a lack of clarity over how to address legal and ethical concerns, as well as concerns regarding public and media opposition.

More recently, research has focussed on developing algorithms to support risk assessment and resource prioritisation related to *individuals.* Perhaps the most widely publicised example of such a tool is Durham Constabulary's Harm Assessment Risk Tool (HART), a machine learning algorithm that assigns individuals 'risk scores' corresponding to their predicted likelihood to reoffend (Oswald et al, 2018). A number of other notable initiatives are underway. West Midlands Police has created its own internal Data Analytics Lab. In parallel, a data ethics committee, the first of its kind within UK policing, was established to advise the Chief Constable and Police and Crime Commissioner (PCC) on the police force's data analytics projects. Avon and Somerset Constabulary uses predictive risk models to assess a range of factors, including likelihood of re-offending, likelihood of victimisation or vulnerability, and likelihood of committing a range of specific offences (Liberty, 2019). Through an app on their mobile and tablet devices, neighbourhood officers can instantly access the 'risk profile' for each offender registered in the force area, which are re-calculated on a daily basis. Hampshire Constabulary is also currently developing a machine learning tool to predict risk of domestic violence offending (Terzis, Oswald and Rinik, 2019).

While police forces have only recently implemented statistical ('actuarial') offender assessment tools, elsewhere in the criminal justice system, similar technology has been used for many years. As Craig and Beech describe, 'in North America and the United Kingdom, actuarial risk assessment has permeated the entire criminal justice system.' (Craig and Beech, 2009). Some of these tools are purely actuarial methods that do not incorporate any human judgement, while others encourage the assessor to use the output of the algorithmic prediction in combination with their professional judgement to arrive at an overall assessment. The most commonly used tools are the Offender Assessment System (OASys), the national risk and needs assessment tool for adult offenders, used by HM Prison and Probation Service (HMPPS) to measure individuals' likelihood of reoffending and to develop individual risk management plans (Howard, Clark and Garnham, 2006; National Offender Management Service, 2015) and the Offender Group Reconviction Scale (OGRS), an actuarial tool used by HMPPS to assess reoffending risk at pre-sentence court report stage, post-sentence, or for offenders who receive out of court disposals (Copas and Marshall, 1998; Howard et al., 2009; National Offender Management Service, 2015). Various other systems have been developed for specific purposes, such as risk assessment of young offenders (Youth Justice Board, 2000; Wilson and Hinks, 2011), violent offenders (Harry, Rice and Quinsey, 1993; Quinsey et al., 2006) and sexual offenders (Thornton et al., 2003; Craig, Beech and Brown, 2006). In many cases, these statistical scoring systems are not used for risk management purposes *per se*, but for 'screening', i.e. to identify a smaller subset of a given population of offenders who require further, more detailed risk assessment. However, the legal and ethical implications of using such statistical scoring systems in an operational policing environment are considerably different to when they are used for offender management purposes or in a clinical setting.

More generally, recent years have seen a proliferation in the use of algorithmic methods across the UK public sector. It is beyond the scope of this chapter to discuss these projects in any detail, however, the reader is directed to a recent report on the use of data scoring in public services published by Cardiff University's Data Justice Lab (Dencik et al., 2018; Jansen, 2019). It is important to note that there is a lack of reliable research demonstrating the potential benefits and 'predictive performance' of such data scoring tools. In the specific context of offender risk assessment, it has been argued that the performance of statistical methods has been significantly overstated, and that they are of little use in identifying the specific nature and causes of risk, or

measures that can be taken to reduce that risk (Cooke and Michie, 2012; Hart, Michie and Cooke, 2007; Webster, Haque and Hucker, 2013; Douglas, Yeomans and Boer, 2005). The debate is ongoing.

Much commentary has highlighted potential risks and issues regarding the introduction of AI and machine learning into police decision-making, particularly relating to the impact on individual rights (Liberty, 2019; Richardson et al., 2019; Moses and Chan, 2018; Lynskey, 2019). There tends to be a divide between those focused upon strengths and opportunities of data science and those who stress the risks and issues. Within the policing context, the authors' previous research has drawn attention to the limited evidence base on the efficacy and efficiency of different systems, their cost-effectiveness, their impact on individual rights and the extent to which they serve valid policing aims (Babuta, Oswald and Rinik, 2018; Babuta and Oswald, 2019). Meijer and Wessels argue for more research into how predictive models work in practice (to see if drawbacks actually occur) (Meijer and Wessels, 2019), and a recent US report on predictive policing by the 'Partnership on AI' (an organisation bringing together for-profit and non-for-profit bodies working on AI) found that more research is required on how data-enabled risk assessment tools inform human decisions, in order to determine what forms of training will support principled and informed application of these tools, and where gaps exist in current practice (Partnership on AI, 2019). It is important to note that the concerns that have been raised regarding the risks of implementing 'predictive policing' tools are largely based on research conducted in the US, and there is a lack of sufficient evidence to demonstrate the extent to which these concerns are applicable to the UK policing context.

In addition to the common law, a number of legal frameworks within the law of England and Wales are applicable to the development and deployment of AI in UK policing. While this chapter cannot do justice to them all, it will include comment in particular upon obligations pursuant to the European Convention on Human Rights, taking effect through s6 Human Rights Act 1998, and administrative law principles applicable to lawful public sector decision-making (Oswald, 2018; Grace, 2019; Cobbe, 2018). These legal frameworks are primarily principles-based, meaning that often difficult context-specific judgements are required on a case-by-case basis regarding such issues as the justification and relevance of data inputs, and the necessity and proportionality both of the data analysis and the way in which the output is then used. Furthermore, the lack of guidance frameworks regarding methods of 'testing' these technologies, particularly within operational environments (Babuta, Oswald and Rinik, 2018; Fussey and Murray, 2019), and the absence of clear scientific standards by which to judge the validity and fairness of the outputs (Hildebrandt, 2018; Oswald, 2019), add considerably to the challenge. In the absence of clear organisational guidelines and codes of practice, it may be difficult for police decision-makers to assess whether the development and deployment of a particular algorithmic tool meets the legal requirements of the various frameworks mentioned above.

In the following section, we review the extent to which predictive assessments supported by machine learning connect with the public protection functions and duties of the police under common law.

Functions of the police in England and Wales under the common law

The operational independence of the police in upholding the law (*Fisher v The Mayor of Oldham* 143 LTR 281), including as regards the deployment of resources and discretion to investigate, is said to be a fundamental principle of policing in England and Wales (The Policing Protocol Order, 2011). A chief constable holds office under the Crown, and is accountable 'to the law' for the exercise of police powers (The Policing Protocol Order, 2011). Under the Police Reform and Social Responsibility Act 2011 (Schedule 2), a chief constable 'may do anything which is calculated to facilitate, or is conducive or incidental to, the exercise of the functions of chief constable.' In order

to decide whether particular information acquisition or data analysis can be regarded as incidental or consequential, the functions of a chief constable need to be understood. But where do we find these functions, or indeed of any constable within a police force of England and Wales? Despite the raft of legislation since the 1980s regulating various aspects of police activity, the underlying legal authority of the office of constable in England and Wales still stems from the common law, as does the constable's duty to maintain the Queen's Peace without fear or favour (The Policing Protocol Order, 2011). 'Police constables owe the public a common law duty to prevent and detect crime. That duty reflects a corresponding common law power to take steps in order to prevent and detect crime' *(R (Bridges) v Chief Constable of the South Wales Police* [2019] EWHC 2341 (Admin)). This contrasts with the UK intelligence agencies and the National Crime Agency, the functions of which are now defined in statute (Security Service Act 1989; Intelligence Services Act 1994; Crime and Courts Act 2013) and the statutory duties of constables within the police services of Northern Ireland and Scotland (Police and Fire Reform (Scotland) Act 2012; Police (Northern Ireland) Act 2000).

The 'Peace' in common law, fundamental to the functions of the English and Welsh police, has traditionally been linked with rioters and other 'barators' (Justices of the Peace Act 1361) although the concept relates more widely to 'public quietness and tranquillity, and the entitlement of every citizen to go about his or her lawful business without interference from malevolent forces' (Lord Judge, 2011). Police duties and other powers related to the breach of the peace are there to fill in the gap left by statutory powers of arrest relevant only to defined crimes, powers which Fenwick has described as 'immensely broad and bewilderingly imprecise' (Fenwick, 2009).

This is not to say that general police powers, responsibilities and particular areas of focus (such as public order) are not subject to a plethora of definitions, statutory requirements, codes of practice and other guidance regulating intrusive and coercive powers, use of data, out of court disposals, formulation of crime and disorder reduction strategies, positive obligations under Articles 2 and 3 ECHR, and subjecting policing activities to regulatory and political oversight.[i] While much of the policing landscape is heavily regulated by statute (thus significantly limiting the role of common law), the fundamental question of what the police in England and Wales are there to do – their *function* – still falls within the remit of the common law, and how this is achieved is left to a great extent to the discretion of the Chief constable, accountable to the common law, by way of judicial review against public law and human rights principles. Where there are gaps in statute that are not explicitly accounted for within existing legal frameworks – as could be argued in the case of new technologies such as artificial intelligence and 'predictive policing' – the onus rests on the force to justify such activity as legitimate for carrying out the function of the police in accordance with the common law.

This approach has consequences. The overarching duty to uphold the law and protect the Peace within the common law permits a degree of flexibility and adaptability, both as regards prioritisation and deployment of resources, and in respect of what preserving the Peace might require at any given time. While in the past, measures to tackle rioters, rebels and outlaws on the highway were likely the priority, today the police may be more concerned with gangs, anti-social behaviour, mental health and domestic abuse, as activities that may threaten 'the entitlement of every citizen to go about his or her lawful business without interference from malevolent forces' but may not justify a 'full' criminal justice response. Such duties may overlap with obligations imposed by article 2 of the ECHR which can imply a positive obligation to take preventative operational measures to protect a person whose life is at risk (*Osman v United Kingdom* [1998] 29 EHRR 245), such as a victim or witness to a crime, thus emphasising the importance of police risk assessments and the policy that informs them (*LXD v The Chief constable of Merseyside Police* [2019] EWHC 1685 (Admin)). Furthermore, circumstances may arise when priorities conflict. Enforcement of the law may, for instance, be

incompatible with the maintenance of order (Police Foundation and Policy Studies Institute, 1996). The common law allows the chief constable the discretion to balance prevention and detection of crime, and maintaining the Peace.

We might look to the Association of Chief Police Officers (ACPO)[ii] Statement of Mission and Values (2011) as the clearest modern explanation of what the police themselves think they are there to do. This sets out that:

> 'The mission of the police is to make communities safer by upholding the law fairly and firmly; preventing crime and antisocial behaviour; keeping the peace; protecting and reassuring communities; investigating crime and bringing offenders to justice.'

No single activity is favoured, thus allowing the adaptation of priorities as circumstances and demands dictate. Linked with the Statement of Mission and Values is the police officer's oath of attestation which includes a commitment to 'cause the peace to be kept and preserved and prevent all Offences against people and property' (College of Policing), indicating the importance of the Peace, and the prominence given to the preventative aspect of policing. This is also reflected in the Peelian Principles of policing by consent: Principle 1 'The basic mission for which the police exist is to prevent crime and disorder'; Principle 9 'The test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with it' (College of Policing, Code of Ethics Reading List).

The very flexibility of the police's functions can however cause uncertainty and dispute. Millie argues that police officers 'clearly do not intervene in "every kind of emergency"; however their remit has grown to such an extent that what is regarded as legitimate police activity is perhaps too wide.' (Millie, 2013, pp. 82-93). Millie lists a wide range of activities in his article: 'crime fighting, crime reduction, dealing with anti-social behaviour, tackling terrorism, public reassurance, traffic duties, immigration control, schools work, offender management, event security, disaster management, making people feel safer' (Millie, 2013). This has implications regarding the 'necessity analysis' of deploying new technology for a specific policing purpose, if such an analysis is founded on a subjective interpretation of what constitutes 'legitimate policing activity'. In their review of the National Analytics Solution, (a project to trial predictive analytics techniques for policing involving a number of major police forces), the Alan Turing Institute Data Ethics Group and the Independent Digital Ethics Panel for Policing concluded that:

> 'We see the NAS as moving law enforcement away from its traditional crime-related role and into wider and deeper aspects of social and public policy. This move requires explanation, justification and legitimation, especially where the ethical dimensions and principles of such policing roles are not well established. The NAS can be viewed as a charter for significant broadening of policy and governance. This would be a significant change with profound ethical, institutional and policy implications.' (The Alan Turing Institute Data Ethics Group and the Independent Digital Ethics Panel for Policing, 2017)

The NAS project team responded that they did not believe that the above comment reflected the modern police service:

> 'While the core function of the Police is the prevention and detection of crime there are numerous areas where we invest resource not directly linked to this such as – inter alia - locating missing persons, dealing with people in crisis with mental health issues (often as a joint team with health services), road traffic accidents including fatalities where there is no

element of criminal activity, dealing with the homeless, responding to suicide, domestic abuse where there is no recordable crime and dealing with anti-social behaviour issues that do not constitute crime but nevertheless have the ability to have a significant impact on the quality of life of the public affected by them.' (National Analytics Solution project team, 2018).

The preventative and public protection mission often overlaps with other agencies, leading to questions as to the appropriateness of such police involvement. (House of Commons Home Affairs Committee, 2007-8). The preventative and 'keeping the peace' functions of the police arguably suffer from a lack of clarity, and development of what could be called 'Austerity AI' in conjunction with those aims has been subject to criticism. In parallel, the police are increasingly required to pick up the slack left by cuts to other public services, most notably local ambulance trusts and mental health services (Babuta, 2017b), raising further questions regarding the delineation of responsibilities between the police and other agencies when it comes to intervention and prevention measures.

'Austerity AI' and the problem of prioritisation

Recent decades have seen an increased focus on risk-based approaches to the prioritisation of resources and triaging of offenders (Yeung, 2018), coupled with a rise in risk management and public protection approaches to future offending (Millie, 2013; Heaton, Bryant and Tong, 2019) and an emphasis on vulnerability (Grace, 2015). Sommerer argues that this may lead to a shift away from defined criminal offences to a more 'diffuse' category of algorithmically defined risk-based behaviour and attitudes (Sommerer, 2018). Reduction in police officer numbers has also created a perceived need to work differently and prioritise effectively. In their report on citizen scoring in public services, Dencik et al. found: 'A recurring theme in the rationale for implementing data systems is the context of austerity, with managers and developers often responding to significant cuts by trying to use data to better target resources. This speaks to the contextual duality of data-driven technologies as one of data-rich and resource-poor contexts.' (Dencik et al., 2018).

'In accordance with law'

The difference in approach to police duties and functions between England and Wales and the rest of the UK has direct relevance to the legal justification of algorithmic tools designed to support the police's functions. According to the European Convention on Human Rights (ECHR), an interference by a police force with an individual human right by way of 'Austerity AI' and associated personal data processing must be 'in accordance with law', 'necessary' and 'proportionate' in the interests of public safety or for the prevention or detection of crime,.[iii] For a measure to be 'in accordance with law', it must be 'accessible' to the person concerned and foreseeable as to its effects, including as to the scope and discretion conferred on the police. (*M.M. v. the United Kingdom* (Application no. 24029/07).

In Scotland and Northern Ireland, the relevant statutes both confirm that activities relating to preventing crime and preserving order are part of the police's duties (Police and Fire Reform (Scotland) Act 2012, s20; Police (Northern Ireland) Act 2000, s32), and due regard must be had to 'policing principles'. In Scotland, these principles include the statement that 'the main purpose of policing is to improve the safety and well-being of persons, localities and communities in Scotland.' (Police and Fire Reform (Scotland) Act 2012, s32). In Northern Ireland, the principles focus upon carrying out functions to secure the support, and with the cooperation, of the local community (Police (Northern Ireland) Act 2000, s31A).

Regarding England and Wales, Hale LJ in *Michael v The Chief constable of South Wales Police* said that: 'There is no doubt that the police owe a positive duty in public law to protect members of the

public from harm caused by third parties.' (*Michael v The Chief constable of South Wales Police* [2015] UKSC 2, para. 195) This common law duty also relates to the positive obligations under Articles 2 and 3 of the European Convention on Human Rights (ECHR) to protect individuals from real and immediate risks of victimisation and violence (*Chief constable of Hertfordshire v Van Colle* [2008] UKHL 50). In *Catt*, however, although noting general police powers under English common law and declining to make a definitive ruling, the ECtHR expressed concern that 'the collection of data for the purposes of the [domestic extremism] database [in this case] did not have a clearer and more coherent legal base' (*Catt v UK* Application no. 43514/15). In reviewing South Wales Police's use of facial recognition, the High Court in *Bridges* was more bullish, finding that (in contrast to physically intrusive acts) the police's common law powers were 'amply sufficient' for photography in public places, biometric matching and compilation of watch-lists (*R (Bridges) v Chief Constable of the South Wales Police* [2019] EWHC 2341 (Admin), paras 68-78).

While many uses of data analytics for policing may prove uncontentious within the common law framework discussed above, expansion into algorithmic predictions of future risk, and the further disclosure of those predictions (for interventions that may or may not be statutorily defined) based on a common law justification could be regarded as a step too far. Such activities are not intrusive in the same way as a physical search or taking of fingerprints. However use of an algorithmic prediction in policing does not seem comparable to overt facial recognition, described by the High Court in *Bridges* as 'no more intrusive than the use of CCTV on the streets.' (*R (Bridges) v Chief Constable of the South Wales Police* [2019] EWHC 2341 (Admin), para 75). Neither does it seem as straightforward as the obtaining and storing of personal information, as approved by the Supreme Court in *Catt*, (*R (Catt) v Association of Chief Police Officers* [2015] AC 1065) especially if the algorithmic process creates a new category of uncertain or contestable information that may then directly affect an individual's treatment or categorisation. The contrast with the statutory functions (although widely drawn) of the Scottish and Northern Irish police, the intelligence agencies and National Crime Agency (and the associated provisions around obtaining, using and disclosing information[iv]) may come further into focus as scrutiny of the use of algorithmic tools and other experimental technology gains traction. This suggests an urgent need for a public debate over the role of the police and the concepts of public safety, prevention and wellbeing in an algorithm-assisted environment.

Furthermore, in considering the second limb of the ECHR test, the necessity and proportionality analysis, and despite the margin of appreciation given to national authorities, lack of clarity regarding the function to which the interference relates inevitably carries with it a risk that necessity will be challenging to make out, in terms of demonstrating how the interference answers a 'pressing social need' and that the reasons for it are relevant and sufficient (*S and Marper v United Kingdom* 30562/04 [2008] ECHR 1581). As Grace points out, 'there are as yet considerable unknowns as to what should be considered to be the proportionate storage or *use* of algorithmically-generated predictions of risk as a type of police intelligence'(Grace, 2019).

Discretion in police decision-making

Police work involves considerable autonomy and discretion (Lister and Rowe, 2015), not only around strategic and policy matters but also for day-to-day operational decisions often taken by lower ranks. (Wilson, 1978) Such discretion 'recognizes the fallibility of interfacing rules with their field of application' (Hildebrandt, 2016). The first Principle of the College of Policing's Authorised Professional Practice on 'Risk' states that 'the willingness to make decisions in conditions of uncertainty (i.e., risk taking) is a core professional requirement of all members of the police service' (College of Policing Authorised Professional Practice). This discretion is not unlimited however and public law expects discretion to be exercised reasonably, and the duty to enforce the law upheld. (*R v*

Metropolitan Police Commissioner ex. P. Blackburn [1968] 2 QB 118; *R v Chief constable of Sussex ex. P. International Trader's Ferry Ltd.* [1999] 2 AC 418.) Conversely, discretion must not be fettered unlawfully, by, for instance, failing to take a relevant factor into account when making a decision, for example by only considering factors that may indicate risk or potential for harm rather than those that might indicate the opposite.

Algorithms have the potential to package relevant factors in a way that could facilitate more efficient decision-making (Babuta, Oswald and Rinik, 2018), contributing to the identification of the factors most relevant to the decision at hand. These tools present a number of threats, however, to legitimate discretionary decision-making. Unnuanced risk scores have been demonstrated to be highly influential on human decision-makers (Cooke, 2010). Their 'binary nature' may even eliminate any discretionary power to deal with the 'hard cases' (Bayamlıoğlu and Leenes, 2018). A significant issue with categorising risk using whole numbers is that this method treats nominal variables 'as if they were scale', implying some form of objective assessment; yet 'how appropriate is it to consider that a risk with a score of 3 carries three times the risk of a score of 1?' (Heaton, Byrant and Tong, 2019), or indeed to conclude that someone categorised as 'low risk' needs no help or intervention for their particular circumstances.

Police forces that have implemented predictive algorithms have stressed that such tools are being used in a way that 'supports' and 'enhances', rather than replaces, professional judgement (Durham Constabulary, 2017; Oswald, Grace, Urwin and Barnes, 2018). In its Authorised Professional Practice on Risk, the College of Policing likewise notes that 'RI [risk identification], RA [risk assessment] and RM [risk management] tools should be regarded as an excellent but limited, means of improving the likelihood of identifying and preventing future offending or victimisation. They can enhance professional judgement but not replace it' (College of Policing Authorised Professional Practice). Nevertheless, a statistical prediction may have a significantly prejudicial effect on the human decision-making process. As Cooke and Michie point out, 'it is difficult for the decision-maker to disregard the number and alter their evaluation even if presented with detailed, credible and contradictory information' (Cooke and Michie, 2012).

The way that officers react to algorithmic outputs, and whether they will be prepared to override algorithmic recommendations with their own judgement, may depend to a large extent on the force's attitude to risk and the extent to which individual officers are held responsible for the consequences of alleged omissions and the criticisms made with the benefit of hindsight (Heaton, Bryant and Tong, 2019). Dencik et al.'s case study of Avon and Somerset police's Qlik tool highlights police officers' frustration that the tool initially generated scores that were contrary to their own knowledge and judgement of the individuals concerned (Dencik et al., 2018). This resulted in further development of the tool in terms of data inputs and use of relevant intelligence that remained uncodified: 'that breakdown in the relationship isn't going to go into Qlik Sense because it's not a crime, it's an intelligence report and Qlik Sense doesn't pick up intelligence. So we were quite frustrated by that at the beginning' (Avon and Somerset inspector quoted in Dencik et al., 2018). Concern was also expressed that too much importance was attached to the tool, resulting in nervousness about the 'defenceability' of taking action contrary to the algorithmic recommendation (Avon and Somerset inspector quoted in Dencik et al., 2018).

Beyond assessing the relevance and importance of factors which may or may not be coded into a statistical model, officer discretion is also crucial when deciding what further action will be taken on the basis of the risk assessment or forecast. The College of Policing notes that statistical prediction 'is recognised as more accurate than unstructured judgement, but is inflexible and blind to specific contexts' (College of Policing Authorised Professional Practice). A numerical 'risk score' provides

the decision-maker with no insight into the specific nature or causes of risk, nor guidance as to what intervention measures can be taken to address the risk (Cooke and Michie, 2012). The third principle of the APP on 'Risk' states that 'Risk taking involves judgement and balance. Decision makers are required to consider the value and likelihood of the possible benefits of a particular decision against the seriousness and likelihood of the possible harms' (College of Policing Authorised Professional Practice). It follows that the soundness and fairness of an officer's decision-making is judged largely on whether they have considered the relative potential benefits and harms of different outcomes. Such a risk-benefit analysis may be highly context-specific and subjective, requiring careful consideration of a range of possible scenarios, including their likelihood and severity.

The ability to assess 'un-thought of' and uncodified relevant factors as part of the decision-making process must be preserved if discretion is to be applied appropriately. We have previously argued that AI and machine learning tools should not be inserted into a process that requires the exercise of discretion where the tool prevents that discretion; either because all of the factors relevant to the decision cannot be included, or required elements of the decision itself cannot be appropriately codified into, or by, the algorithm (Oswald, 2018). Use of an algorithmic tool should similarly not prevent the consideration of a range of different potential interventions or measures that can be taken to reduce any identified risk. Furthermore, as Lynskey points out in connection with the prohibition on automated decision-making in Article 11 of the Law Enforcement Directive and the question of adverse effect, much 'depends on how the decision-making process occurs in practice. In this context, one would need to gauge to what extent the final decision entails the discretion and judgment of the officer making that decision' (Lynskey, 2019). Practical considerations, in particular design of the human-computer interface, the avoidance of unnuanced framing of results (such as 'traffic-lighting' of risk levels), and organisational culture and processes, will be crucial to these issues.

Impact on rights

It is not our intention here to repeat the extensive research and commentary available on the issues of data protection, privacy, discrimination and bias, and transparency and explainability as these relate to machine learning. We instead refer back to the preventative and public protection role of the police supported by machine learning risk assessment tools. From the perspective of the police, it is clearly preferable to predict and prevent crime before it happens, rather than simply responding to and investigating criminal events after they have occurred. Few would question the validity of this logic as the rationale for implementing 'predictive policing' technology. However, legal and ethical issues arise when these preventative strategies involve interventions or other 'pre-crime' policing activities which may interfere with individuals' human rights or civil liberties, because they have been statistically identified as posing some risk of future offending. Furthermore, strategies of 'smart prevention' risk weakening society's moral narrative by disrupting conventional understanding of criminal responsibility and focusing upon reducing practical options to commit crime rather than moral reasons for compliance (Brownsword, 2019).

A potential risk in this regard is that the subjects of a 'data scoring' system are implicitly assessed based on the extent to which they conform to a particular group or 'class', rather than being considered as an individual case. In the context of criminal offending, this issue has been recognised for well over a hundred years. As Holmes remarks to Watson in *The Sign of the Four* (Conan Doyle's second Sherlock Holmes mystery):

> 'While the individual man is an insoluble puzzle, in the aggregate he becomes a mathematical certainty. You can, for example, never foretell what any one man will do, but you can say

> with precision what an average number will be up to. Individuals vary, but percentages remain constant.' (Doyle, 1890)

While often presented as an individual-level prediction, the output of a statistical risk assessment tool can be better understood as a group-level classification or categorisation. Rather than answering the question, 'what is the *likelihood* that this individual will behave in a certain way?', the algorithm is in fact answering a different question: 'to what extent is this individual *similar to* other individuals in the data who went on to behave in a certain way?' As summarised by Sutherland et al., 'predictive judgments are meaningful when applied to groups of offenders. However, at an individual level, predictions are considered by many to be imprecise' (Sutherland et al., 2012). The distinction between group-level classification and individual-level prediction is crucial, but often overlooked or misinterpreted.

When using group classification methods as a means of 'risk scoring' at the individual level, there is a risk that the police's preventative role may deviate from individual justice to group-based intervention, potentially adversely discriminating against individuals on the basis of the extent to which they conform to a certain 'profile' as identified in historic data. This may engage the Equality Act (and public sector equality duty pursuant to that Act) if such discrimination were to correspond to one or more protected characteristics, and could also result in the creation of new targeted groups not linked to protected characteristics, on the basis of systematic 'profiling' of individuals (Moses and Chan, 2018). When the risk scoring system also uses measures of association with known offenders as a predictor of risk, as in the Metropolitan Police's 'Gangs Matrix', individuals may be labelled as higher risk merely as a result of association with a particular group or network. This raises further questions around rights to non-discrimination under Article 26 of the International Covenant on Civil and Political Rights (ICCPR), as well as Articles 8 and 14 ECHR (corresponding to the right to respect for private and family life, home and correspondence, and protection from discrimination, respectively).

In practice, inclusion of measures of association as 'risk predictors' can lead to individuals being treated as 'guilty by association', even if there is no evidence to suggest they have been involved in criminal activity. Amnesty's investigation into the Gangs Matrix concluded that 'once on the matrix, they become *de facto* "gang nominals", a label which carries the stigma and suspicion of involvement in violent crime… the person is often automatically treated as someone who poses a risk of violence – even if they should not be on the matrix, or are on the matrix only because they have been a victim of violence.' (Amnesty, 2018) The ICO's investigation into the Gangs Matrix found numerous breaches of data protection laws, concluding that 'The Gangs Matrix does not clearly distinguish between the approach to victims of gang-related crime and the perpetrators, leading to confusion amongst those using it' (Information Commissioner's Office, 2018). This 'presumption of guilt' resulting directly from the algorithmic risk score may raise questions regarding the engagement of Article 6 ECHR (the right to a fair trial), where the assessment of guilt has in effect been pre-determined prior to any trial. Sommerer argues for a new broad reading of the presumption of innocence, 'a reading not limited to the criminal trial, but instead also related to risk assessments…where the criminal justice system attaches materially negative consequences to an individual's high-risk score', thus applying the presumption not only to the past, but to future prejudgments (Sommerer, 2018). Commenting on the COMPAS tool used for bail assessments in the US, Sommerer notes further that 'the likelihoods turn into "legal truth" for defendants when a judge at a bail hearing is presented with a high-risk classification (which generally neglects to mention the underlying statistics)' (Sommerer, 2018). A new broad presumption would therefore require a special uniform standard of certainty to apply to the ranking of an individual as high risk and therefore attaching to them potentially negative criminal justice consequences. This would also

suggest the need for laws, codes of practice and procedures relating to the recording, retaining and disclosure of material relevant to a criminal investigation to be reviewed in the light of the use of machine learning generated recommendations or classifications.

Beyond risks of discrimination, profiling and privacy violations, risk scoring of individuals based in part on their known associates and network of contacts may also lead to a 'chilling effect' where individuals become reluctant to go about their normal social activities, thereby engaging Articles 10 and 11 ECHR (right to freedom of expression, and right to freedom of assembly and association, respectively). In their independent report on the Metropolitan Police's trial of live facial recognition technology, Fussey and Murray noted that 'the deployment of LFR technology may generate a chilling effect whereby individuals refrain from lawfully exercising their democratic rights due to a fear of the consequences that may follow. For instance, they may be reluctant to meet with particular individuals or organizations, to attend particular meetings, or to take part in particular protests, at least in part due to the fear of "guilt by association"' (Fussey and Murray, 2019). The sharing of data between other agencies may also contribute to this chilling effect, causing individuals to become reluctant to engage with other public services for fear that their interaction with these services may be subsequently coded into a statistical model and used as an indicator of future risk. Amnesty concluded that 'Data sharing between the police and other government agencies means that this stigmatising "red flag" can follow people in their interaction with service providers, from housing to education, to job centres. It is important to examine the impact this has on their rights.' (Amnesty, 2018). Therefore, while use of police data alone to train predictive systems carries risks concerning bias and discrimination, the use of a wider range of data sets from other sources can affect individuals' rights and freedoms in other, more complex ways which may be difficult to quantify or even identify.

Finally, while the risk of being subject to intervention or interference from police and other authorities is often discussed as a potential negative outcome of being subject to a risk scoring system, being judged as *ineligible* for a particular intervention or initiative could also impact on individuals' rights in a way that is far harder to detect. Risk scoring systems are trained to identify statistically significant correlations and patterns in historic data. Some variables may not be statistically significant because they do not appear very frequently in historic data, but are very strong predictors when they do occur. Variables can also interact with each other in ways that are not captured by the algorithm. As a result, there is a risk that the algorithm may not take account of factors which are relevant to an individual's risk of offending (either because these factors are too rare to be captured by a statistical model, or because they interact in a way that is not coded into the algorithm), meaning those individuals then fail to receive the support they need to prevent them engaging in problematic behaviour.

Safeguards, governance and oversight

There are various stakeholders in the 'regulatory space' relevant to police use of predictive analytics (Hancher and Moran, 1998).[2] As mentioned previously, police use of analytics engages aspects of various legal frameworks, codes of practice and professional standards, and there is a lack of coordination and clarity regarding delineation of responsibilities as regards scrutiny, oversight and regulation.

Some stakeholders play a major role in overseeing and setting professional standards for policing in England and Wales, such as Chief Constables, Police and Crime Commissioners (PCCs), the College

of Policing, the NPCC, the Home Office and HMICFRS. Others have a more limited remit or one confined to specific issues, such as the Investigatory Powers Commissioner's Office (IPCO), the Information Commissioner's Office (ICO) and other commissioners or regulators such as the Surveillance Camera Commissioner and Forensic Science Regulator. In addition, a number of other bodies are engaging in advisory or investigatory activities, including the Centre for Data Ethics and Innovation (an advisory body currently situated within the Department for Digital, Culture, Media and Sport), the Office for Artificial Intelligence, Parliamentary committees, other independent committees, and various non-government academic and campaigning organisations with sector expertise or policy-making functions.

But despite this crowded 'regulatory space', there is a lack of clarity regarding who should take the lead in providing national guidance and oversight of compliance in relation to police use of analytics. As a result of this lack of national leadership and guidance, forces continue to operate with a great deal of autonomy when it comes to technological development, with different forces investing in different pieces of technology for the same purposes. This lack of national coordination results in duplication of efforts, unnecessary overspending, and a lack of compatibility and interoperability between local, regional and national information systems.

The College of Policing's Authorised Professional Practice (APP) is the official source of professional practice for policing in England and Wales. It includes sections on Management of Police Information (MoPI), risk assessment, intelligence management and a Code of Ethics based on the Principles of Public Life developed by the Committee on Standards in Public Life. Police officers and staff are expected to have regard to this APP in discharging their responsibilities, but individual forces have the autonomy to operate outside of these nationally agreed guidelines if deemed appropriate. The NPCC is of particular importance given its role in 'the national operational implementation of standards and policy' (NPCC, 2019), and joint approaches on information management and technology. The NPCC Coordination Committees (of which there are eleven, each led by a Chief Constable) are responsible for identifying additional guidance that may need to be incorporated into APP, and these are submitted for consideration by the College's 'Gateway Group'. APP is subject to ongoing review in consultation with the relevant National Policing Business Area.

HMICFRS has a clear oversight and inspection remit as part of its annual PEEL (police effectiveness, efficiency and legitimacy) inspections, Data Integrity inspections, and national thematic inspections. Adherence to APP and other College of Policing standards is assessed as part of these inspections. However, HMICFRS is not a regulator, rather an 'inspectorate', meaning it has no enforcement powers. The recommendations produced as part of HMICFRS inspections are not legal requirements, and chief constables and PCCs have a considerable degree of discretion in deciding how (if at all) to act upon these recommendations. PCCs are required to publicly respond to HMICFRS inspections within a period of 56 days, summarising the action to be taken in response to each recommendation. Closely related to the HMICFRS inspection framework is the generation of 'force management statements', which include the chief constable's own evaluation and projections for the coming year against a set of pre-determined criteria.

While the policing inspection programme and framework for 2019/20 includes specific thematic inspections focussed on cyber-crime, this does not extend to wider issues concerning digital investigation and intelligence, or methods of data exploitation. Since 2015, HMICFRS has inspected forces' crime-recording practices as part of an ongoing rolling programme, covering the extent to which forces are adequately recording crime data. It is a natural progression for this inspection framework to be expanded to include forces' use of analytical tools applied to this data, against a set of national standards in the form of APP. At present, the 'ALGOCARE' guidance (Oswald et al.,

2018) is the only *de-facto* national guidance in this area, and has recently been adopted by the NPCC Business Change Council and recommended to chief constables alongside additional explanatory documentation (Terzis, Oswald and Rinik, 2019). A new set of APP could build on the existing 'ALGOCARE' guidance and provide a set of national standards against which forces can be inspected as part of future HMICFRS inspection programmes. This guidance could also assist policing bodies in crafting appropriate contract specifications and standards for AI tools, and should include advice on how performance should be tested and judged.

Beyond HMICFRS, the ICO has a specific regulation and enforcement function relating to data protection, and may issue enforcement notices to police forces when it identifies a breach of data protection laws. However, as discussed in this chapter, police use of algorithms can impact on human rights and civil liberties in multiple ways beyond those captured in data protection legislation, and there is an argument that the ICO's remit may need to be expanded to account for the relevance of these other legal frameworks. However, this is an unrealistic prospect at present as the ICO is critically under-resourced. The ICO's data protection functions are funded solely by notification fees paid by organisations that process personal data ('data controllers'). The monetary penalties generated by ICO enforcement activity are paid into the Treasury's Consolidated Fund and not kept by the ICO, meaning it lacks the resources needed to take on additional investigation and enforcement responsibilities beyond data protection.

When algorithms are used in a context that would require a warrant under relevant surveillance legislation (Regulation of Investigatory Powers Act 2000; Investigatory Powers Act 2016), IPCO also has an important regulation and enforcement function. This includes ensuring that input data is not held for longer than is justified and is only used for the purposes specified in the initial warrant. In a recent investigation into the Security Service (MI5's) collection and analysis of communications data, IPCO identified serious compliance risks relating to the length of time that data collected under lawful interception warrants was stored within one or more of MI5's technology environments (Javid, 2019). However, in most cases the algorithmic tools discussed in this chapter would not be used in a way that would require a warrant and would therefore remain outside IPCO's remit. It is possible that IPCO's remit will need to be expanded in future to account for the use of potentially intrusive technologies which does not necessarily meet the threshold of 'surveillance' as defined in current legislation.

Beyond *ex post facto* oversight of the police's compliance with relevant legislative requirements, another challenge lies in ensuring that the analytical tools being used meet the necessary scientific standards to render them accurate and reliable enough to be used in an operational policing environment. Predictive algorithms produce probabilistic forecasts, not certainties, and the margin of error associated with these forecasts can vary considerably from one tool to the next. There are no minimum standards for the scientific validity and relevance of algorithmic outputs, which would enable the police to judge the level of confidence to assign to a prediction. The Forensic Science Regulator could potentially play an important role here – particularly if such tools were to be used in a criminal justice context – but currently lacks the statutory enforcement powers needed to enforce such quality standards (Tully, 2019).

Beyond ensuring compliance with 'the letter of the law', independent ethics committees can also provide oversight and scrutiny of police use of data analytics. The promotion of ethical principles and guidelines has been gaining traction, although many of these initiatives can be criticised for a high level of abstraction, limited consideration of existing legal and regulatory regimes, and lacking any enforcement or oversight mechanisms. By contrast, two public sector ethics committees established specifically to oversee innovative data analytics projects are worthy of consideration: the

National Statistician's Data Ethics Advisory Committee (NSDEC) and the West Midlands Police and Crime Commissioner and West Midlands Police Ethics Committee. Both these committees operate in accordance with terms of reference, and review submissions against specified principles, which include legal compliance. Both committees have a commitment to transparency, with papers and minutes published online (subject to any necessary operational confidentiality).

The West Midlands committee's terms of reference tasks the committee with tracking a project from development to deployment, as it is anticipated that unforeseen consequences could occur when a project moves from the development stage to operational roll-out, with the PCC and chief constable required to respond to the Committee's feedback and provide reasons for any disagreement with the Committee's recommendations. Based on the proceedings of the NSDEC since 2015, the Statistics Authority has developed self-assessment and 'precedent' administrative processes, allowing researchers to assess projects in advance of full ethical review by NSDEC and compare new proposals against projects previously approved by NSDEC.

Although entitled 'ethics' committees, the remit of these bodies is not in fact narrowly defined; they could be said rather to be oversight committees, testing proposals against the 'public good', and providing the benefit of a 'fresh pair of eyes.' The structure of these bodies might usefully be further studied in order to provide a template that could be used more widely within policing for oversight of the deployment of AI. Many police forces have already established Ethics Committees (not necessarily focussed on technology). A draft terms of reference was produced by the College of Policing, noting that 'Ethics Committees offer an opportunity for the Police Service to develop a structured environment in which to discuss and debate some of the most difficult and contentious issues we face' (College of Policing). In May 2019 the London Policing Ethics Panel published its final report on live facial recognition, in which it issued a number of recommendations to the force regarding ongoing use of the technology (London Policing Ethics Panel, 2019). However, more detailed technical analysis is required to understand these complex issues in sufficient detail, and it is essential that such committees include members with specific data science expertise.

Conclusion

Bearing in mind the significant impact the police's use of predictive analytics can have on citizens' civil liberties, and the various legal frameworks that may be engaged by the use of this technology, the lack of any clear national guidance or professional standards is a cause of great concern. In the long term, primary legislation may be required to account for these advances in the police's use of technology. Specifically, the roles and responsibilities of the police of England and Wales may need to be explicitly defined in the form of statutory functions, as is the case with the police services of Scotland and Northern Ireland. This may be necessary not just for police use of algorithms, but more generally to provide reassurances regarding the legitimacy of the 'public protection' and preventative functions of various policing powers and duties. In the short to medium term, it is essential to develop a clear framework to facilitate trials of experimental technology, in order to judge its relative benefits and harms in a controlled environment, before such tools are deployed operationally in a way that could interfere with individuals' human rights and civil liberties. Failure to do so could erode public trust in the police and undermine future attempts to engage in meaningful dialogue.

End notes:

[i] Police and Criminal Evidence Act 1984, Criminal Justice and Public Order Act 1994, Police Act 1996, Human Rights Act 1998, Crime and Disorder Act 1998, Police Reform and Social Responsibility Act 2011, Legal Aid, Sentencing & Punishment of Offenders Act 2012, Police (Conduct) Regulations 2012, Data Protection Act 2018, Protection of Freedoms Act 2012, Criminal Procedure and Investigations Act 1996, Terrorism Act 2000, Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016, Code of Ethics, Management of Police Information, to name but a few.
[ii] Now the National Police Chiefs' Council (NPCC).

[iv] See for instance s1(5) Crime and Courts Act 2013: 'The NCA is to have the function (the "criminal intelligence function") of gathering, storing, processing, analysing, and disseminating information that is relevant to any of the following— (a) activities to combat organised crime or serious crime; (b) activities to combat any other kind of crime; (c) exploitation proceeds investigations...'

References

ACPO (2011) *Statement of Mission and Values.*
Amnesty (2018) *Inside the Matrix*.
Babuta, A. (2017a) 'Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities', *RUSI Occasional Papers*. London: Royal United Services Institute.
Babuta, A. (2017b) 'A thinning blue line? The context of current debate on Britain's police levels', *RUSI Commentary*. London: Royal United Services Institute.
Babuta, A., Oswald, M. and Rinik, C. (2018) 'Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges', *RUSI Whitehall Reports*, 3-18. London: Royal United Services Institute.
Babuta, A. and Oswald, M. (2019) 'Data analytics and algorithmic bias in policing', *RUSI Briefing Paper*. London: Royal United Services Institute.
Bachner, J. (2013) *Predictive policing: preventing crime with data and analytics*. IBM Center for the Business of Government.
Bayamlıoğlu, E. and Leenes, R. (2018) 'The "rule of law" implications of data-driven decision-making: a techno-regulatory perspective', *Law, Innovation and Technology*, 10(2), pp. 295-313.
Bennett Moses, L. and Chan, J. (2018) 'Algorithmic prediction in policing: assumptions, evaluation, and accountability, *Policing and Society*, 28(7), pp. 806-822.
Bowers, K.J., Johnson, S.D. and Pease, K. (2004) 'Prospective hot-spotting: the future of crime mapping?', *British Journal of Criminology*, 44(5), pp. 641-658.
Brownsword, R., (2019) *Law, Technology and Society: Re-imaging the Regulatory Environment* Abingdon: Routledge.
Catt v UK (Application no. 43514/15).
Chief constable of Hertfordshire v Van Colle [2008] UKHL 50.
Cobbe, J. (2018) 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making', a pre-review version of a paper in Legal Studies, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3226913 or http://dx.doi.org/10.2139/ssrn.3226913 (accessed 10 October 2019).
The Code of Ethics Reading List, College of Policing.
College of Policing, *Authorised Professional Practice: Understanding risk and vulnerability in the context of domestic abuse.*
College of Policing, 'Ethics Committees', available at: http://www.college.police.uk/What-we-do/Ethics/Documents/Ethics_Committees.pdf (accessed 10 October 2019).
Cooke, D. J. (2010) 'More prejudicial than probative', *The Journal of the Law Society of Scotland*, 55, 20–23.
Cooke, D.J. and Michie, C. (2013) 'Violence risk assessment: from prediction to understanding–or from what? To why?', In Logan, C. and Johnstone, L. (eds.) *Managing Clinical Risk.* London: Routledge, pp. 22-44.

Copas, J., and Marshall, P. (1998) 'The Offender Group Reconviction Scale: A Statistical Reconviction Score for Use by Probation Officers', *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, 47(1), 159-171.
Craig, L. and Beech, A. R. (2009) 'Best practice in conducting actuarial risk assessments with adult sexual offenders', *Journal of Sexual Aggression*, 15, p. 197.
Craig, L.A., Beech, A. and Browne, K.D. (2006). Cross-validation of the risk matrix 2000 sexual and violent scales. *Journal of interpersonal violence*, 21(5).
Crime and Courts Act 2013.
Dencik, L., Hintz, A., Redden, J. and Warne, H. (2018) *Data Scores as Governance: Investigating uses of citizen scoring in public services.* Research Report, Cardiff University.
Douglas, K.S., Yeomans, M. and Boer, D.P. (2005) 'Comparative validity analysis of multiple measures of violence risk in a sample of criminal offenders', *Criminal Justice and Behavior*, 32(5), pp. 479-510.
Doyle, A.C., 1890. *The sign of the four*. London: Spencer Blackett.
Durham Constabulary written evidence to Commons Science and Technology Committee inquiry into algorithms in decision making, 26 April 2017.
Europol (2017), *Serious and Organised Crime Threat Assessment 2017: Crime in the Age of Technology.* The Hague: Europol
Fenwick, H. (2009), 'Marginalising human rights: breach of the peace, "kittling", the Human Rights Act and public protest', *Public law*, 2009(4).
Ferguson, A.G. (2017), *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York: NYU Press.
Fisher v The Mayor of Oldham 143 LTR 281.
Fussey, P. and Murray, D., (2019), *Independent Report on the London Metropolitan's Police Service's Trial of Live Facial Recognition Technology*. University of Essex.
Grace, J. (2015) 'Clare's Law, or the national Domestic Violence Disclosure Scheme: the contested legalities of criminality information sharing', *The Journal of Criminal Law*, 79(1), pp.36-45.
Grace, J. (2019) '"Algorithmic impropriety" in UK policing?', *Journal of Information Rights, Policy and Practice*, 3(1).
Hancher, L. and Moran, M. (1998) 'Organizing Regulatory Space', in R. Baldwin, C. Scott and C. Hood (eds), *A Reader on Regulation*, Oxford: OUP.
Harris, G.T., Rice, M.E. and Quinsey, V.L. (1993) 'Violent recidivism of mentally disordered offenders: The development of a statistical prediction instrument', *Criminal justice and behavior*, 20(4), pp.315-335.
Hart, S.D., Michie, C. and Cooke, D.J. (2007) 'Precision of actuarial risk assessment instruments: Evaluating the "margins of error" of group v. individual predictions of violence', *The British Journal of Psychiatry*, 190(S49), pp.s60-s65.
Heaton, R., Bryant, R. and Tong, S. (2019), 'Operational risk, omissions and liability in policing' *The Police Journal*, 92(2), pp.150-166.
Hildebrandt, M. (2016), 'New animism in policing: re-animating the rule of law', *The SAGE Handbook of Global Policing*, pp.406-28.
Hildebrandt, M. (2018), 'Preregistration of machine learning research design' in eds. Bayamlioglu, Baralouc, Janssens, Hildebrandt, *Cogitas Ergo Sum: 10 Years of Profiling the European Citizen*. Amsterdam University Press.
HMIC (2017), *PEEL: Police Effectiveness 2016: A National Overview*. London: Her Majesty's Inspectorate of Constabulary.
House of Commons Home Affairs Committee (2007-8), 'Policing in the 21st Century' Seventh Report of Session 2007-8 HC 364-1.

Howard, P., Clark, D. and Garnham, N. (2006) *An Evaluation and Validation of the Offender Assessment System (OASys)*. London: Home Office.
Howard, Philip and Francis, Brian and Soothill, Keith and Humphreys, Leslie (2009) *OGRS 3: The revised Offender Group Reconviction Scale.* Research Summary, 7/09. London: Ministry of Justice.
Information Commissioners Office (2018), 'Enforcement notice issued to Metropolitan Police Service', 16 November 2018.
Intelligence Services Act 1994.
Jansen, F. (2019), *Data Driven Policing in the Context of Europe*, working paper, 7 May 2019.
Justices of the Peace Act 1361.
Javid, S. (2019), 'Investigatory Powers Act 2016: Safeguards Relating to Retention and Disclosure of Material': Written statement by Sajid Javid - HCWS1552, 9 May 2019.
Joh, E.E. (2014) 'Policing by numbers: big data and the Fourth Amendment', *Wash. L. Rev., 89*.
Johnson, S.D., Birks, D.J., McLaughlin, L., Bowers, K.J. and Pease, K. (2007), 'Prospective crime mapping in operational context: Final report', *UCL, Jill Dando Institute of Crime Science: London, UK*.
Johnson, S.D. (2008) 'Repeat burglary victimisation: a tale of two theories', *Journal of Experimental Criminology*, 4(3), pp.215-240.
The Rt Hon The Lord Judge, Lord Chief Justice Of England And Wales (2011), The Police Foundation's John Harris Memorial Lecture, *Summary Justice In And Out Of Court*, Drapers Hall, London, 7 July 2011.
Kent Police Corporate Services Analysis Department (2014) 'PredPol Operational Review [Restricted and Heavily Redacted]', available at: http://www.statewatch.org/docbin/uk-2014-kent-police-predpol-op-review.pdf (Accessed 10 October 2019).
The Law Society of England and Wales (2019) *Algorithms in the Criminal Justice System.* London: The Law Society.
LXD v The Chief constable of Merseyside Police [2019] EWHC 1685 (Admin).
Lister, S. and Rowe, M. (2015) 'Accountability of policing', In *Accountability of Policing*, pp. 1-17. London: Routledge.
London Assembly, Budget and Performance Committee (2013), *Smart Policing*.
London Policing Ethics Panel (2019) *Final report on live facial recognition.*
Lynskey, O. (2019) 'Criminal justice profiling and EU data protection law: precarious protection from predictive policing', *International Journal of Law in Context*, 15(2), pp.162-176.
M.M. v. the United Kingdom (Application no. 24029/07).
Meijer, A. and Wessels, M. (2019) 'Predictive Policing: Review of Benefits and Drawbacks', *International Journal of Public Administration*, pp.1-9.
Michael v The Chief constable of South Wales Police [2015] UKSC 2.
Millie, A. (2013) 'What are the police for? Re-thinking policing post-austerity', in *The future of policing* (pp. 82-93). Routledge.
Mohler, G.O., Short, M.B., Malinowski, S., Johnson, M., Tita, G.E., Bertozzi, A.L. and Brantingham, P.J. (2015) 'Randomized controlled field trials of predictive policing', *Journal of the American statistical association*, 110(512), pp.1399-1411.
National Analytics Solution project team (2018) Response to The Alan Turing Institute and IDEPP, 2018.
National Offender Management Service (2015) 'A compendium of research and analysis on the Offender Assessment System (OASys), 2009-2013'. London: NOMS.
Osman v United Kingdom [1998] 29 EHRR 245.

Oswald, M., Grace, J., Urwin, S. and Barnes, G.C. (2018) 'Algorithmic risk assessment policing models: lessons from the Durham HART model and "experimental" proportionality', *Information & Communications Technology Law*, 27(2), pp. 223-250.
Oswald, M. (2018) 'Algorithmic-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power', in 'The growing ubiquity of algorithms in society: implications, impacts and innovations' issue of Philosophical Transactions of the Royal Society A.
Oswald, M. (2019) 'Technologies in the twilight zone: Early lie detectors, machine learning and reformist legal realism'. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3369586 (accessed 10 October 2019).
Police Foundation and Policy Studies Institute (1996) 'The Role and Responsibilities of the Police'.
The Policing Protocol Order 2011 Cm. 2850.
Police Reform and Social Responsibility Act 2011, c.13 Schedule 2.
Police and Fire Reform (Scotland) Act 2012.
Police (Northern Ireland) Act 2000.
Quinsey, V.L., Harris, G.T., Rice, M.E. and Cormier, C.A. (2006) *Violent offenders: Appraising and managing risk*. American Psychological Association.
R (Catt) v Association of Chief Police Officers [2015] AC 1065.
R (Bridges) v Chief Constable of the South Wales Police [2019] EWHC 2341 (Admin).
R v Metropolitan Police Commissioner ex. P. Blackburn [1968] 2 QB 118.
R v Chief constable of Sussex ex. P. International Trader's Ferry Ltd. [1999] 2 AC 418.
Richardson, R., et al. (forthcoming), 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', *New York University Law Review Online*.
S and Marper v United Kingdom 30562/04 [2008] ECHR 1581 (4 December 2008).
Security Service Act 1989.
Sommerer, L. M. (2018) 'The Presumption of Innocence's Janus Head in Data-Driven Government', in eds. Bayamlioglu, Baralouc, Janssens, Hildebrandt, *Cogitas Ergo Sum: 10 Years of Profiling the European Citizen*. Amsterdam University Press.
Sutherland, A.A., Johnstone, L., Davidson, K.M., Hart, S.D., Cooke, D.J., Kropp, P.R., Logan, C., Michie, C. and Stocks, R. (2012), 'Sexual violence risk assessment: An investigation of the interrater reliability of professional judgments made using the Risk for Sexual Violence Protocol', *International Journal of Forensic Mental Health*, 11(2), pp.119-133.
Terzis, P., Oswald, M. and Rinik C (2019) *Shaping the State of Machine Learning Algorithms within Policing*, 26 June 2019. Winchester: University of Winchester.
Thornton, D., Mann, R., Webster, S., Blud, L., Travers, R., Friendship, C. and Erikson, M. (2003) 'Distinguishing and combining risks for sexual and violent recidivism', *Annals of the New York academy of sciences*, 989(1), pp.225-235.
Tully, G. (2019) 'Forensic Science Regulator annual report 2018'.
The Alan Turing Institute Data Ethics Group and the Independent Digital Ethics Panel for Policing (2017). 'Ethics Advisory Report for West Midlands Police'.
Webster, C.D., Haque, Q. and Hucker, S.J. (2013) *Violence risk-assessment and management: Advances through structured professional judgement and sequential redirections*. John Wiley & Sons.
Wilson, E., and Hinks, S (2011) 'Assessing the predictive validity of the Asset youth risk assessment tool using the Juvenile Cohort Study (JCS)', *Ministry of Justice Research Series*, 10(11).
Wilson, J.Q. (1978) *Varieties of police behavior*. Harvard University Press.

Yeung, K. (2018) 'Algorithmic regulation: A critical interrogation', *Regulation & Governance*, 12(4), pp.505-523.
Youth Justice Board (2000) *ASSET: Explanatory Notes.* London: Youth Justice Board.