THE POLICE FOUNDATION

The UK's policing think tank

DATA-DRIVEN POLICING AND PUBLIC VALUE

IAN KEARNS AND RICK MUIR

MARCH 2019

DATA-DRIVEN POLICING AND PUBLIC VALUE

IAN KEARNS AND RICK MUIR

MARCH 2019

Acknowledgments

The authors would like to thank all those who contributed to this research. In particular we are grateful to Accenture, BT and the Institute for Policy Research at the University of Bath who generously provided the funding for this project. We are also grateful to the members of our Project Advisory Group, including David Darch, Allan Fairley, Lord Toby Harris, Giles Herdale, Simon Kempton and Professor Tom Kirchmaier. We would like to thank all those police forces we visited as part of the research in particular Avon and Somerset Police and Hampshire Constabulary.

Authors

Dr Ian Kearns is a Senior Associate Fellow of the Police Foundation and during the period in which he was working on this report was also a Visiting Fellow at the Institute for Policy Research at the University of Bath. He has 25 years of experience working in the public, private and NGO sectors. He is a former Deputy Director and Acting Director of the Institute for Public Policy Research (IPPR) where he provided strategic direction on digital government, the new digital economy, national security and crime. Prior to this Ian was a Director in the Global Government Industry Practice of Electronic Data Systems (EDS), an IT services firm with a $20bn turnover. Ian also co-founded and served as the first Director of the European Leadership Network, a network of former Prime Ministers, foreign and defence ministers and other senior figures focused on security issues. He now serves on the organisation's Executive Board of Directors.

Dr Rick Muir is the Director of the Police Foundation. Prior to that he was the Associate Director for Public Service Reform at the Institute for Public Policy Research (IPPR). He has a D Phil in Politics from the University of Oxford. He is a Visiting Professor at Northumbria University, a Fellow of the Royal Society of Arts, Manufactures and Commerce (RSA) and a member of the Cumberland Lodge Police Steering Committee. He has previously been a local councillor and school governor.

About the Police Foundation

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Its mission is to generate evidence and develop ideas which deliver better policing and a safer society. It does this by producing trusted, impartial research and by working with the police and their partners to create change.

CONTENTS

SUMMARY

Policing is operating in a context of particularly rapid change. Police forces are operating under considerable stress, faced with reduced budgets at the same time as changing patterns of demand. Crime is changing, in part driven by the technological revolution we describe in this report. New skills are being demanded of police officers. The public is increasingly tech savvy and expects the police to be so too. This transforming context inevitably requires far reaching change in the nature of policing.

This report looks at how the police can meet this challenge by the imaginative use of data-driven driven technologies. In particular the report focuses on how data-driven policing can contribute to public value.

By **data-driven**, we mean the acquisition, analysis and use of a wide variety of digitised data sources to inform decision making, improve processes, and increase actionable intelligence for all personnel within a police service, whether they be operating at the front-line or in positions of strategic leadership.

By **public value**, we mean the full value that a police force contributes to society across a number of measurable dimensions, including outcomes in relation to crime, the efficient use of public funds, and the quality of the police relationship with the public.

CONTEXT

Direct funding from central government to police forces declined by 30 per cent in real terms between 2010/11 and 2017/18. At the same time demand on the police has been changing and in many areas intensifying. Some categories of crime such as violent crime, acquisitive crime such as burglary, and some vehicle crime are increasing after years of decline. There has been a shift towards dealing with complex areas of crime such as domestic violence and child sexual exploitation and abuse, which require a different skill set and are more resource intensive to investigate. We have seen a rise in demand for the police to respond to non-crime incidents such as mental health crises and missing persons.

A huge amount of crime is also either moving online or is being cyber-enabled. Around half of all crime affecting individual victims in England and Wales is now cybercrime or fraud (much of which is cyber- enabled). The internet has created new types of computer misuse crime and has opened up new opportunities for people to commit older types of crime, such as fraud and child sexual abuse, on a much larger scale.

It is also already clear that the onset of a digital society is creating new and profound challenges for the police. The volume of digital forensic material being seized for almost all crime types is massive. The police are also now having to deal with a public that is used to living far more of its life online, which is translating into a public appetite to engage with the police using digital channels.

All this amounts to a radically different landscape for UK policing and there is no reason to believe the pace of change will ease off.

THE NEAR HORIZON

There are a large number of new technological developments of relevance to policing. Notable developments include the emergence of 5G networks and the growth in criminal use of encryption. We focus on two other phenomena that we think are likely to have a growing and major impact on the policing and crime landscape *in the near term*. These are the 'internet of things' and Blockchain. Both not only add complexity to the existing landscape of crime and policing but actually introduce whole new domains in which crime can be committed, investigated and prevented.

It is projected that by 2020, 31 billion devices will be connected to the internet worldwide, rising to more than 75 billion by 2025. This will have two major consequences for policing and crime. First, it is increasing the 'attack surface' of interest to criminals and new risks are being created as a result. Hackers may be able to get access to people's information and money and may take control their internet enabled devices.

Second, the advent of the internet-of-things is going to change the game when it comes to police investigations. Police officers increasingly need to get up to speed with the data that connected devices hold, and with how that data can be accessed, preserved and used as evidence.

If anything, the impact of blockchain technologies might be even greater. Blockchain is a shared distributed ledger (like a digital record book) that records

transactions and tracks assets across a network. It is called blockchain because it stores data in blocks that are linked together to form a chain. Each block confirms when a transaction took place and contains a hash that forms a unique identifier linking the blocks together.

Blockchain poses two challenges for law enforcement. First, with banks and other financial institutions cut out of the loop, the police lose a vital source of information on financial transactions that often help them to build cases against criminals and to secure convictions. Second, given that the identities of those conducting the transactions, and the transactions themselves, are encrypted, it is also very hard for the police to be able to link specific payments to specific individuals.

Criminals have noticed, and have become enthusiastic users of crypto-currency platforms that are based on blockchain to facilitate crimes such as money laundering. One analysis has found that one quarter of bitcoin users, and a half of all bitcoin transactions, were associated with illegal activity.

INNOVATION CASE STUDIES

It is not, however, only the criminals who are using new technology. There is a stated desire and intent on the part of police leaders in England and Wales to adapt to, and embrace today's digital society. The Digital Policing Portfolio (DPP) set up by the National Police Chiefs' Council (NPCC) has been central to the implementation effort, leading three core streams of work across Digital Public Contact, Digital Intelligence and Investigation (DII), and what became known as Digital First (the attempt to integrate digitised policing with the wider the criminal justice system). Individual forces are also running innovative data-driven projects up and down the country.

We review the evidence emerging from this work, but also cast the net much wider beyond both policing in this country, and beyond policing itself, to examine innovative uses of digital and data-driven approaches by private sector organisations and citizens groups where these are relevant to the police and crime agenda. We make no claim, of course, to be exhaustive.

Our focus throughout is on showcasing activity that relates to the delivery of public value through its impact. Where evidence of impact is not yet publicly available, we point to use cases where data-driven approaches are likely to deliver impact and public value in future. Given this focus, the material is organised not according to the type of technology in use or the specific sector deploying it, but around nine dimensions of Public Value.

For example, we show how Avon and Somerset Police is using software to bring together data from across fragmented databases and presenting it in useable interfaces that help the force, supervisors and individual officers know a lot more than they used to about a whole range of issues, whether these are to do with performance, officer deployment or an individual victim or suspect.

We also show how the Dutch police have recruited 1.6 million participants onto a digital collaboration platform which allows the police to send incident information out to citizens and in turn enables citizens to share any intelligence they may have. 10 per cent of resulting actions lead directly to an arrest and a further 40 per cent are thought to play a valuable role in the investigative process.

We show how Hampshire Constabulary has identified data-driven policing as a core contributor to their own effort to build a relationship of trust and confidence between the force and the public. This has principally taken the form of training a large number of officers and staff to the point where they have the knowledge and skills required to operate in a digital and data rich environment. The approach has been deployed both to train specialist capability to deal with serious, less frequent crime, and to enable identification and investigation of the digital footprint of volume crime.

These are among 23 innovation case studies mapped out against nine dimensions of public value.

CHALLENGES

Despite the benefits of data-driven technologies to policing, significant barriers and challenges prevent their future adoption. There are concerns about the way some police forces have misused data, such as the way some new information systems can result in the over-policing of certain individuals, neighbourhoods, and communities while others are left alone, a development that could ultimately undermine trust between the police and communities rather than enhance it.

The issue of the right to privacy also arises as citizens leave an ever more extensive digital trace from their movements, behaviour and interactions. At the same time the police are able to know more about us by bringing more and more data together and have access to surveillance tools, as such as cameras and facial and

numberplate recognition software. Complacency would be both unwise and ultimately could allow 'technology creep' to the extent that public perceptions of the legitimacy of police action were undermined.

Another challenge concerns the problem of bias in the data upon which predictive policing models are built. This data reflects information reported to and collected by the police and hence will reflect institutional and individual interpretations of policing priorities and biases, some of which can reflect social biases about race, social status and gender.

Public support for data-driven approaches to policing cannot be taken for granted either. For instance, attitudinal surveys find that the public are hostile to the idea that machines should be involved in making decisions within the criminal justice system.

Another major set of barriers to be overcome with regard to advancing the data-driven policing agenda are the practical delivery challenges. Both police leaders themselves, and Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)[1] has warned that the police are struggling to cope with the sheer volume of digital data and evidence now available. There also remains considerable workforce dissatisfaction with the state of police IT.

Behind these survey numbers and comments sit practical, structural, and legacy problems that have long been known about but are still unaddressed. Some relate to the poor quality and inaccurate or duplicated nature of much data held in police databases. Some to the fact that different police forces store different kinds of data using different codes on the same issue, in the context of a lack of agreed data sharing standards. Forces also take different attitudes about which officers are allowed access to particular systems and the circumstances around this. And many legacy technology systems still in use are effectively closed and cannot be integrated with others, either within a force, between forces or between the police and/or other public agencies.

We are also already at the point where some policing practices are leaving legal and regulatory frameworks behind. For instance, police forces experimenting with data-driven approaches, and with the use of algorithmic decision-support systems in particular, are doing so in the absence of any guidance or codes of practice on how this should be approached or what kind of safeguards should be put in place before experiments take place.

1 In July 2017 HMIC took on responsibility for fire and rescue service inspections and was renamed HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS). Inspections carried out before July 2017 refer to HMIC.

RECOMMENDATIONS

Recommendation 1

The police should support deliberative democracy initiatives that give groups of citizens the chance to learn about, and explore the complexities of, data-driven policing in-depth before passing more considered judgement on what is and is not acceptable police practice in the age of big data.

Recommendation 2

Privacy and ethics commissions should be introduced into the governance structures of every police force in the country to address growing privacy concerns about the use of surveillance technologies that are increasingly the source of much police data.

Recommendation 3

New regulations should be introduced to govern the use of algorithmic decision support tools in policing and the criminal justice system.

Recommendation 4

The College of Policing should develop further Authorised Professional Practice with regard to how algorithmic decision support tools should be integrated into policing practice.

Recommendation 5

Police inspection regimes should be amended so as to regularly monitor compliance with Recommendations 3 and 4. This is something that Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services should cover under the legitimacy strand of the PEEL inspection framework.

Recommendation 6

All police forces should review policies and procedures with regard to data stewardship.

Recommendation 7

Central government should provide additional funding for police officer training in a number of priority areas related to the data-driven policing agenda.

Recommendation 8

We need a new, coordinated approach to data accuracy in policing systems. This should include:

- Improved education and training for police officers and administrators with regard to the importance of accuracy and detail when data is being captured.
- Provision of formal staff training programmes by private companies providing predictive and data-driven policing systems.
- Greater use of automated checklists to ensure officer compliance with data input rules, and use of automated technology to transcribe officer input into formal documents which can then be automatically transmitted into a central database.

Recommendation 9

UK policing needs a common set of data standards and data entry codes to be used across the country. The Police ICT company should be given the role of developing one and its subsequent use should be mandated across all police forces. A common set of access protocols across all police forces are also needed so officers can be sure that other forces are not only capturing the same data, in the same way and in the same format, but that officers of the same rank and role are engaging with that data too.

Recommendation 10

The purchase by any police force in the UK of any 'closed' technology or system that is unable to be quickly and easily made interoperable with other equipment and systems should be banned. It is almost certainly a waste of public money and cannot be justified in a service whose effectiveness requires the joining up of data and systems within and across force boundaries.

Recommendation 11

Police forces in the UK should examine and replicate a similar initiative to Burgernet Netherlands which could include the public in helping to fight crime in a more structured way.

Overall, the set of recommendations set out here, if implemented, would put the whole country, its philosophy of policing, and the police themselves in a much stronger position to embrace data-driven policing while maintaining public confidence. The maintenance of that public confidence is essential to the ability of the police service to pursue the kind of public value that this report has demonstrated data-driven policing can provide.

1. INTRODUCTION

1.1 THE FOCUS OF THIS REPORT

This report examines the relationship between data-driven policing and public value. By **data-driven**, we mean the acquisition, analysis and use of a wide variety of digitised data sources to inform decision making, improve processes, and increase actionable intelligence for all personnel within a police service, whether they are operating at the front-line or in positions of strategic leadership.

By **public value**, we mean the full value that a police force contributes to society across a number of measurable dimensions, including outcomes in relation to crime, the efficient use of public funds, and the quality of the police relationship with the public. More specifically, in this report we have explicitly drawn on, and further adapted, the concept of a **'policing bottom line'** first developed by Professor Mark H. Moore at Harvard University.[2] This suggests that the police, and sometimes businesses and citizens themselves, can deliver public value in one or more of nine distinct ways in relation to policing and crime, including through:

- Reducing crime.
- Improving crime detection.
- Reducing public fear.
- Reducing public vulnerability.
- Action to ensure civility in public spaces.
- The use of police authority and force in a fair and just way.
- Action to improve public trust and confidence in the police and the wider criminal justice system.
- The delivery of a quality service experience to citizens.
- The efficient and fair use of public funds.

Our focus on these dimensions of public value has shaped our approach to both the collection and presentation of evidence in this report. In deploying it, the working assumption throughout has been that it captures something important about the goals and methods of a consent-based model of policing of the kind we already have, and value, in the United Kingdom. In the material that follows, and in exploring the possible benefits and downsides of a data-driven approach, we are therefore less interested in what data can do in the abstract, and more interested in what it can offer across each of these nine indicators of public value.

1.2 RATIONALE

We have chosen to focus on the link between data-driven approaches and public value for four important reasons.

First, to develop a stronger evidence base regarding data-driven approaches to policing. Use of data-driven technologies are thought by many to hold out the promise of a new era, bringing advances in many areas including police workforce productivity and wellbeing all the way through to better crime investigation, detection and prevention. The hope is that data-driven approaches may also be able to help improve levels of public and victim trust and confidence in the police.

At the same time, however, there is a perception that adopting new technologies and approaches can be a highly complex process that can alienate staff who are already under pressure. And some data-driven initiatives might also undermine the relationship between the citizen and the police, giving rise to concerns about decision-making by machine in the justice system and about increased levels of surveillance and reduced levels of privacy. The application of new technology might also sometimes lead to a shift of police officers from the street to back office functions which, though potentially very effective and efficient in the effort to fight crime, may undermine perceptions of public safety. We hope this report can help police leaders, policy-makers and the public to see the balance of opportunities and risks involved in adopting data-driven approaches and help us as a society to navigate our way through the challenges.

Second, the pace of technological change is accelerating and the question of how the police should

2 See for example Moore and Braga (2003).

adapt to change, not whether they should adapt, is already pressing. In this context it is worrying that many forces are experimenting and changing in a vacuum, with limited advice and guidance on what is and is not good practice. This report helps to fill that gap by mapping out what police agencies are doing here and around the world, and considers not just how the police must adapt but how the regulation of data-driven policing, and how the public and political debate, must adapt too.

Third, massive budget cuts are already impacting policing in the UK and are demanding forces up and down the country look for new ways to operate to get either more out of the same resource, or more for less. This financial driver of change is playing out alongside the technology driver, and while technology may hold some of the keys to the efficiency gains we seek, the two drivers can and do also collide at the point at which business cases have to be made for new investments in technology and data-led approaches, as opposed to investments in other areas of policing. A better evidence base related to what data-driven policing can and cannot deliver can only help to manage this apparent tension.

Fourth, the public value approach to policing is itself beginning to come under attack from some sections of the media. Some are beginning to criticise police activity that appears unrelated to criminal investigation, branding community relations work, for example, as time wasted that should be spent on hunting down criminals.[3] While this might be superficially attractive, it ignores the way in which the different elements of public value relate to each other. High quality relationships between the police and the public often translate into improved intelligence that can both help prevent and detect crime. Unless the full notion of the policing bottom line we have outlined here is protected, there is a danger that experimentation with data-driven approaches could become limited to a very narrow range of police activity. In the long-run, this would be to the detriment of UK policing.

1.3 THE STRUCTURE OF THE REPORT

The report is organised into five main chapters.

The next section, Chapter 2 outlines more of the context in which the police are currently operating. It focuses on cuts to police budgets; current crime trends and the challenges these are presenting; and changing public expectations about the way they interact with the police. It also highlights the risk that the police may be overwhelmed by data if new ways of managing it are not found.

Chapter 3 examines the near horizon with regard to two technological developments that are already with us but set to grow in significance. One of these is the 'internet of things' and the other, blockchain. Both are emblematic of the speed and scope of technological change, and both are already heavily used by criminals. They present major challenges to policing and raise questions about the extent to which law enforcement can police a digital society alone, or indeed at all, given the profound and pervasive nature of the technologies in question.

Chapter 4 moves on to an account of police innovation and experimentation with data-driven approaches, because it is not only the criminals who can and are making use of the new. The material in this chapter is structured around the nine public value dimensions listed earlier. It presents a mixture of hard evidence of results from data-driven experiments where possible and use-cases that should translate into public value at some point in future but where evidence is yet to be made available. Some of this material is drawn from the UK and some from other jurisdictions around the world. In this chapter, the focus is entirely on the benefits or potential benefits that a data-driven approach might be able to bring.

Chapter 5, by contrast, considers the many challenges yet to be overcome with regard to full scale adoption of a data-driven approach. It explores potential problems with police misuse or mishandling of data; the problem of data bias; concerns over privacy; policy and regulatory gaps within which UK policing is currently having to operate; and major technology and workforce issues with regard to the adoption of new technologies

3 See for example, Wilkins (2017) and Hitchens (2018). Sara Thornton, the Chair of the National Police Chiefs' Council also recently made comments to the effect that the police should be focused on 'core crimes' such as violent crime and burglary and not wider social ills such as 'hate crime', see Morrison (2018).

and approaches. It also considers public attitudes and concerns with regard to increased use of algorithmic decision support tools in police and criminal justice decision-making.

Chapter 6 contains recommendations on future action that could help the UK seize the opportunities of data-driven policing while managing the down-sides and maintaining public confidence throughout the process.

1.4 A NOTE ON METHODOLOGY

The research for this report has consisted of a number of different elements. These included:

- A search and review of secondary literature on data-driven approaches to policing, along with the collation of evidence of public value from some of the most promising examples of innovation.
- Interviews with police leaders, project leads, and those tasked with conducting evaluations on a smaller set of innovation case studies.
- Examination of relevant data-driven projects led by authorities other than the police, where those projects have implications for public value delivery with regard to policing and crime.
- Private interviews with police and other stakeholders, to ascertain views on both the promise, and potential perils of fully embracing a data-driven approach. Many of these interviews were conducted on a background basis. They are not always explicitly referenced and where they are, the identity of interviewees has been protected.
- Discussions with members of a project advisory board made up of academics, police officers, private sector representatives and other thinkers and policy-makers knowledgeable about either UK policing, or what data-driven approaches can deliver, or both.

There is a huge amount of experimentation under way in UK policing and in other jurisdictions around the world and, inevitably, it has only been possible to capture a fraction of it in this report. Nevertheless, we believe both the evidence presented and its relationship to a comprehensive 'policing bottom line' (captured in the public value metrics we have used) shines a valuable light on what data-driven policing can offer. Pursuing this approach will be vital if policing is to meet the new and increased demands it faces at a time of severely reduced police budgets. Unless they embrace such an approach the police may lose the confidence of an in increasingly tech savvy digital citizenry. The effort to invest in and pursue data-driven policing will only be worthwhile, however, if the challenges and potential downsides are addressed too.

2. CONTEXT

Policing is operating in a context of particularly rapid change. Police forces are operating under considerable stress, faced with reduced budgets at the same time as changing patterns of demand. Crime is changing, in part driven by the technological revolution we describe in this report. New skills are being demanded of police officers. The public is increasingly tech savvy and expects the police to be so too. This changing context inevitably requires far reaching change in the nature of policing.

Direct funding from central government to police forces declined by 30 per cent in real terms between 2010/11 and 2017/18.[4] Demand on the police, on the other hand, has diversified and, in some complex resource intensive cases, increased over the same period, with a large amount of police time no longer spent directly responding to reports of criminal activity, but on concerns expressed over the public safety and welfare of citizens, and incidents related to mental health.[5]

Against this backdrop, we are seeing some important categories of crime, such as violent crime, acquisitive crime such as burglary, and some vehicle crime, now increasing.[6]

While a direct line cannot be drawn from budget cuts to increases in crime, it is clearly the case that the police are trying to meet more demand with less resource, and that the cracks are beginning to show. This situation is unlikely to change any time soon and it is undoubtedly providing an important driver for some police forces to experiment with new technology and data-driven approaches to the way they work.

A huge amount of crime is also either moving online or is being cyber-enabled. The Digital Policing Board recently told the House of Commons Home Affairs Select Committee Inquiry into Policing for the Future, that 'fraud and computer misuse is now approximately half of known recorded crime.'[7] The National Crime Agency (NCA) noted in evidence to the same committee that: 'Fraud and wider economic crime are increasingly cyber-enabled.' It also noted that both fraud and child sexual exploitation and abuse (CSEA) have been transformed in scale and complexity by the internet. The number of referrals of online CSEA activity to the NCA, for example, increased from 400 per month in 2010 to 4,075 a month in 2016 as offenders seized the opportunity to use live streaming and encryption services to engage in their activities.[8]

Much hate crime has also moved online, as has a lot of activity to radicalise people into committing acts of terrorism, and more sophisticated efforts to commit election fraud. New crimes, such as online vigilantism have also emerged. And cyber-attacks – such as those by foreign Organised Crime Groups (OCGs) targeting the UK for financial benefit – have also increased in frequency.[9]

One important feature of cybercrime and cyber- enabled crime is that they do not respect policing jurisdictions. As we become a more digital society, the likelihood of offenders and their victims living in the same local community is diminishing. Crime is more likely to involve networks operating across numerous jurisdictions. Relevant digital data is also sometimes only available in other jurisdictions, requiring cooperative national and international partnerships to access it. In one recent bribery and money laundering case, over 100 electronic devices were seized in another country at the NCA's request and the NCA, for legal reasons, had to build a digital forensics laboratory there 'to allow their authorities to process and analyse the material before transmitting it to the UK for NCA digital review and analysis.'[10]

This does not mean that cyber and cyber-enabled crime has no local footprint. On the contrary, in interviews conducted as part of the research for this report, more than one senior police officer assessed that around 90 per cent of local crime now left some sort of digital footprint or had been cyber-enabled in some way. This

4 NAO (2018).

5 College of Policing (2015); NPCC (2017); Muir (2017).

6 ONS (2019).

7 Digital Policing Portfolio (2018).

8 NCA (2017).

9 NCA (2017).

10 NCA (2018)

reality is becoming part of the everyday experience of local policing. And as the NCA has noted:

> *"The growth of online marketplaces with off the shelf cyber-tools is placing high-end tools in the hands of less sophisticated criminals. This presents challenges for police forces, who must be equipped to deal with cyber offending at an unprecedented scale, affecting a large number of local victims."*[11]

It is also already clear that the onset of a digital society is creating new and profound challenges for the police. The volume of digital forensic material being seized for all types of crime, to give just one example, is massive. The is because the public now leaves behind a much bigger trail of searchable information for the police to engage with. As The Economist recently noted:

> *"Smartphones passively track and record where people go, who they talk to, and for how long; their apps reveal subtler personal information, such as their political views, what they like to read and watch and how they spend their money.' If a person drives, 'police cars, streetlights and car parks equipped with autonomous number-plate readers (ANPRS) can track all his/her movements."*[12]

The volume of this digital data threatens to overwhelm the police's capacity to handle it.[13] The NCA, Metropolitan Police Service (MPS) and the National Police Chiefs' Council (NPCC) recently reported to parliament that in one case led by the MPS, 'a simple case involving two mobile phones resulted in 20,000 items of data (messages, photos, internet history) needing to be examined, which took around 150 officer hours to review and schedule. This is but one example; in 2015 MPS forensic staff examined 40,000 devices and in 2018 it is likely to be 200,000').[12] Unless new ways of dealing with this problem are found, some police forces will be unable to cope with this workload, leading to failures to catch criminals, or to miscarriages of justice because digitally available data was not examined, or both. The consequences for public confidence in the police could be profound.

The police are also now having to deal with a public that is used to living far more of its life online. Work conducted for the Metropolitan Police Service (MPS) and the Mayor's Office for Policing and Crime (MOPAC) in London confirms that this is translating into a public appetite to engage with the police using digital channels. Although it showed that the reporting of crime through different channels had remained broadly the same over the last three years, with around 70 per cent of crime reported on the phone, around eight per cent at counters, and with very little reported online, this is attributed by MOPAC and the MPS to the limited digital options made available to the public at the time. When Londoners were asked about the future, and how they would prefer to contact the police, 'the proportion wanting to use online reporting methods increased significantly to 37 per cent across the website, social media and other digital methods (such as live chat).'[13] Among Londoners aged 18 and over who had accessed the internet at some point in the last 12 months, 95 per cent said they would either strongly consider or were open to using a police online service in future.[14] And even among the 65-75 age group, that number only fell to 91 per cent.[15] If the police do not fully embrace the potential for online interaction, there is again a danger that they will fail to provide the type of service the public expects in the 21st century. Again, the potential impact on public confidence could be profound.

All this amounts to a radically changed landscape for UK policing and as the next chapter makes clear, there is no reason to believe the pace of change will ease off. If anything, it is likely to increase, criminal use of new technologies is likely to expand and become ever more sophisticated, and the police will need to run just to stand still.

11 NCA (2017).

12 The Economist (2018b) p. 3.

13. NCA (2017) p.6, para 30.

14 NCA, MPS, NPCC (2018).

15 MOPAC, MPS (2017).

16 MOPAC, MPS (2017).

17 MOPAC, MPS (2017).

3. THE NEAR HORIZON

In this chapter, we take a closer look at some of the newer technological developments of relevance to policing and crime. There are a number of these developments and a whole paper could be dedicated to each of them separately. Notable developments include the emergence of 5G networks and the growth in criminal use of encryption. Here, however, we focus on two other phenomena that we think are likely to have a growing and major impact on the policing and crime landscape *in the near term*. These are the internet of things and blockchain. Both not only add complexity to the existing landscape of crime and policing but actually introduce whole new domains in which crime can be committed, investigated and prevented. Each is examined in turn.

3.1 THE INTERNET-OF-THINGS AND CRIME

It is projected that by 2020, 31 billion devices will be connected to the internet worldwide, rising to more than 75 billion by 2025. Analysts predict that smart cities (26 per cent), industrial devices (24 per cent), and connected health (20 per cent) will dominate this growth but other sectors will be involved too. It is thought smart homes technology will account for around 14 per cent of growth, connected cars seven per cent, smart utilities four per cent and wearable technology three per cent.[18]

From connected traffic cameras and sound monitors to pacemakers and Fitbits, smart cars, doorbells, watches, phones, coffee-makers and home or virtual assistants, connected devices are going to be, and in many cases already are, gathering vast quantities of data on our habits, movements and environments and sending it back to manufacturers who hope to either mine it or sell it for commercial advantage. This will also mean that new data is increasingly available and accessible from the huge number of connected devices involved.

This historic trend will have two major consequences for policing and crime. First, it is increasing the 'attack surface' of interest to criminals and new risks are being created as a result. In 2015, hackers demonstrated to WIRED magazine that they could remotely hijack a Jeep's digital systems over the internet, resulting in the manufacturer, Chrysler, recalling 1.4 million vehicles.[19] In future, hackers may demonstrate that they can hack not only individual vehicles, but whole fleets of vehicles, effectively taking control of them remotely. Another example of an attack was the Mirai botnet distributed denial- of- service (DDoS) attack on the Dyn domain name system (DNS) in October 2016.[20] This took major internet brands like Twitter, Paypal, Netflix and Facebook temporarily offline. The attack was facilitated via the hacking of devices like CCTV security cameras and baby monitors with software that commanded them to attack and overwhelm Dyn's servers. Dyn's initial estimate of the size of the attack indicated that it had involved tens of millions of hijacked devices.[21] The Mirai software scanned connected devices continuously and such is the weak level of security on many of them that it was able to use well-known factory default passwords to gain access.

One specific new risk is related to the distribution of ransomware onto devices which, as the name implies, will only be removed once the targeted individuals or institutions have paid a ransom.[22] Ransomware often encrypts a user's files, effectively locking them out of their own IT systems until the ransom is paid. The most high-profile case in the UK so far was the May 2017 attack on the NHS, which successfully, though only temporarily, shut down large parts of the NHS IT system. The potential for such attacks is huge, and not restricted to any particular sector. Similar attacks are possible against connected industrial and transport safety systems, as well as against commercial entities and services.

It is not only institutions and systems that are at risk but also individuals. Many connected devices hold personal information, which in some cases could include compromising personal messages that criminals could use for purposes of blackmail. Some devices hold information on the status of home management

18 Columbus (2017).

19 Tech UK (2017).

20 Symantec (2016).

21 Dyn (2016).

22 Tech UK (2017) p.4.

systems that could let criminals know when a home-owner is not at home. And some devices may be of little concern as holders of information in their own right, but may serve as gateways to whole networks of greater value to criminals, or just to specific pieces of more valuable information stored elsewhere. Mike Barton, the Chief Constable of Durham Constabulary, has been explicit, and right, in warning of this danger. '"If your fridge is connected up to your local supermarket so that it can order things when they are needed, then it's going to be connected to your bank account and it's that, that is the worry. That all of these devices, none of which are seen as that threatening or that necessary to protect, become the open back door."[23] For this reason he has also warned that the internet of things is likely to lead to a 'crime harvest' not least because the manufacturers of many connected devices fail, in their rush to get products to market as quickly as possible, and at the cheapest price, to embed any security measures into their devices at all.[24]

There are even fears, expressed in a recent F-Secure report, that embedded medical devices such as pacemakers could be hijacked by criminals who could demand a ransom in return for not manipulating those devices in ways that might be life-threatening to those wearing them.[25] If this seems far-fetched, it is as well to note that the former Vice President of the United States, Dick Cheney, confirmed in an interview with CBS in 2013 that his heart pacemaker had had its wireless function disconnected to prevent a possible assassination attempt by hackers.[26]

Second, the advent of the internet-of-things is going to change the game when it comes to police investigations. Police officers increasingly need to get up to speed with the data that connected devices hold, and with how that data can be accessed, preserved and used as evidence. Challenging though this may be, it is going to be a necessity. As the Head of the Digital Forensics Lab, Mark Stokes, told the Times newspaper in January 2017: 'The crime scene of tomorrow is going to be the internet-of-things.'[27] And as noted in the previous chapter, accessing it is going to present a potentially massive challenge for the police in terms of workload. It will also often mean engaging with third party holders of the data, some of whom may not even be in the UK. The onset of the internet-of-things is therefore going to create logistical, jurisdictional and sometimes legal challenges. We should expect it to also create ethical and political ones as well since accessing data via devices linked to specific individuals may involve major invasions of privacy and a fundamental, and at this stage unregulated, shift in the relationship between the police and the public.

3.2 BLOCKCHAIN

If anything, the impact of blockchain technologies might be even greater.

Blockchain is a shared distributed ledger (like a digital record book) that records transactions and tracks assets across a network. It is called blockchain because it stores data in blocks that are linked together to form a chain. Each block confirms when a transaction took place and contains a hash that forms a unique identifier linking the blocks together.

The hash is cryptographically generated and the transactions on a blockchain are immutable. They can be seen by every participant in the chain, and they cannot be changed without everyone in the chain knowing about it.

On top of this platform, cryptocurrencies have been developed. These use the distributed nature of blockchain to facilitate peer-to-peer cash payments that do not need to be routed through a bank. Payments can be sent directly from one party to another and are logged in an encrypted but publicly available distributed ledger, so that the same money cannot be spent twice or counterfeited. Given that the transactions are recorded in a decentralized network of computers, the system is said to be impossible for hackers to corrupt.

The problem for law enforcement is twofold. First, with banks and other financial institutions cut out of the loop, the police lose a vital source of information on financial transactions that often help them to build cases against criminals and to secure convictions. Second, given that the identities of those conducting the transactions, and the transactions themselves, are encrypted, it is also very hard for the police to be able to link specific payments to specific individuals.

23 Palmer (2018).

24 Palmer (2018).

25 F-Secure Cyber Security Research Institute (2018).

26 Vaas (2013).

27 Tech UK (2017).

The criminals have noticed, and have become enthusiastic users of cryptocurrency platforms to facilitate crimes such as money laundering.[28] Rob Wainwright, the former head of Europol, is on record stating that he believes some three to four per cent of the continent's annual criminal takings of £3bn to £4bn are crypto-laundered, and he thinks the problem will get worse.[29] Michael McGuire of the University of Surrey has also logged many examples, and methods of crypto-laundering.[30]

Bitcoin has received a lot of the attention, and rightly so. One analysis from the University of Technology in Sydney found that one quarter of bitcoin users, and a half of all bitcoin transactions, were associated with illegal activity. In 2017, that amounted to an estimated value of $72bn, a sum close to the US and European markets for illegal drugs.[31] But there are over 1,500 cryptocurrencies in operation and some of them are better at protecting user identity than bitcoin itself. Europol has warned that cryptocurrency exchanges such as Monero, Ethereum and Zcash are becoming favoured platforms for criminal activity.[32] And an analysis by Blockchain Intelligence Group estimated that illegal activity accounts for about 20 per cent of all activity across the five cryptocurrencies of bitcoin, Monero, Zcash, Ether and Litecoin, amounting to a value of around $600 million a day.[33]

Cryptocurrencies and the platforms and exchanges they are traded on are themselves also becoming new focal points for crime, and not only as places to hide the proceeds of crimes committed elsewhere. According to the Anti-Phishing Working Group (APWG), criminals reportedly stole just under £1bn in cryptocurrencies between the beginning of January 2017 and May 2018.[34]

Some of these thefts took the form of physical attacks on cryptocurrency owners. But phishing attacks are commonplace too. Chainalysis, a research firm that monitors activity on blockchain platforms, found evidence of "more than $115 million worth of stolen value affecting nearly 17,000 victims on the Ethereum blockchain alone."[35] Cryptophishing usually involves fraudulently persuading investors looking for cryptocurrencies to invest in to send money to the wrong address, in just the same way that email phishing works to persuade vulnerable and/or gullible investors to part with their money. Crypto-Ponzi schemes are also in evidence. The US Federal Trade Commission recently opened a case against cryptocurrency company My7Network for just such a scheme in which it is alleged that participants were encouraged to buy bitcoins, donate them to earlier 'upline' investors, and then help to recruit a new wave of investors to come in and do the same for them.

Another area of concern is the use of cryptocurrencies to fund terrorist organisations. On 28 August 2015, Ali Shukri Amin, a resident of Virginia in the US, was sentenced to eleven years in prison for conspiring to provide material support and resources to Islamic State.

The Financial Action Task Force, an independent NGO, reported that Amin had 'tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilise this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system "to send money, using bitcoin, to the mujahedeen."[36]

Looking ahead, there appears to be a likelihood that the technology to provide and protect anonymity will get better and better creating a major headache for the police. In some extreme scenarios, the technology will put criminals just beyond reach and raise profound questions about whether the policing of a digital society is actually possible to anything like the same extent we have become used to in the offline world. Some are also not so sure that blockchain platforms will remain impossible to hack. The 'Heartbleed' bug that affected cryptographic software in 2014 is pointed to as an

28 Ramey (2018); Bloomberg 2017.

29 The Economist (2018c).

30 McGuire (2018).

31 Foley et al (2018).

32 O'Leary, R. (2017); Greenberg, A. (2017).

33 Ramey (2018).

34 Chavez-Dreyfuss (2018).

35 Watkins (2017),

36 FATF (2015).

example of what could, potentially, go wrong. If a similar problem hit one of the major cryptocurrency platforms, given the scale of their current use, the concern is that billions of pounds could be stolen before anyone knows about it.[37]

While dark market usage of cryptocurrencies may still represent only a small percentage of the use of such currencies overall, as their use grows, the numbers of crimes committed, the numbers of victims affected, and the economic value of crypto-currency crime all seem set to increase. We can expect blockchain technology and the cryptocurrencies it facilitates to feature more and more prominently in debate among policing practitioners and policy-makers alike as a result.

37 Watkins (2017).

4. INNOVATION CASE STUDIES

It is not, however, only the criminals who are using technology. There is a stated desire and intent on the part of police leaders in England and Wales to adapt to, and embrace today's digital society. This is perhaps most clearly expressed in the Policing Vision 2025 published by the National Police Chiefs' Council (NPCC) and the Association of Police and Crime Commissioners (APCC).[38] In that document, police leaders commit, among other things, to use digital policing to:

- Make it easier for the public to contact the police wherever they are in the country.
- Make better use of digital evidence and intelligence.
- Transfer all material in a digital format to the wider criminal justice system.

They also agreed to deliver these outcomes by:

- Using new technology to communicate with citizens who are living more of their lives online.
- Gathering comprehensive information about victims, offenders and locations quickly, often through use of mobile devices, and using analytics to help target police resources more effectively on the basis of the insights generated.
- Developing digital investigation and intelligence capabilities to improve understanding of the digital footprint of crime, so as to more effectively counter it.
- Giving the workforce the digital tools and expertise necessary to investigate all incidents and crimes effectively and efficiently.
- Improving data sharing and integration to establish joint technological solutions and the transfer of learning across and between forces and other agencies.
- Working with the Police ICT Company to prioritise investment in developing common data standards and encouraging national approaches to technology investment, future capability development and identification of skills and training requirements.

The Digital Policing Portfolio (DPP) has been central to the implementation effort, leading three core streams of work across Digital Public Contact, Digital Intelligence and Investigation (DII), and what became known as Digital First (the attempt to integrate digitised policing with the wider the criminal justice system). Individual forces are also running innovative data-driven projects up and down the country.

We review the evidence emerging from some of this work in this chapter, but also cast the net much wider beyond both policing in this country, and beyond policing itself, to examine innovative uses of digital and data-driven approaches by private sector organisations and citizens groups, where these are relevant to the police and crime agenda. We make no claim, of course, to be exhaustive. The material presented here is a mere snapshot of a fraction of what is going on and there is far too much innovation under way to describe all of it in a single report.

Our focus throughout, however, is on showcasing activity that relates to the delivery of public value through its impact. Where evidence of impact is not yet publicly available, we point to use cases where data-driven approaches are likely to deliver impact and public value in future. Given this focus, the material in this chapter is organised not according to the type of technology in use or the specific sector deploying it, but around each the nine dimensions of public value we identified in Chapter 1. To recap, we defined public value as deliverable through:

- Reducing crime.
- Improving crime detection.
- Reducing public fear.
- Reducing public vulnerability.
- Action to ensure civility in public spaces.
- The use of police authority and force in a fair and just way.
- Action to improve public trust and confidence in the police and the wider criminal justice system.

38 NPCC, APCC (2016).

- The delivery of a quality service experience to citizens.
- The efficient and fair use of public funds.

We deal with each in turn.

4.1 REDUCING CRIME

With regard to reducing crime, the use-cases of a data-driven approach are already clear, and the evidence base with regard to what such an approach can deliver is starting to mount.

Chicago Police Department

The Chicago Police Department (CPD) is using data integration and analytics programmes to both predict and prevent violent crime across the city. Civilian analysts and police officers are working together in Strategic Decision Support Centres (SDSCs) deployed, as of May 2018, in 13 of 22 police districts across the city. These bring together data from surveillance cameras and gunshot detection systems with analysis of data on previous crime patterns to identify the places where violent crime is likely to occur. The evidence suggests they are already having a significant effect. While 2016 was the deadliest in Chicago for 20 years, with 3,550 shootings and 762 murders, in 2017, the year in which the SDSC approach was initially deployed, those numbers fell to 2,785 shootings and 650 murders. The falls were steeper in the areas with a functioning SDSC than in those without and in some districts, the change was startling.[39] In the district of Englewood, a poor, mainly black neighbourhood, shootings fell by a massive 67 per cent and murders by 44 per cent.[40] While full causality cannot be demonstrated, there is a correlation between SDSC deployments and the steepest falls in violent crime and the CPD itself believes the SDSCs, and the different community relations and early interventions they have stimulated, are key to the improved outcomes. In April 2018, CPD Police Superintendent Eddie Johnson told the public that improved use of technology had contributed to 'twelve straight months in a row of sustained gun violence reductions.'[41] In the first three months of 2018, shootings were down a further 34 per cent on the same period in 2017 in the districts with a functioning SDSC, compared to a 28 per cent reduction across the city as a whole.

Vancouver Police Department

The Vancouver Police Department has also implemented a city-wide predictive policing tool to target property crime. The system uses machine learning to predict where break-ins are likely to occur. It pushes that information to the onboard computers of patrol vehicles at two hourly intervals so officers can alter their patrol locations with a view to preventing them. Predictions are offered within either a 100 or 500-metre radius of a particular location. A six-month pilot project in 2016 saw property crime reduced by as much as 27 per cent in areas where it was tested, compared to data held on the previous four years. The accuracy of the system was also tested by generating predictions of locations for property crime on a given day, and the police then monitoring what actually happened without taking steps to intervene. According to the VPD Chief Officer, Adam Palmer, it achieved up to 80 per cent accuracy in those tests.[42]

Avon and Somerset Police

Avon and Somerset Police has begun moving in a similar direction. It has rolled out Qlik Sense, a software tool that can extract data from more than ten separate police databases and link it together, along with data from emergency call logs and long-term data on recorded crimes in the area. On top of that, software developers working within the force have put together more than 40 apps that can be used to conduct searches of the entire dataset, based on features such as a suspect name, an address, or a number plate.[43] This overcomes a common problem facing many police forces, which is that they do not know what they know, because up to now it has been too time consuming and costly to query every database held by a force and to build up an overall picture. That task now happens in seconds.

The real value of the system is that it can then combine predictive analytics with data visualisations to give officers a much better idea not only of any situation and immediate context they are facing but also of the places and individuals likely to be at highest risk

39 The Economist (2018a).

40 ABC17 Chicago (2018).

41 Schuba (2018).

42 CBC (2017).

43 Background interviews with responsible officers in Avon and Somerset Police.

and vulnerability, and they can alter force deployment decisions, strategy and even operational tactics as a result of that insight. Anecdotal evidence from early use of the system indicates that the better resource targeting and problem management that this is allowing is beginning to reduce demand across key areas.[44] Survey data from users of the system also indicates that 67 per cent of users think it makes them better informed and 56 per cent that it makes them more effective.[45] Adam Crockford, one of the officers who oversee significant incidents, has said of Qlik Sense that it helps officers to "prioritise the priorities" at a time of tight resources, a crucial point given that the number of officers in Avon and Somerset is down 15 per cent from 2010, and the force's budget has been cut by 18 per cent over the same period.[46]

Further areas of impact highlighted by the force include:

- Greater visibility for call handlers and supervisors have helped improve responsiveness, with Avon and Somerset now having one of the lowest abandoned 101 call rates in the country.
- Supervisors now have more performance information which has led to more timely supervisor reviews and risk assessments.
- Neighbourhood teams are able to be much more focused on high demand places and people, allowing for more targeted problem solving activity.
- Professional standards departments have become more timely in resolving complaints following the deployment of Qlik on their case management processes.

Tests of the software to see how and whether it might have prevented serious failures in the past have also powerfully demonstrated the potential value of this new approach. In one very serious case from 2013, in which an Iranian refugee, Bijan Ebrahimi, was murdered in Bristol despite having previously made dozens of calls claiming he was being harassed by neighbours, the finding was clear. At the time, he was largely dismissed as a nuisance. But tests of predictive analytics software have shown that he would have been flagged as one of the most at risk potential victims in the entire force area. While no-one can be sure, there is reason to believe that had the new data integration and analytics platform been in use, that murder may have been preventable.

West Midlands Police

West Midlands Police is also using a data-driven approach to deepen insight into the challenges facing its force area and is in the early phases of a planned series of pilot projects that use insight to change outcomes for the better. As with Avon and Somerset, over 80 previously unconnected information systems and databases have been brought together behind a single platform that allows officers to interrogate the data held via a single search. The new platform makes it easier to cut into and analyse the data the force holds in more powerful ways, generating new insights into crime patterns and into the networks of individuals that may be responsible. West Midlands Police has recently hired a small data science team to help facilitate this process and is beginning to focus in on specific crime challenges with a view to turning a better understanding of the problem into more effective, multi-agency crime prevention interventions.

Projects under development or early operation include an initiative focusing on young age violent offenders that not only identifies the likelihood of future offences being committed by an individual but also which individuals are likely to become influential hubs in wider networks of offenders. This should allow improved intervention in relation to those most likely to lead other young people into a life of crime. This powerful combination of data analytics with network mapping and analysis should be replicable in relation to other crime types and enable fresh discussion with other relevant agencies, as to how best to intervene to prevent violent and other types of crime in future.[47]

Argentina's use of electronic monitoring tools

Another data-driven approach to crime prevention has been demonstrated in Argentina. A study of electronic monitoring (EM) there looked at people linked to serious offences who received EM rather than a prison sentence. It found use of EM cut the risk of re-offending nearly in half, compared with a period in prison. Offenders in the EM programme received no additional counselling, education, training or other interventions. This suggested that EM provided an effective way to address recidivism rates and that the easiest way to keep people out of prison may be not to put them there in the first place.[48]

44 Private correspondence with Avon and Somerset Police.

45 Private correspondence with Avon and Somerset Police.

46 Wright (2018).

47 This paragraph draws on private conversations between the authors and officers leading the work at West Midlands Police.

48 Di Tella and Schargrodsky (2013).

Use of blockchain technologies to prevent crime

Outside the police and criminal justice sector altogether, a number of private sector organisations are using data-driven approaches to develop novel ways of preventing crime. One such example is Everledger's use of blockchain technology to combat the illicit trade in blood diamonds. These diamonds usually appear on the market as a result of a militia, rebel or government army in a conflict zone taking over a mine and using it to fund further violence and oppression. At the other end of the market, purchasers of diamonds cannot be sure of their origins. Everledger uses over 40 features of a diamond, including colour and clarity, to create a diamond's unique digital ID.[49] Once information is logged in the blockchain, it is both immutable and and can be checked by those processing a diamond, to make sure they are dealing with the same stone that is logged into the system. It is now possible to track a diamond that might have been mined in Colombia, cut and polished in India, shipped to wholesalers in Switzerland, and then passed to retailers in the UK and elsewhere.

In early 2017, in a further demonstration of how blockchain might be able to help counter fraud and unethical sourcing in the diamond market, De Beers, which mines, trades and markets over 30 per cent of the world's diamonds, announced that it would create the first blockchain ledger for tracing stones from the point at which they are mined right up to the point at which they are sold to the individual.[50]

The same technology is being applied to other precious stones, and also to combat counterfeiting of fine wines. Again, in the latter case, a unique digital ID for a bottle of wine is created using information about the bottle, the label and the cork, enabling its movements to be tracked, but also checked by everyone processing or potentially buying it.[51] Elsewhere, the online art world, which has been subject to increasing fraud, is being transformed by companies like Verisart, which digitally registers and authenticates artworks, tracks their movements, and both demonstrates their provenance and protects the rights of the original artist.[52] This should help to prevent cases like that of the three individuals prosecuted in New York in 2017 for counterfeiting Damien Hirst prints and selling them online for $400,000.[53]

This may be the tip of the iceberg with regard to crime prevention through the deployment of blockchain technologies.

4.2 CRIME DETECTION

Burgernet Netherlands

Burgernet Netherlands is a digital collaboration platform that allows the police in the Netherlands to work together with citizens to combat crime and create safer communities.[54] First introduced in 2009, it allows a police control room to send mobile alerts, in the form of either voice or text messages, to citizens who have chosen to participate, notifying them of incidents such as burglaries, the stealing of vehicles, cases of missing persons, or other criminal activity in their neighbourhood. This allows citizens both to be vigilant and to share any information they might have on the crime by calling the free Burgernet number whereupon they can be put straight through to the control room. The operator of the control room can then push intelligence out to officers in the field. At the end of any incident, all those who responded to the alert receive an update on the eventual result. Strong data security is an integral part of the system, to protect the identities of those who contribute.

Burgernet was first trialled in nine municipalities in 2008-09 and since then has been rolled out across the entire country. It now has approximately 1.6 million citizen participants who are estimated to be involved in 1,700 to 2,000 Burgernet 'actions' per month. Of these, an average of 10 per cent directly lead to the police being able to make an arrest. Another 40 per cent are said to play some indirect but valuable role in helping the police investigation process. In March 2017, the Netherlands Police decided the scheme had been sufficiently successful to warrant the building of Burgernet 2.0. This will expand the network further onto social media platforms and allow citizens and the police to exchange, in real-time, videos and photos to aid the crime reporting and detection process.

49 Volpicelli (2017).

50 Marr (2018).

51 Volpicelli (2017).

52 Thomson (2015).

53 Rodrigues and Urban (2018).

54 For an overview of the system and how it works, see: https://www.burgernet.nl/content/over-burgernet

Facial recognition in the state of New York

Another notable crime detection initiative has been developed in the state of New York. Governor Andrew M. Cuomo announced publicly in August 2017 that the New York Department of Motor Vehicles (DMV) had used facial recognition technology to identify over 7,000 cases of possible identity theft and fraud in the preceding 18 months. This had been achieved through a major technology upgrade to the system in January 2016 that doubled the measurement points used when examining each driver's photograph. As a result, the capability of the system to find matches of new identities being entered into the system with ones already there was vastly improved, helping to identify those trying to use multiple identities. Investigations resulting from matches found led to 4,000 arrests and another 16,000 people facing some sort of administrative action. Cuomo subsequently described the facial recognition technology as central to law enforcement's ability to crack down on identity theft, fraud and other crimes. The DMV no longer issues a new driving licence without the associated driver photograph being cleared through the facial recognition system.[55]

The internet-of-things as an aid to crime detection

Beyond these specific case studies, it is possible to point to the internet-of-things as a whole as a new use case with regard to crime detection.

When police started using distributed gunshot detection sensors called ShotSpotter in Camden, New Jersey, for example, they found that 38 percent of gunshots in one neighbourhood were not being reported or detected at all. This enabled the police to focus more resource on that area than previously had been the case.[56] Moving forward, visions of the future smart city envisage connected devices managing traffic flows, public lighting and other systems. If these systems were integrated with sensors and cameras across the cityscape they could have huge crime detection potential. One idea is to integrate ShotSpotter with connected streetlight systems to help manage the response to firearms incidents. A recent commentary in Police Chief Magazine in the US painted the picture:

> *"With a Safe Cities integrated technology approach, upon discharge of a firearm, the streetlights in the area (assuming it's dark at the time) would immediately be brought to higher brightness. Video surveillance equipment in the area would be activated and turned in the direction of the gunfire and license plate readers would be activated to capture license plates in the area. The video would be captured and transmitted to the command and control facility and could then be relayed to the responding officers."*[57]

More widely, the potential is that with enough connected devices deployed, law enforcement officers would be in a position to quickly know, in serious crime cases, where potential suspects were at the time of a crime, who they were with, and what they were doing. A joint venture between Microsoft and the NYPD called Domain Awareness System already provides some of this functionality in New York City by pulling data together from the thousands of CCTV cameras, hundreds of ANPR systems, and other data sources available in the city. The NYPD now says it can track where a suspect's car has been for months past, and can alert police officers on patrol to any criminal history linked with a specific number plate.

Cases are also now emerging where evidence gathered from internet connected devices is proving crucial in making arrests. In the UK, one case of multiple burglary was solved after BT wifi routers were examined in a row of four houses, each of which had been broken into in the middle of the day. The routers showed that the same mobile phone had connected to the free BT-FON service at each of the houses on the day the burglaries had taken place. The police were able to use that information to track down the perpetrator.[58]

In the United States, a number of more serious cases have clearly demonstrated the crime detection potential of internet connected devices. For example:

> *"Richard Dabate claimed a would-be burglar beat him and shot his wife, Connie, in their home in Ellington, Connecticut, shortly before Christmas in December 2015. But she was wearing a Fitbit that showed her walking 1,217ft around the house well after the time her husband said she was shot. When detectives checked her phone they found a list titled: 'Why I Want a Divorce'. Dabate's murder trial is pending."*

55 New York State Governor (2017).

56 CBS (2015).

57 Searcy (2017).

58 This paragraph is based on a background interview with a senior UK police officer aware of the case.

'Ross Compton said he was sleeping when his house in Middletown, Ohio, caught fire in September 2016. He said he grabbed some possessions and jumped out a window. Investigators pulled data from his pacemaker which, according to a cardiologist, undermined Compton's account. He has been charged with aggravated arson and insurance fraud."[59]

It is clear already therefore that if the police do not rapidly ramp up their ability to analyse the available digital data, many serious crimes could go unresolved in future, even though the evidence exists to lead to prosecutions. It is this reality that is driving the growth in numbers of digital media investigators (DMIs) recruited and/or trained by the police. In Hampshire for example, where some officers believe 90 per cent of all crimes now leave some sort of digital footprint, moves are afoot to increase the number of DMIs from 40 to 70.[60]

4.3 REDUCING FEAR

Another area where a data-driven approach is increasingly in evidence concerns the management of major emergencies and public incidents. A prime example is the management of one such incident in 2017. On a late November afternoon, the police were called to Oxford Circus amid reports of gunfire at the tube station, and online videos showing people running from the scene. It appeared that a full- blown terrorist incident was under way, possibly in a number of different locations in that part of the city.

The far-right activist, Tommy Robinson, began spreading the word on Twitter that this 'looked like another jihad attack.' The singer, Olly Murs, tweeted to his 8 million followers from Selfridges: 'Fuck everyone get out of Selfridges now gun shots !!'. As some shoppers fled the store, others were running into it from outside in search of safety. The whole incident was being shared on social media in real-time, stoking a considerable sense of public panic.[61]

As the police investigated however, it became clear that it was a false alarm, triggered most likely by a minor scuffle between two men on the underground station platform. While the police had initially responded to calls and social media posts related to the incident with an armed response, over the next 60 to 90 minutes they used the Metropolitan Police twitter feed to calm the situation and give information and advice to the public using the hashtag #OxfordStreet. Between 17.16 and 18.06 that evening, they put out the following tweets to effectively demonstrate control of the situation:

*17.16: Police called at 16:38 to a number of reports of shots fired on #**OxfordStreet** & underground at Oxford Circus tube station. Police have responded as if the incident is terrorist related. Armed and unarmed officers are on scene and dealing along with colleagues from @BTP (British Transport Police)*

*17.17: If you are on #**OxfordStreet** go into a building and stay inside until further direction. Avoid travelling to the Oxford Street area. At this stage police have not located any causalities.*

*17.39: Police remain on scene in #**OxfordStreet** Oxford Circus – no evidence of shots…*

*17.42: We have not located any trace of suspects, evidence of shots fired or casualties. Officers still on scene. If you are in a building stay there, if you are on the street in #**OxfordStreet** leave the area. Officers continue to search the area. More updates as soon as we have them.*

*18.04: Our response on #**OxfordStreet** has now been stood down. If you sought shelter in a building please now leave, and follow the direction of police officers on the ground if you need assistance.*

*18.06: Additional officers remain on duty in the West End to reassure the public. We thank the public for their patience and assistance during our response. If you see anything suspicious dial 999 immediately #**OxfordStreet***

This incident illustrates both how important it is for the police to be monitoring social media data streams today and how social media is increasingly important to their own ability to influence public behaviour in times of emergency or public stress. This trend is only likely to continue and grow.

59 Carroll R. (2017); Lartey (2017)..

60 Interview with senior member of Hampshire Constabulary.

61 Davies (2018).

4.4 ENSURING CIVILITY IN PUBLIC SPACES

One of the most interesting examples of using data-driven technologies to promote civility in public spaces has come via technology enabled citizen activism. In many locations, the public are now capturing video in the hope of ensuring both the fairness of citizen-police interactions, and the prosecution of those involved in violent and other types of crime. A number of highly controversial cases where the police have used lethal force in the United States has triggered some of this.

In March 2017, the American Civil Liberties Union (ACLU) of Texas launched its ACLU Blue App. This allows citizens to upload video of interactions they have witnessed between the police and the public. The video is reviewed by ACLU staff and then uploaded to the ACLU Texas Youtube page where it can be viewed not only by lawyers acting on behalf of members of the public who believe they have been the victims of police misconduct but also by the public at large.[62] The aim is to showcase not only negative incidents but also examples of positive police behaviour. The ACLU Blue App is just one of many that have been developed and most of the others are designed to redress the balance in terms of what is often seen as unjustified use of force by the police. Other apps such as Mobile Justice, CopWatch and Stop and Frisk, offer a way to capture video and quickly upload it to a public party before law enforcement officers try to interfere with the recording (something that has been known to happen on a number of recorded occasions in the US).[63]

In the UK, a number of police forces have begun moving in a similar direction, helping to provide such apps to the public. Examples include hate crime reporting apps developed by both the Metropolitan Police and by West Yorkshire Police. A cyber harassment app to monitor and help police online activity is also in the early stages of development in Bedfordshire Police.

4.5 IMPROVING PUBLIC SAFETY/REDUCING VULNERABILITY

There have also been a number of data-driven innovations with regard to both improving public safety and reducing vulnerability.

Artificial intelligence and machine learning to combat child sex trafficking

In the United States, hundreds of police forces and thousands of police officers are now using artificial intelligence and advanced facial recognition tools to identify young, vulnerable people being trafficked for sex, and to also identify the individuals organising the trafficking operation and profiting from it behind the scenes. Some forces in the UK are also now experimenting with these tools. The software being used draws on archives of millions of records of previous escort and sex ads and related forum data collected from public websites. Some of the tools being used conduct analysis of text used in advertisements, picking up patterns in language that might indicate offers of under-age sex and generating new leads for the police. Some use powerful advanced facial recognition tools to identify the same young person being advertised in a number of different places and at different times. These tools frequently identify matches between photos of the same young person which at first glance look like different people and would previously have been missed by officers. The ability to better identify suspicious advertisements, make connections between images being used in different places, and to investigate phone numbers that are being used in multiple advertisements is putting powerful new investigative tools into the hands of law enforcement.

The 2017 Impact Report of Thorn, a US non-profit organisation providing some of these tools to the police, presents survey data drawn from law enforcement users of its products. It states that in that year, 18,119 victims of child sex trafficking were flagged by officers using its tools, 5,791 children were individually identified, and 103 were rescued from situations where their abuse was being recorded and distributed.[64] Some 6,553 traffickers were also identified, allowing the police to engage in targeted disruption and arrests.[65]

62 CNN (2017).

63 See a short video on these apps at: https://edition.cnn.com/videos/us/2015/10/01/civil-rights-app-breaking-ground-orig-jl.cnn/video/playlists/breaking-ground-orig/

64 Thorn (2017).

65 Thorn (2018).

Other human trafficking

Such tools are also being used by those involved in the monitoring and investigation of other types of crime such as wider human trafficking.[66] In Arizona in the United States, the Transaction Record Analysis Center (TRAC), a non-profit organisation affiliated to the Arizona Attorney General's Office, has used tools from other AI providers to link its database of approximately 75m financial transactional records to data on phone numbers and images being used in advertisements to more effectively map trafficking networks and to identify their victims. TRAC accesses data on transactions over $500 obtained from 14 of the world's largest money service businesses (MSBs), including Western Union, Moneygram, and Ria in Texas, New Mexico, Arizona, California, or the entire country of Mexico. For each such transaction, it receives a name, date of birth, ID number, telephone number, and any address provided by the person sending the money, as well as the location the transaction was initiated from. TRAC also receives the same information for the individual the money is being sent to, along with the store location where he/she picked the money up. It uses this data to help identify patterns of activity related to crime. When it decided to get more involved in the fight against human trafficking, it initially faced the difficult task of manually running Google searches on individual telephone numbers suspected of being related to sex trafficking. Now however, TRAC is able to query hundreds of thousands of telephone numbers on a daily basis, linking numbers being used in financial transactions and sex advertisements at the same time, which means that the users of the TRAC database (some 6,000+ law enforcement officers) can identify sex traffickers receiving proceeds from victims far more quickly and effectively.'[67] The software being used is enabling law enforcement officers to uncover traffickers that were previously out of sight, and is leading to new indictments as a result.[68]

Durham Constabulary Harm Assessment Risk Tool

In the UK, another notable innovation to help improve public safety has come in the form of the Durham Harm Assessment Risk Tool (HART). This was 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 also to help achieve more consistent decision-making and, through more effective decision-making and offender triage, get offenders on to the most effective path to desistance in committing crime, and therefore to help keep the public safe.[69] This could also ultimately produce cost savings and longer-term reductions in harm to the public. 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 forces 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. The Durham Constabulary has been very clear that the HART system is only an aid to decision-making and not the decision maker itself. Decisions remain with the custody officer's judgement.

An independent validation study of the tool was conducted in 2016 with custody data for the whole of 2013. The model's forecast for each single custody event in 2013 were compared to the actual known outcomes over the two years since. The overall accuracy of the model was 62.8 per cent. However, of all those who actually displayed high-risk behaviour, only 52.7 per cent were forecast to be high risk in the validation test. While this figure seems low, at least it is transparent. It is hard to know whether that level of accuracy is better or worse than the judgements being made by individual custody officers in the past because those statistics have not previously been available. Moreover, for what might be considered the worst form of error, the judgement of someone as low risk who turns out to be high-risk, the error rate was only 2.4 per cent. Accuracy rates for the low risk category were also themselves much higher, at around 75 per cent.

66 Melendez (2017).

67 The description of TRAC here is drawn from private correspondence between the software company involved and senior TRAC officials, provided to the author on a background basis. However, Rich Lebel, the Director of TRAC has also gone on public record in praise of the software and the ways in which it is transforming TRAC's counter trafficking effort. See Kupper (2018).

68 An example of a publicly available case study where facial recognition software has been used to help secure an indictment can also be found here: Marinus Analytics (2018). https://www.cs.cmu.edu/news/ai-good-spinoff-success-story

69 Sherman and Neyroud (2012).

These were achieved by the system erring on the side of being too cautious rather than not cautious enough, meaning that some people who were actually low risk were classified over-cautiously as moderate or high-risk. Some might consider this to be the correct bias for the system to have, given the need to prioritise the safety of the public.[70]

These accuracy rates in the system were achieved drawing only on data from within Durham Constabulary. The system was not drawing on data from other local agencies or national systems such as the Police National Computer or the Police National Database. Were it to do so, and should other systems do so in future, it is reasonable to expect algorithmic accuracy to improve. Such approaches and technologies are being tried elsewhere, and though controversial, the pressure to be consistent on one hand, and to achieve both the most cost-effective outcome and the best result for both the public and the offender will mean they are likely to become more widely experimented with.[71] We return to some of the issues raised by this kind of innovation in the final two chapters of the report.

Staffordshire Police's use of social media

Staffordshire Police's use of social media has also demonstrated an important use case with regard to attempts to protect some of the most vulnerable in society. One case, reported in February 2017, concerns their response to a report of a missing woman who was thought to be suicidal. The report that the 32-year-old woman had gone missing was received in the early hours of a Saturday morning. The police acquired a photograph of her and information on the general area in which she had last been seen, and were able to distribute that data quickly by posting it on to their Facebook page within 40 minutes of the initial call being received in the police control room. At around 2am, a barmaid finishing a shift in a rural pub logged on to her personal Facebook page and, because she had previously 'liked' the Staffordshire Police Facebook page, saw the alert. She responded, on Facebook, with a comment on the police posting to say she had served the missing woman earlier that evening. The police asked the barmaid to phone in and when she did, she was reportedly surprised to find the control room expecting her call. On the basis of that call, a patrol car was dispatched and focused on the area between the pub and the missing woman's home address. She was found a short time later, at about 2.45am, unconscious at the side of the road having taken an overdose. In the time between the police posting the initial alert and the appeal being closed at 3am, some 7,200 people had seen the police Facebook post and 330 had either shared or commented on it, offering a powerful demonstration, even in the early hours of the morning and in a rural area, of the way in which the police can distribute acquired information directly to the public and quickly receive actionable intelligence in response.[72]

The internet-of-things, virtual reality and public safety

We can expect both the internet-of-things and virtual reality to play bigger roles in approaches to public safety. A Tech UK report on policing and the internet-of-things, published in 2017, describes some of what lies ahead: "Systems are already being designed" it stated, "that allow connected ambulances, police cars and fire engines to communicate directly with other vehicles on the road. A device in the emergency vehicle would broadcast that it is approaching before the drivers of other vehicles could see or hear flashing lights and sirens, which could dramatically improve response times."[73]

Virtual reality companies are also modelling the complex and interconnected ways in which cities might react to major emergencies and incidents, facilitating improved emergency service and public authority understanding of such incidents and their level and quality of preparedness.[74] It is important also not to forget the importance of what data-driven tools and approaches can do to assist law enforcement officers who often put themselves in harm's way. Connected devices may help police officers to stay safe while on duty. A pilot project in Dubai is using sensors attached to an officer's uniform to send information to a control room when an officer may be incapacitated or lying horizontally.[75]

70 Oswald et al (2017).

71 For an example of their use, and surrounding controversy see Liptak (2017).

72 Policemediablog.com (2017).

73 Quoted in Tech UK (2017) p. 21. See also Jaguar News (undated).

74 See for example Franklin-Wallis (2017).

75 Gilbert (2015).

4.6 USING POLICE AUTHORITY FAIRLY

Another crucial and highly sensitive issue being addressed via data-driven approaches concerns the issue of police use of authority and force in a fair way. Two innovations are worth reviewing with regard to this.

Body worn cameras

One of the ways in which police forces are trying to address the issue of fair use of police authority is through deployment of Body Worn Cameras (BWCs). However the picture is here is not straightforward. Some studies, such as one in 2015 by the Edmonton Police Service in Alberta, Canada, have shown no measurable impact of BWC deployment on either use of force rates or the numbers of complaints made against the police.[76] Another review of the findings of ten BWC studies showed no impact on use of force levels overall.[77] It also, worryingly, noted increased rates of assaults on officers who were using BWCs. This finding was backed up by a further study that showed a 15 per cent increase in rates of assault on officers when they turned on the BWC in the middle of an encounter, suggesting that the move may be seen by some as an escalation of an ongoing incident.[78]

The idea that the way in which BWCs are used is influential in their overall impact has been picked up by other studies that show more positive effects. One review of a number of cases showed that when BWCs were activated at the start of interactions with citizens, and those citizens were advised of what was happening, use of force declined by 37 per cent.[79] A large number of other studies of BWC use by the police have also shown both reductions in citizen complaints against officers and reductions in the number of incidents of police use of force, suggesting that while the context of BWC deployment is important, the data such technology gathers might well be having a significant and positive impact on police-citizen interactions. One evaluation of BWC use in Rialto, California, showed a near 90 per cent drop in complaints against the police and a 60 per cent drop in use of force by officers.[80] Other studies in Mesa, Arizona, and in both Orlando and Tampa in Florida have shown similar positive results.[81]

In the UK, officers involved in a decade's worth of BWC use in Northamptonshire have also reported significant declines in number of complaints against the police as a result of widespread BWC deployment.[82] And a randomized controlled trial of body worn video use in ten London boroughs between May 2014 and April 2015 showed positive results:

> *"During the Metropolitan Police Service trial period 261 complaints were recorded, comprising 462 allegations. Analysis showed that BWV reduced the number of allegations against officers, particularly of oppressive behaviour. The odds of an officer receiving an allegation of oppressive behaviour were 2.55 higher if the officer was in a non-BW Video team, compared to a BW Video team. Complaints related to how the officer interacted with the public also reduced significantly."*[83]

While the research evidence shows a nuanced picture therefore, there are good reasons to view body worn cameras and body worn video as a public value adding tool, capable of helping steer police-public interactions in the right direction.

Seattle Police Department's use of data analytics

The issue of police use of force and authority has been approached in a different way in Seattle. In 2011, the US Department of Justice (DoJ) Civil Rights Division accused the Seattle Police Department of an excessive use of force over a prolonged period, amounting to a violation of the constitutional rights of citizens.[84] The DoJ said this was due, in part, to what it described as a lack of oversight from senior officers. For much of the time since, the Seattle Police Department (SPD) has

76 Edmonton Police Service (2015).

77 Ariel et al (2016).

78 The Economist (2018d).

79 Ariel et al (2016).

80 Ariel et al (2014).

81 White et al (2017).

82 Spencer and Cheshire (2017).

83 Owens and Finn (2018).

84 Seattle Times (2011).

been under court-ordered monitoring to ensure that it is carrying out the reforms necessary to address the problem. As part of wider reforms, it has introduced a new analytics platform to track all of the force's interactions with the public.[85] This gathers data on all 911 calls; complaints received; use of force incidents (including demographic data with regard to those against whom force has been used); Terry stops (stop and search); as well as crisis events, where a citizen is experiencing a health or mental health crisis that may require a non-punitive response.

The system also includes a records management function, which means it can flag up instances where police responses or actions have not been timely or reports are incomplete. This system has merged six previously used systems together and represents a major advance over the disparate, incomplete and often non-existent records with regard to the use of force that previously existed. It now contains 17 sets of data points that can be brought together in bespoke visualisations to show both police leaders, and the public, up to date information on how the SPD is interacting with the public. This means, for example, that if a senior officer wants to know how many times in the past three months an individual white male officer has used force against, or Terry stopped, a black male, that information can be instantly visualised. Recent historical trend data is also easily available.

The system can also present public interaction data linked to individual police officers, so it is easily visible how many times an individual officer has been involved in a use of force incident over a given time period. While there was some unease among officers on its initial introduction, the system has been reasonably well received since then because it is capable of presenting a highly nuanced picture of the context within which an individual officer is operating. Far from a simple flag being issued by the system if a particular use of force threshold is reached by an officer in a given period, it also presents information on where the officer has been patrolling, what shifts he or she has been working, what their training history is, whether and how often they have been calling in crisis event teams to offer non-punitive help to citizens with mental health problems, and whether there have been any notable changes in the pattern of the officer's interaction with the public in the recent past. It can even generate 'Officer Team' data, so it can spot whether an individual officer's patterns of engagement with the public changes when on patrol with a particular colleague. All of this means it is possible for managers to get a fully nuanced view of what might be happening with regard to an individual officer who has triggered a flag for involvement in a number of 'use of force' incidents. It also means training can be offered and patrol rotas amended to iron out any particular issues.

What is more, all of the data on use of force, Terry stops, and data with regard to the demographics of those being stopped or subjected to force, plus much else besides, is published in a series of SPD dashboards available to the public on the SPD website.

The analytics platform is but one element in a wider package of changes the SPD has undertaken in recent years and direct causality is hard to prove. Nonetheless, this data-driven approach to tracking both more routine, and potentially controversial interactions with the public, has contributed to a situation in which the number of 'use of force' incidents in Seattle in July 2018 was at a four-year low.[86]

4.7 IMPACT ON TRUST/ LEGITIMACY

While it is theoretically plausible to assume that data-driven improvements to things like crime prevention, crime detection, and fairer use of police authority will contribute to increased public trust in, and perceived legitimacy of, the police, the actual relationship between data-driven policing and this dimension of public value is more complex. There are both upsides, but also potentially very serious downsides to the impact of data-driven policing on the police relationship with the public. We return to some of the potential down-sides in the next chapter. Here, we focus on some of the more positive dimensions.

Hampshire Constabulary: investment in people

One key aspect of trust in the police relates to competence in a digital age.

Hampshire Constabulary has identified data-driven policing as a core contributor to its own effort to build a relationship of trust and confidence between the force and the public. This has principally taken the form of training

85 The description offered here of the system and its functionality is based upon telephone interviews with some of the team responsible for introducing it.

86 See Seattle Police Department Use of Force Dashboard, available at: https://www.seattle.gov/police/information-and-data/use-of-force-data/use-of-force-dashboard.

a large number of officers and staff so that they have the knowledge and skills required to operate in a digital and data rich environment. The approach has been deployed both to train specialist capability to deal with serious, less frequent crime, and to enable identification and investigation of the digital footprint of volume crime.

At the more specialist end of the spectrum, 50 senior managers and leaders have taken crypto-currency courses designed for senior investigating officers. These cover the history of crypto currency and involve examination of case studies where crypto-currency has impacted on policing. Officers are trained to understand the potential for unlawful use of cryptocurrencies and in both the capabilities available, and limitations of, investigative methods with regard to cryptocurrencies.

Another 40 members of staff have received intermediate crypto currency investigation training. This covers an understanding of the basic concepts behind blockchain technology, and what is involved in the ability to acquire, store, and transact in bitcoin. It also involves understanding the available tools for examining the bitcoin blockchain, and training in being able to identify viable lines of enquiry from one or more bitcoin transactions, as well as an understanding of best practice for the seizure and handling of bitcoin. Over 2,000 members of the force have also seen a training video which explains what cryptocurrencies are, how they work, and what the legal bases, processes and safest methods are with regard to crypto-currency seizure.

Across the force, officers and staff are also receiving training to operate in the emergent digital environment. Over 700 staff have received digital mindset training, which consists of either half day or one-day sessions that cover digital investigative opportunities with regard to volume crime, basic seizure advice and new ways of facilitating the investigation of old offences using modern technology. A whole new staff category, called Digital Media Adviser (DMA), has been created. Around 40 of these DMAs are deployed in the Public Contact Centre and are trained either to ask questions that might point to the availability of a digital footprint with regard to crime reports, or to offer advice to members of the public who are concerned that they or a member of their family may be a victim of some sort of cyber-related or cyber-facilitated crime. DMAs, for example, receive a two-hour training session on applications that can be installed on devices in order that parents can monitor the activities of their children quite lawfully. This is in response to the contact centre receiving a large number of enquiries from concerned parents about which is the best application to install or purchase on their child's device for monitoring purposes. The course also covers the legality and practical aspects of giving such advice.

Last year, the force also held a Digital Discovery Week that saw 1700 delegates take part in over 75 different training sessions over the course of the week. A series of follow-on Digital Discovery Workshops are now being planned to accommodate up to 500 people, and to focus in on particular areas in more detail. One workshop, for example, will educate officers with regard to vehicle and transport system data that is available and that may be useful in investigations.

Hampshire Constabulary became the first UK law enforcement Cisco Academy on 1st November 2017. This enables Hampshire to deliver free of charge to its staff industry recognised and accredited IT training courses and qualifications.

The entire thrust of this effort is designed to communicate, and demonstrate, to the public that Hampshire Constabulary understands the digital and data rich environment it is operating in and can both handle that environment effectively itself, and help the public to do so too. It is grounded in a belief that digital is not only a specialist area but now a core one in almost all crime types, and that if the police do not look and sound like they understand that, an increasingly tech savvy public will quickly lose trust and confidence in the police's ability to perform their crime prevention and crime fighting function in the digital age. It is of course too early to say whether this investment in staff capability has impacted on perceived trust levels in the force, but this will be worth monitoring in the years ahead.

Blockchain and trust in the criminal justice system

Another area where data-driven approaches may affect trust is the use of blockchain technologies in the wider criminal justice system. There is intense focus on the potential for blockchain technologies to increase transparency, accountability, and therefore trust with regard to the storage, safeguarding and sharing of evidence and intelligence related to ongoing investigations and criminal cases. In Australia, AUSTRAC, the financial intelligence agency and the Australian Criminal Intelligence Commission have recently awarded a $1 million contract to Singapore based consultancy HoustonKemp to build a blockchain based system to record intelligence and data collected by the police.[87] China's Ministry of Public Security,

87 Reuters (2017).

which is formally in charge of all Chinese police forces, has built its own blockchain application to securely place evidence from investigations into cloud storage.[88] Patented in November 2017, the system timestamps and stores data submitted to the cloud after receiving multiple signature confirmation from both police and cloud service provider, in an attempt to make deposition procedures more transparent and tamper proof.[89] Once entered into the blockchain, the system is intended to provide an immutable copy of the data and information on who entered it and the time and date the entry occurred.

A blog post by Al Davidson, Technical Architect at the Ministry of Justice in London, in November 2017 acknowledged and commented on the potential of this kind of development, especially in relation to trust.[90] "There is", he said, "no need for everyone to just trust a single authority. Trust is distributed and decentralised among the users."

In India, another blockchain project called 'Police 2020' is developing the technology for similar security reasons but is extending it to achieve more transparent and efficient access to data for a variety of stakeholders.[91] The problem of effective data-sharing between organisations is a significant and recognised in all jurisdictions. Often officers and officials are unsure of what information about a case can and should be shared with whom, and they end up withholding it out of fear they will make a mistake. The combination of blockchain technology with smart contracts that lock in varying levels of permissions can address this and effectively automate the decision. This automation of trust could bring enormous advantages. In the Indian case, it is envisaged that victims and complainants will be able to receive controlled access to the system and automatic updates every time there is a development in their case. Through different permission levels and access protocols, information will be more easily shared between institutions, agencies and individuals related to a case, and between the police and prosecutors and defence lawyers, while keeping the information secure and tamper free for everyone. It is possible that such a system might have helped in recent controversial, and damaging, cases related to evidence disclosure here in the UK.

4.8 THE DELIVERY OF A QUALITY SERVICE TO CITIZENS

Evidence is also beginning to mount that data-driven approaches can help to provide a better service for citizens engaging with the police.

Metropolitan Police Contact Centre

One example of this comes from the Metropolitan Police Contact Centre (Met CC). The Met CC has introduced a powerful combination of an interactive voice response (IVR) system, new functionality to the force website, (such as the ability to report crimes and antisocial behaviour online), and the automation of some back-office processes to drive a better experience for the public when contacting the Met. The IVR system, which has only been in operation for a number of months, interacts with people calling the Met and routes calls to the most relevant place. It has reduced call waiting times relative to the period prior to the introduction of the system and improved the speed at which callers are directed on. Callers have the option to press 9 to speak personally to a call handler at any point in the interaction. They also can choose to switch to the new online platform and continue their contact with the force via the website if they wish. When they do so, their information is captured via online forms and automatically turned into draft crime or incident reports for officers to review. From the citizen's point of view, this speeds up the process by which crime numbers are allocated which not only reassures them that the police are aware of their crime and able to respond to it but provides the basis upon which certain activities such as making insurance claims can be commenced more quickly. Take up of online services more generally has been good, including of online chat, and the early evidence indicates that services such as this are achieving high satisfaction ratings from the public using them.[92]

Single Online Home

There is emerging evidence that the public is beginning to warm to the idea of interacting with the police via online platforms. In the first six weeks of operation of the Single

88 Bitcoin News (2018).

89 Coindesk (2018).

90 Davidson (2017).

91 New Indian Express (2018).

92 Interviews with senior staff at the Metropolitan Police Contact Centre.

Online Home, one of the highest profile projects in the Digital Public Contact strand of work of the Digital Policing Portfolio, 4,365 crime reports and 2,259 road traffic reports were received online across the two forces initially using the service (Hampshire Constabulary and Thames Valley Police). This amounted to just under nine per cent of all crime reports for the period. A survey was conducted to understand how users of the online service might have contacted the police were the online service not available. Of the 4,109 responses received, 1522 stated they would have rung 101, a further 1,764 had actually started by ringing 101 but had then opted for the online service, 388 would have entered a police station, and 214 wouldn't have contacted the police in any other way. This shows that a considerable portion of the public prefers the ease of the online service to phone and in-person contact when the option is available. It also indicates that the online platform is actually bringing in additional crime reporting that otherwise would not have taken place.[93]

4.9 EFFICIENT AND FAIR USE OF PUBLIC FUNDS

When it comes to data-driven approaches and efficiency gains, two factors are holding many forces back from publishing hard data. These relate to legacy IT systems on the one hand and the poor quality of baseline data available on the other. The two problems are related in that the laborious nature of manually inputting and extracting data from databases that couldn't talk to each other often meant data was not collated and therefore, from a management point of view, not really available. This has left forces cautious about the claims they make with regard to the concrete benefits of new systems and processes. Over time, however, and as data collection, extraction and analysis becomes easier, this problem will diminish. And in the meantime, some evidence of efficiency gains is beginning to emerge.

These come in the form of cost savings; time savings on laborious bureaucratic tasks which then free up police officers to engage in more value-added activity; and the more effective targeting of activity to achieve greater effect with less police resource. Some of the innovations profiled in this chapter, along with others taking place elsewhere, are already generating these kinds of benefits or are suggestive that they will occur. For example:

- One estimate suggests that ongoing police efforts to share data in digital format online with the wider criminal justice system, rather than via DVD, could save as much as £22 million per year nationally.[94]
- The innovations just profiled in the Met CC are saving officer time with regard to the routing of calls and the completion of crime and incident report forms. A joint report by the Mayor's Office for Policing and Crime (MOPAC) and the Metropolitan Police in London noted that the new MPS website, in use since March 2017 for non-emergencies and crime reporting, 'has reduced the need to call back members of the public for more details or send officers purely to find out additional information. This allows the MPS to deploy officers where they can provide the greatest value to the public and provide a better service to Londoners.'[95]
- The police forces using AI tools to combat child sex-trafficking in partnership with Thorn are reporting time savings of as much as 65 per cent on investigations.[96]
- The integration of different datasets in the West Midlands Police and Avon and Somerset Police is saving much of the time that officers would previously have spent on manual data extraction from multiple systems, while also generating new insights that enable the better targeting of scare resource.
- Predictive policing tools are also helping to reduce crime through better targeting of patrols.

The potential for more efficiency gains in future is very clear too. The combination of blockchain technology with smart contracts that lock in varying levels of permissions, is one example. In 2010, Her Majesty's Inspectorate of Constabulary (HMIC) found that during the prosecution of a standard domestic burglary there were 70 'rubbing points' where the progress of a case was dependent upon one justice agency securing information from another. In addition, as part of this process there were at least seven occasions where data

93 Data provided to the authors by the NPCC Digital Policing Portfolio.

94 This statistic is drawn from an interview with a member of staff in the NPCC Digital Policing Portfolio.

95 MOPAC, MPS (2017).

96 Thorn (2017).

needed to be transferred between agencies. This level of complexity presents multiple moments for mistakes to be made and for duplication to occur. Blockchain technology could enable automatic updates and design in rules to prevent error.[97] The same process could also save huge amounts of officer time.

More widely, the the internet-of-things has further potential to contribute a vast flow of information to police control rooms that can then be used, in conjunction with other data, to help spot patterns of activity and potential crime, and to help improve the prioritisation and allocation of scarce police resources with benefits across both police efficiency and outcomes.

97 Muir (2017).

5. CHALLENGES

Despite the benefits of data-driven technologies to policing, there remain significant barriers and challenges remain to their future adoption. There are wide-ranging concerns in a number of areas such as the way some police forces have, on occasion, misused data; the implications for personal privacy; the building of predictive models on the basis of inevitably biased and inaccurate data; and questions over the ethics of, and public anxiety about, algorithm use in decisions that can have profound implications for both procedural fairness and individual human lives. There are also questions about whether the police workforce is ready, able and being supported well enough to take on the challenge.

5.1 POLICE MISUSE OF DATA

While Chicago Police Department has seen some good results from the use of data-driven predictive models it has also been subject to criticism over how its Strategic Suspects List (SSL) or 'Heat List' of individuals most likely to be involved in homicides or shootings has been used. Police officials have been quick to celebrate the predictive accuracy of the Heat List, noting that on Memorial Day weekend in 2016, 78 per cent of the 64 people shot had been on the list and on Mother's Day of the same year, 80 per cent of the 51 people shot had been on the list. A study by RAND however, found that:

> *"at risk individuals were not more or less likely to become victims of a homicide or shooting as a result of being on the Strategic Suspect List (SSL)….. We do find, however, that SSL subjects were more likely to be arrested for a shooting."*[98]

The implication here is that the police had not made efforts to intervene with individuals on the list, for example in coordination with social services, and used the predictive policing approach not to prevent crime and reduce harm to Heat List individuals themselves but to produce a 'data-driven most wanted list' that could facilitate arrests after the event.[99]

Practices of this kind can feed a sense that new information systems are being used to justify over-policing of certain individuals, neighbourhoods, and communities while others are left alone, a development that could ultimately undermine trust between the police and communities rather than enhance it.

There have also been other instances where the police have failed in their duty of care with regard to keeping personal information secure and instances where individual police officers have used access to improved data sources to commit crimes themselves. The Economist reported on such incidents in its recent review of police use of information and communications technologies:

> *"In 2015," it noted, "a journalist in Boston found the city's entire number-plate recognition system online, including the addresses of everyone with a city parking permit, and the names of thousands of people suspected of being terrorists or gang members. Such data can be abused personally as well as constitutionally. A policeman in Washington DC, was convicted of extortion for blackmailing the owners of cars parked near a gay bar."*[100]

The International Association of Chiefs of Police has also recognised the potential dangers of police misuse of data. With regard to Automatic Number Plate Recognition Systems (ANPRS) for example, it has noted that their use could impact on freedom by "recording vehicles going to political gatherings, abortion clinics or other sensitive issues."[101]

What all this demonstrates is that data can be used to deliver public value but if it is mishandled or misused it can destroy public value and create enormous problems for the police, the citizen and the criminal justice system at large.

5.2 PRIVACY

As more and more datasets are joined up, concerns about surveillance and violations of privacy come to the fore. Developments like the aforementioned Domain Awareness System in New York City and the use of AI tools to combat people trafficking have already generated privacy concerns. In the UK, in a submission to the parliamentary Home Affairs Committee inquiry into Policing for the Future, the campaign and advocacy

98 Quoted in Ferguson (2017).

99 Ferguson (2017)

100 The Economist 2018b, p.6.

101 The Economist 2018b, p.6.

group Big Brother Watch criticised the proposed National Law Enforcement Data Service (NLEDS). NLEDS is a plan to create an integrated database of all police held information and to store it on a cloud service provided by Amazon Web Services, from where it would be accessible remotely from hand held devices and in car-based computers being used by the police on patrol. It would also, Big Brother Watch argued, be available to unspecified other government departments and agencies who could:

> *"… check an individual's identity, offending history, status, and location, to analyse data to identify links between people, objects, locations and events, and to set up automated alerts for new or changed data and events of interest. This would appear to allow government departments unprecedented access to sensitive information about individuals who have come into contact with the police and the criminal justice system."*

Big Brother Watch's complaint is not only about substance but process. Its submission goes on:

> *"There has been no consideration of this new system by Parliament. Whilst modernised policing systems are welcome, there needs to be significant and meaningful consideration of the privacy issues involved in such a large database of personal information, the access to such a database via an application available to all police officers, and the use of machine learning algorithms in the criminal justice system."*

Similar concerns have been raised about other technology systems that the police are using to help them deliver data-driven public value, such as automated facial recognition systems used in public places, and automated number plate recognition systems. The latter have dramatically increased in numbers in recent years, resulting in some 25 to 40m number plates being scanned every day in the UK with the data being stored for 12 months. The Surveillance Camera Commissioner has previously described this as one of the "largest non-military databases in the UK", holding up to 20 billion records. Not only do some see this as one of the largest citizen tracking systems in the entire world but in his 2015 Annual Report the Surveillance Commissioner noted that:

> *"There is no statutory authority for the creation of the national ANPR database, its creation was never agreed by parliament."*

Further privacy concerns relate to the way in which the police are, in some instances, conducting investigations. Victims of sexual offences, for example, are often being asked to provide access to the entire contents of their mobile phones, laptops, tablets, social media accounts and passwords related to any personal data stored on a cloud service. From the policing point of view, this is an attempt to access data that may be vital to getting to the truth in a case but it is highly controversial and makes some victims feel like they are the ones being investigated and put on trial. It can fundamentally alter the relationship between the citizen, the police and the criminal justice system.

There are even tools available that can automate this process without requiring the citizen's consent. Technology built by the Israeli company, Cellebrite, used by more than 10,000 law enforcement agencies in 150 countries, allows users to 'bypass the locked phone's passcode and continue to use one of several extraction methods. Logical extraction reveals immediately accessible data: stored text messages, email, pictures and instant messages. With more time, Cellebrite's machines can also perform a physical extraction, revealing more information, including data that may have been deleted. The neatly organised, labelled data can then be viewed, saved, shared, filtered and searched.'[102]

Technology already available today can in fact be used to almost eliminate privacy completely and to engage in highly effective attempts at social control. In China the authorities have covered the regions of Xinjiang and Tibet with facial recognition cameras and iris scanners for precisely this purpose. In January 2018 the European Parliament-imposed export controls on surveillance technology in response to just this concern.[103]

Few would suggest that the UK is in danger of the same level of surveillance and social control today but privacy concerns are real. Complacency would be both unwise and ultimately could allow 'technology creep' to the extent that public perceptions of the legitimacy of police action were undermined.

102 Quoted from The Economist 2018b, p.6.

103 The Economist (2018b).

5.3 DATA BIAS

Another very significant challenge concerns the problem of bias in the data upon which predictive policing models are built. That the data is biased is beyond doubt for the simple reason that crime, and data collected about crime, are not one and the same thing. Crime is a largely hidden activity that occurs whenever a person violates the law but not all crime comes to light. Crime data on the other hand is data that has been reported or that has been collected by police forces and others. It also includes data that isn't specifically about law-breaking incidents as such but information like arrests of people suspected of crime but subsequently released, and reports of incidents witnessed while out somewhere on patrol. Police data isn't collected objectively or uniformly but reflects institutional and individual interpretations of policing priorities and biases, some of which can reflect social biases about race, social status and gender.

Algorithms in predictive policing models are essentially statistical processes applied to datasets to find patterns in the data. As they are built, they learn to predict future patterns of crime on the basis of an initial 'training data' set. If that dataset is biased, as it always is, the algorithms effectively embed the bias and search for repetitions of it rather than challenge it. While the hope is that systems improve as they come into contact with more and more data, the consequences can be profound.

A study by Kristian Lum and William Isaac of the Human Rights Data Analysis Group in the United States showed that the supposedly race neutral algorithm of Predpol, a leading provider of predictive policing tools, suggested the targeting of black neighbourhoods twice as much as white ones after it was trained on historical drug crime data in Oakland, California. It found similar biases when it analysed the data in relation to income distribution, with poorer neighbourhoods being targeted much more than wealthier ones. The problem with this outcome is that wider estimates based on population models and public health surveys suggested illicit drug use was more or less equal across income and racial groups in Oakland.[104] Biases in the data wrongly led to the over-policing of some communities and neighbourhoods and the under-policing of others.

Over time, this would lead to a lot more data being gathered about individuals and incidents in the targeted neighbourhoods than elsewhere, and biases in the data would be reinforced based on what was essentially biased police practice.

From a political and policy point of view, bias in historical data fundamentally changes the context in which algorithms are being used. It is not difficult to see that if bias is inherent in the data being used by, for example, the Durham Harm Assessment Risk Tool (HART), the issue is not just one of suspicion of new technologies and approaches but one of its impact on the very principle of procedural fairness in the justice system. As an investigation into this area by The Economist noted in 2018: "A proprietary algorithm that recommends a judge punish two people differently based on what they *might* do offends a traditional sense of justice, which demands that punishment fits the crime not the potential crime."[105]

As it happens, the team involved in the HART system deployment and evaluation in Durham were themselves acutely aware of these dangers and have, in published research, pointed to some areas of the justice system where it would be inappropriate to use this kind of tool. Their work nonetheless became the focus of some considerable controversy. As AI systems are used to help automate the process by which the police can trawl through the growing and vast amounts of digital evidence related to cases, this controversy will only grow.[106]

5.4 PUBLIC ANXIETY

Public support for data-driven approaches to policing cannot be taken for granted either. While some of the activities outlined earlier in this report, such as better use of data to save police time or to more effectively monitor incidents of stop and search or the use of police force are unlikely to stimulate much controversy, others are clearly of far more public concern. Research by the Royal Society of Arts (RSA) in 2018 found almost zero support for machines taking on any kind of decision-making role. Only two per cent of the public thought machines should be taking decisions in the justice system, and 60 per cent were opposed.[107] Additional public opinion research carried out for the

104 See a discussion of some of the findings of this analysis in Isaac and Dixon (2017).

105 The Economist (2018b) p.10.

106 The Guardian (2018).

107 Balaram et al (2018).

Centre for Justice Innovation drilled a little deeper, to find that 44 per cent might be comfortable with the use of artificial intelligence to support *human decision-making* in the justice system, but with an almost identical number opposed to its use at all.[108] These numbers perhaps partly reflect lack of familiarity with what AI systems can and already do today but they also indicate that among members of the public there are certain deeply held beliefs about the role that human as opposed to machine judgement should play in the making of important decisions in the criminal justice system. A police force moving too quickly into this terrain without taking the public with it is embarking on a high-risk strategy.

5.5 PRACTICAL DELIVERY CHALLENGES

Another major set of barriers to be overcome with regard to advancing the data-driven policing agenda are the practical delivery challenges. Both police leaders and Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) have warned that the police are struggling to cope with the sheer volume of digital data and evidence now available. In an evidence session to the House of Commons Home Affairs Committee Inquiry into Policing for the Future in June 2018, Cressida Dick, the Commissioner of the Metropolitan Police, said her biggest worry was 'the exponential rises in digital data and the impact that that is having.'[109] Sara Thornton, the Chair of the National Police Chiefs' Council separately has called for the use of artificial intelligence systems to help the police sift through and make use of the vast quantity of digital evidence now available in police investigations.[110] This message built on an earlier one from Mike Cunningham, who led a review into the police's ability to manage demands and resources for the HMIC(FRS) in late 2016. He found that many forces had a significant gap in digital skills which were sometimes leading to unacceptable delays in tasks like getting data off mobile phones. He also expressed the concern that "the urgency of the issue is not matched by the urgency with which the service is responding" and the clear view that while forces might be able to access the right capability somewhere in the force eventually, the service was effectively being overwhelmed by the scale of the digital evidence available.[111]

The recent CoPaCC survey of Police ICT User Perspectives 2018, also highlights major causes for concern. The survey, which secured a usable sample of responses from 3,364 serving police officer and staff respondents, made up of 2,303 police officers from the federated ranks, 995 staff, and 66 senior officers, asked a series of questions about experience of police ICT use. The questions covered, among other things, overall levels of user satisfaction; views on the level and appropriateness of investments being made into ICT; trust in the information being held in police ICT systems; and perceptions of how well those systems are integrated with each other. They also asked users what they thought about the level of training and support on offer when new systems and technologies were introduced.

The survey findings were stark. Respondents were not happy with the overall state of ICT provision with only two per cent declaring themselves fully satisfied. Over half (55 per cent) were either quite, very, or completely dissatisfied. Some 57 per cent also disagreed with the statement that their force has invested wisely in ICT. A half either didn't feel they could trust information on police ICT systems or neither agreed nor disagreed with the proposition that they could. And 72 per cent felt police ICT systems were not well integrated with each other with only one per cent being completely satisfied on this measure. This represented a slight worsening compared to the findings of the smaller, inaugural CoPaCC survey that asked the same question in 2017. Nearly two thirds of respondents (63 per cent) were also unhappy with the quality and timing of ICT training on offer.

The survey question responses were complimented by some 18,515 individual comments offered by respondents, which added colour to the story presented in the percentage figures just outlined. Common themes identified in those comments included complaints about inappropriate technology being deployed, training being sometimes non-existent, and the need to constantly re-enter the same information into a number of systems that ought to be able to talk to one another but evidently couldn't. While there were some signs of progress compared to the findings of the 2017 survey, particularly on issues like better deployment of mobile devices to officers on the front line, and ability to access a computer when

108 Bowen and Gibbs (2018).

109 House of Commons Home Affairs Committee (2018) p. 4.

110 See Gayle (2018).

111 BBC News (2016).

one was needed, the overall survey findings indicate a police service failing to rise to the challenge set out in the 2025 NPCC and APCC policing vision. It is also interesting to note that the most dissatisfied group of users by far was the federated ranks. Views among senior officers and staff were slightly, and in some cases significantly, more positive.[112]

Behind these survey numbers and comments sit practical, structural, and legacy problems that have been long known about but are still unaddressed. Some relate to the poor quality and inaccurate or duplicated nature of much data held in police databases. Some to the fact that different police forces store different kinds of data using different codes on the same issue, in the context of a lack of agreed data sharing standards. Different forces also take different attitudes to which officers are allowed access to which systems and under which circumstances. And many legacy technology systems still in use are effectively closed and cannot be integrated with others, either within a force, between forces or between the police and/or other public agencies.

These practicalities reflect the structural reality that UK policing is fragmented. As a recent RUSI report noted:

> *"Forces pursue technological change independently in response to local requirements, with little inter-force coordination. Although there are regional structures and partnerships in place, the wide variation in the level of technological development makes it difficult for forces to collaborate when designing new technology."*[113]

Structural fragmentation is also visible in the approach to innovation. Where innovation is taking place, as seen in many of the UK case studies profiled in the previous chapter, the effort is too small scale, too scattered, and there is not enough evaluation and sharing of learning. No clear structural home exists for the latter either. And too often officers working on digital projects are also working in isolation.

And then there is the constrained fiscal condition within which policing in the UK is being forced to try to meet the challenge. In its own submission to the House of Commons Home Affairs Committee inquiry in Policing for the Future, the Digital Policing Board said this:

> *"The barriers to effective digital transformation include the state of existing technology, the capacity to invest during austerity, development of a compelling case for priority against other investment requirements and effective digital leadership."*[114]

While on the one hand, therefore, it is clear that data-driven approaches to policing have huge potential to deliver public value and to impact on the policing bottom line, on the other hand, it is equally clear that the remaining practical, human resource, organisational, structural, public opinion, and ethical challenges that must be addressed before it can fully advance are formidable, to say the least.

5.6 POLICY AND REGULATORY GAPS

We are also already at the point where some policing practices are leaving legal and regulatory frameworks behind. While privacy laws are clear about the need for governments to obtain prior legal authorisation to enter a private citizen's home or to examine private papers, for example, tools such as the Cellebrite technology described earlier are used in something much more akin to a legal grey area or even vacuum.[115] Another area of controversy surrounds retention of, and public access to, body worn camera footage.

Meanwhile, police forces experimenting with data-driven approaches, and with the use of algorithmic decision-support systems in particular, are doing so in the absence of any guidance or codes of practice on how it should be approached or what kind of safeguards should be put in place before experiments take place. This is despite the fact that there are clear concerns about how such systems could influence decision-makers, impact on individual lives, and potentially conflict with data protection, human rights and equalities legislation.

Whatever the intention is in using such systems, and whatever caveats are put in place with regard to machine learning algorithms operating on probability and correlation rather than certainty and causation, little is known about how algorithmic decision support tools

112 CoPaCC (2018).

113 Babuta (2017) p.39.

114 Digital Policing Portfolio (2018) p.9.

115 The Economist (2018b).

affect police decision making in practice. There is a clear risk that police officers using such systems might come to rely uncritically on their outputs when making important decisions. This risk might be most serious in cases where automated systems are thought to have high predictive accuracy, leaving officers without the confidence to use their own judgement to challenge or contradict a course of action an algorithm is suggesting. This would essentially contradict the legal requirement on decision-makers to take all relevant factors and information into account when making decisions and it might directly contradict the Data Protection Act 2018, which provides safeguards to protect individuals from decisions based solely on automated systems. Where decision-support systems are only being used in an advisory capacity, there is the alternative danger that officers will only take their outputs on board when they chime with whatever personal biases or assumptions they themselves hold.

The lack of transparency and understanding of how many algorithmic decision support tools actually work is also a big problem.[116] Many algorithmic tools in use today are described as 'black boxes' sucking data in and producing predicted outcomes without being able to show how those predictions have been arrived at. Making the source code accessible to other experts can help to some extent, and there may be many cases in future where access to the software code in use will in fact be needed for evidential purposes. But many private sector providers of such tools are reluctant to open up access to their software code for commercial reasons. And even where access to the code is allowed, this does nothing to explain to the lay person, or to the person whose life is being subjected to an algorithmically arrived at decision, how any particular prediction in an individual case has been arrived at. It is this lack of auditability that led the House of Lords Select Committee on Artificial Intelligence to conclude that:

> *"it is not acceptable to deploy any artificial intelligence system which could have a substantial impact on an individual's life, unless it can generate a full and satisfactory explanation for the decision it will take."*[117]

Some tools being used can provide this, such as that in the Durham HART tool outlined earlier. In that case, the random forest forecasting embedded in the algorithm can be unpacked to show how a particular prediction was arrived at. Many other tools however, cannot meet this test. A lot of work is going into cracking this problem, and some private sector providers are now claiming they can provide algorithmic auditing as a service. The Information Commissioner's Office also recently expressed the hope that data analytics methods such as Natural Language Generation (NLG) might be able to create plain English explanations of how an algorithm arrived at a prediction with regard to an individual, and this may soon become possible. But we are not there yet, and current decision support systems in use by the police have no such function. Far from being a technical matter, this strikes at the heart of an individual's ability to question any algorithmic prediction that may have been influential in a decision affecting them and as such it is potentially undermining of the fundamental principle of procedural fairness upon which the legitimacy of the justice system depends.

It is also worth noting that the problems with bias and privacy outlined earlier may create other legal problems for any police force using algorithmic decision support tools. If such tools are indeed biased or the police are too intrusive in their quest for relevant data, the entire data-driven approach in use may contravene the European Convention on Human Rights (ECHR), which includes the right to freedom from discrimination and the right to respect for private life. Problems with regard to compliance with the Data Protection Act 2018 may also go well beyond the issue of whether an individual has been subjected to a fully automated decision or not. The Act requires that data concerning an individual must be processed in a way that is lawful and fair, and that the data must not be kept any longer than is necessary. Any tool that has been influential in decision-making and that operates on the basis of probabilities rather than certainties, or that may draw upon long held data, would appear to be legally questionable in terms of its compliance with such criteria.[118] Where a dataset being operated on by an algorithm is itself demonstrated to be systematically biased with regard to

116 For a more in depth discussion of the issues raised in this section, see Babuta et al (2018).

117 House of Lords (2017). p.128.

118 Note the Information Commissioner's findings in relation to the MPS' operation of the London Gangs Matrix: Information Commissioner's Office (2018).

a certain category of individuals, on the basis of race or gender for example, legal cases could also be brought under the Equalities Act 2010.

It is of course the case that decisions made without such algorithmic tools can be and often are challenged with regard to compliance with such legal demands and rights, and new algorithmic tools could help to overcome human biases that might already be leading to unfair decisions in the justice system. But that possibility does not in itself remove the legal barriers and pitfalls that might befall law enforcement bodies adopting widespread use of algorithmic tools.

Data-driven approaches could also lead to direct changes in police behaviour in operational environments. Some systems put risk scores on specific addresses. The Economist recently reported on one such system:

"Beware assigns threat scores in real time to addresses as police respond to calls. It uses commercial and publicly available data, and it has a feature called Beware Nearby, which generates information about potential threats to police near a specific address, meaning officers can assess the risk when a neighbour calls the emergency services. This raises privacy concerns but it could cause other problems, too. For instance a veteran who has visited a doctor and taken medicine prescribed for PTSD, who also receives gun catalogues in the post, could be deemed high risk. Police might then approach his house with guns drawn, and it is not hard to imagine that kind of encounter ending badly. Such threat scores also risk infection with bad data. If they use social media postings, they also raise free expression concerns. Will police treat people differently because of their political opinions?"[119]

119 The Economist 2018b, p.11.

6. RECOMMENDATIONS

As the previous chapter makes clear, the challenges are political and ethical and not just technical. To move things forward, we need significant reform at all levels.

One of the notable features of the current debate on data-driven policing in the UK is the absence of any formal mechanisms for including the public voice in it. This is a critical gap which, if not filled, could undermine public confidence in the entire enterprise.

As noted earlier in the report, think tanks have made efforts to engage the public, primarily through opinion poll research, and the findings indicate public concern especially around algorithmically driven decision-making in the criminal justice system. But between opinion polls and formal mechanisms of police accountability to elected officials, whether they be Cabinet Ministers, other parliamentarians, Police and Crime Commissioners, or city Mayors, there is a huge opportunity to engage the public more creatively.

Recommendation 1: We now need at least one, and preferably more, deliberative democracy initiatives that give a group of citizens the chance to learn about, and explore the complexities of, data-driven policing in-depth before passing more considered judgement on what is and is not acceptable police practice in the age of big data.

Such deliberative democracy exercises typically involve recruitment of a group of citizens to play the role of a 'mini-public' and then asking them at the outset what they think of a particular issue or set of issues that are under review. This is then followed by a period in which they are briefed in-depth on the issues and allowed to ask questions and engage in discussion before then being asked to give their more considered opinions once again.

For citizens, such exercises offer a chance to get beyond the hype and examine the real issues in depth. For policy-makers and police leaders, they could provide essential insights into the mood of the public, what the public feels comfortable with, what trade-offs the public considers acceptable, and what steps might mitigate major public concerns with regard to more extensive use of a data-driven approach.

Deliberative public engagement like this could be funded by central government, Police and Crime Commissioners and industry sources, since all have a vested interest in ensuring public confidence in data-driven policing. The sessions could be designed and run by independent think tanks or other bodies capable of providing a neutral setting.

Participants should include not only citizens but elected officials, and the exercises themselves could take on a number of different forms. From the G1000 Citizens' Panel and the Citizens' Cabinet used to address a number of public policy challenges in Belgium, to the Citizens' Assembly on Electoral Reform in British Columbia and the Grandview Woodlands Citizens' Assembly on city planning in Vancouver, there are many deliberative democracy experiments from elsewhere in the world that can be learned from.[120]

Whatever model is ultimately adopted, the important point is that such mechanisms now be used to give the public a structured chance to have a say on the further deployment of the data-driven policing that will increasingly affect their lives.

Recommendation 2: Privacy and ethics commissions should be introduced into the governance structures of every police force in the country to address growing privacy concerns about the use of surveillance technologies that are increasingly the source of much police data.

These should be made up of experts from policing, computer science, law and ethics but they should also include Police and Crime Commissioners and representatives of the general public. Our suggestion is that they mirror the existing governance structures of policing, to allow for the fact that different regions of the country

120 For a description and some analysis of the initiatives mentioned here, see Chwalisz (2015).

may wish to make different trade-offs. These commissions should work alongside police forces and should:

- Evaluate the rationale for the introduction of new surveillance systems and other data capture, integration and analysis systems under consideration, before they are introduced.
- Develop rules together on how the technology and new systems are to be used, again **before** they are introduced.
- Receive annual reports on the way systems and citizen data are being used.
- Consider any rules or restrictions on the future commercial use of citizen data collected by private technology providers.

Some forces in the UK have had the wisdom to form expert advisory boards on the ethical dimensions of the new data-driven approaches being introduced but these are informal. The Independent Digital Ethics Panel for Policing is also in existence and is playing a useful role.[121] But there needs to be a major expansion of effort in this area if public confidence and the legitimacy of policing is to be preserved in a data-driven digital society.

Some experiences from the US could be informative here. Not only do cities like Seattle and Oakland have chief privacy officers who are responsible for vetting and managing the privacy implications of new policies and technologies introduced by their city governments but some of them already have privacy commissions. Oakland's is a nine-member advisory body to the city council, established in 2016, after citizens resisted its plan to introduce a 'domain awareness system' similar to the one Microsoft and the New York Police Department have collaboratively deployed in New York City.[122] The Oakland Police and the privacy commission meet once a month. They review surveillance systems in use and how citizens' data is being used. They also produce technology use policies together. The police department submits public annual reports on how often and for what purpose its surveillance systems are used and the approach has been reportedly 'non-confrontational'.[123]

It will be far better for police forces and Police and Crime Commissioners in the UK to proactively engage with and manage these privacy and data use issues in this kind of way than to attempt the stealthy introduction of systems and deal with any controversy and political heat only as it flares up. Private sector providers should also perceive an interest in this proactive approach being introduced since there are already cases on record of contracts with technology providers being ended due to elevated public concern over the civil rights and privacy implications of systems already in use.[124]

Recommendation 3: Introduce new regulations to govern the use of algorithmic decision support tools in policing and the criminal justice system.[125]

We already know, as pointed out in the last chapter, that the public has concerns about this. To manage it, there is a need to:

- Insist that software code used in such systems is transparent and available to independent checks and analysis. Crucial decisions in the criminal justice system that affect lives cannot be left to unseen and unchallengeable 'black box' processes.
- Ban the use of decision-support systems in the criminal justice system that cannot be deconstructed to show how predictions of possible future behaviour have been arrived at in individual cases.
- Enforce the requirement that explanations of such algorithm influenced decisions are made in simple language so defendants and others can understand and challenge them.

Clear regulations around these issues would help to ensure that citizens and their legal teams can understand and challenge new processes and tools and therefore hold the police accountable for their use.

121 See https://idepp.org

122 The Economist (2018b).

123 The Economist (2018b).

124 The Economist has noted that some cities in California reportedly re-thought contracts with Vigilant, for example, over concerns that the latter's contract with Immigration and Customs Enforcement (ICE) would allow ICE to use ANPR data on Vigilant systems in California to help target undocumented immigrants. New Orleans also reportedly ended its relationship with Palantir because although the latter donated its predictive policing product to the city, 'civil-rights activists feared the firm was using New Orleans as a testing ground for its surveillance products'. The Economist (2018b), p12.

125 Recommendations 3-5 in this chapter draw on some of the thinking already expressed in Babuta et al (2018) and House of Lords (2018).

Recommendation 4: Develop, via the College of Policing, further Authorised Professional Practice on how the police integrate algorithmic decision support tools into policing practice. In particular this practice should cover:

- How forces present algorithmically generated predictions of future behaviour to the individuals who are the subject of those predictions.
- How forces should manage possible tensions between machine generated judgements and professional ones, and how the management of such tensions is explained to those the subsequent decisions effect. Especially where predictive tools point to suspicion with regard to a particular individual this should not in and of itself be sufficient to launch an investigation into that person. Predictive models targeting individuals still risk a high rate of false positive identifications and the consequences for personal privacy and liberty could be profound if excess confidence is placed in such tools. Additional screening processes and professional crime analyst judgements must also exist to prevent investigations of individuals being automatically triggered by algorithms.

Recommendation 5: To ensure that the changes suggested in Recommendations 3 and 4 above are implemented in practice, police inspection regimes should be amended so as to regularly monitor and report on force compliance. This is something that Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services could cover under the legitimacy strand of the PEEL inspection framework.

Recommendation 6: All police forces should review policies and procedures with regard to data stewardship.

The introduction of the General Data Protection Regulation (GDPR) has introduced additional compliance regulations but from a public value point of view, all forces should ensure they have effective policies and procedures in place internally, not only to control access to data, but to be able to track who has accessed what data, when, and for what purpose. This requires security protocols, networking tracking and data audit systems which may cost both money and time to put in place but are essential to ensuring public confidence in the police's ability to be effective stewards of what is often sensitive private data.

The risks here, as noted earlier in the report, are not only from maliciously motivated external attacks to acquire data for personal, financial or political advantage, but also from police misuse of data or failure to operate professionally with regard to data security. As we move towards a big data society, the issue of data security becomes ever more central. It is a concern for all industries and sectors from healthcare to government services, providers of consumer products as well as the IT and computer services industry. Policing is no exception. One additional aspect of this that should be explored is the potential for blockchain technologies and automated smart contracts to be used to ensure fully secure and fully traceable access to data held by the police.

Recommendation 7: Central government should provide additional funding for police officer training in a number of areas related to the data-driven policing agenda.

This funding should be directed to:

- A major expansion of the number of trained digital media investigators to rapidly expand the capacity of UK policing to operate in digital environments and crime scenes.
- A major expansion in the number of data analysts employed by the police.
- Far more widespread training and adoption of the Hampshire Digital Media Advisers model to provide the public with better advice on digital issues and to serve as a more effective gateway to the development of more in-depth digital investigation capabilities.
- The development and running of training courses in how to understand, use and incorporate algorithmic decision support tools into police decision-making processes.

Recommendation 8: A new, coordinated approach to data accuracy in policing systems should be developed. This should include:

- Improved education and training for police officers and administrators on the importance of accuracy and detail when data is being captured.
- Provision of formal staff training programmes by private companies providing predictive and data-driven policing systems as part of the 'grand police-provider bargain'. This should be negotiable since the police's role in capturing crime data is helping these companies to better develop their predictive tools for the future.
- Greater use of automated checklists to ensure officer compliance with data input rules, and use of automated technology to transcribe officer input into formal documents which can then be automatically transmitted into a central database.

Again, one way of embedding this would be through the development and dissemination by the College of Policing of new Authorised Professional Practice with regard to the management of data accuracy in police systems.

Recommendation 9: UK policing needs a common set of data standards and data entry codes to be used across the country. The Police ICT company should be given the role of developing these and their subsequent use should be mandated across all police forces. Also needed are a common set of access protocols across all police forces so officers can be sure that other forces are not only capturing the same data, in the same way and format, but that officers of the same rank and role are engaging with that data too.

A debate has been raging for years on how best to ensure that data held across force systems and boundaries is effectively joined-up. The National Law Enforcement Data Service system will join up some existing databases by putting them together on the same platform.

However, the CoPaCC survey mentioned earlier in this report on police attitudes and experiences with regard to the joining up of systems and confidence in police data is damning and further change is clearly required.

Implementation of the recommendation made here would help to build confidence that the data held in police systems was accessible, useful and accurate, and would help to avoid previous problems for example with the Police National Computer where many officers lost confidence that this would in fact be the case.

Recommendation 10: The purchase by police forces of any 'closed' technology or a system that is unable to be quickly and easily made interoperable with other equipment and systems should be banned. It is almost certainly a waste of public money and cannot be justified in a service whose effectiveness requires the joining up of data and systems within and across force boundaries.

Recommendations 9 and 10, taken together, would address one of the long-standing barriers and sources of complaint with regard to the ability of police forces to work effectively with each other and would make it easier for UK policing to join up systems and data with other public sector bodies with whom they may need to work in close partnership.

Recommendation 11: Police forces in the UK should examine and replicate a similar initiative to Burgernet Netherlands which could include the public in helping fight crime in a more structured way.

Peelian principles suggest police officers are citizens in uniform. In the digital age we need the police relationship with the public to be far more dynamic and continuous, and to find more proactive ways for citizens to help the police. No-one would suggest vigilantism, but a tech-enabled sense of shared responsibility for combating crime would be a step in the right direction.

Overall, the set of recommendations set out here, if implemented, would put the whole country, its philosophy of policing, and the police themselves in a much stronger position to embrace data-driven policing while maintaining public confidence. The maintenance of that public confidence is essential to the police's ability to pursue the kind of public value that this report has demonstrated data-driven policing can provide.

REFERENCES

ABC7 Chicago (2018) *Chicago Given $10 million to expand predictive policing* [online]. Available at: https://abc7chicago.com/chicago-given-$10m-to-expand-predictive-policing-officer-training/3327651/

Ariel, B., Sutherland, A., Henstock, D. et al (2016) Wearing body cameras increases assaults against officers and does not reduce police use of force: results from a global multi-site experiment. *European Journal of Criminology* 13(6), pp.744-755.

Ariel, B., Farrar, W.A., and Sutherland, A. (2014) The effect of police body worn cameras on use of force and citizens' complaints against the police: A randomized controlled trial. *Journal of Quantitative Criminology* 31(3), pp. 509-535.

Babuta, A. (2017) *Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities.* [online]. Available at: https://rusi.org/publication/occasional-papers/big-data-and-policing-assessment-law-enforcement-requirements

Babuta, A., Oswald, M. and Rinik, C. (2018) *Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges: Whitehall Reports 3-18.* London: RUSI. Available at: https://www.rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical

Balaram B., Greenham T. and Leonard J. (2018) *Artificial Intelligence: Real Public Engagemen.*, London: Royal Society of Arts.

BBC News (2016) Police forces 'overwhelmed' by digital evidence, watchdog finds. *BBC News,* [online] 3 November. Available at: https://www.bbc.co.uk/news/uk-37846705

Bitcoin News (2018) Chinese Police Develop Blockchain Based Evidence Storage., *Bitcoin News*, [online] 9 May. Available at: https://bitcoinnews.com/chinese-police-develop-blockchain-based-evidence-storage/

Bloomberg J. (2017) Using Bitcoin or other cryptocurrencies to commit crime? Law Enforcement is on to you. *Forbes*, [online]28 December. Available at: https://www.forbes.com/sites/jasonbloomberg/2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#5670418a3bdc

Bowen P. and Gibbs B. (2018) *Just Technology: Emergent Technologies and the Justice System*. London: Centre for Justice Innovation.

Carroll, R. (2017) Inspector gadget: how smart devices are outsmarting criminals. *The Guardian*, [online] 23 June. Available at: https://www.theguardian.com/technology/2017/jun/23/smart-devices-solve-crime-murder-internet-of-things

CBC (2017) Vancouver Police Now Using Machine Learning to Predict Property Crime. *CBC News*, [online] 23 July. Available at: https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111

CBS (2015) Shotspotter Technology Helps Cops In Camden Zero-In On Gunshots When They Happen. *CBSNew York*, [online] 12 January.. Available at: http://newyork.cbslocal.com/2015/01/12/shotspotter-technology-helps-cops-in-camden-zero-in-on-gunshots-when-they-happen/

Chavez-Dreyfuss G. (2018) About $1.2 billion in cryptocurrency stolen since 2017 – cybercrime group reports. *Reuters*, [online] 24 May. Available at: https://uk.reuters.com/article/uk-crypto-currency-crime/about-1-2-billion-in-cryptocurrency-stolen-since-2017-cybercrime-group-idUKKCN1IP2Q4

Chwalisz, C. (2015) *The Populist Signal: Why Politics and Democracy Need to Change.* London: Rowan & Littlefield International.

CNN (2017) ACLU Builds New App to Start New Conversations Around Policing. *CNN*, [online] 15 March. Available at: https://money.cnn.com/2017/03/15/technology/aclu-blue-app-policing/index.html

Coindesk (2018) China's Security Ministry Touts Blockchain for Evidence Storage. *Coindesk*, [online] 9 May. Available at: https://www.coindesk.com/chinas-police-ministry-touts-blockchain-for-secure-evidence-storage

College of Policing (2015) *College of Policing analysis: Estimating demand on the police service* London: College of Policing. Available at: https://www.college.police.uk/News/College-news/Documents/Demand%20Report%2023_1_15_noBleed.pdf

Columbus L. (2017) Round-up of Internet of Things Forecasts. *Forbes*, [online] 10 December. Available at: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#243cef891480

CoPaCC (2018) *Police ICT User Perspectives* [online]. Available at: https://policinginsight.com/reports/police-ict-user-perspectives-2018/

Davidson A. (2017) *Increasing trust in criminal evidence with blockchains* [online]. Available at: https://mojdigital.blog.gov.uk/2017/11/02/increasing-trust-in-criminal-evidence-with-blockchains/

Davies, W. (2018) How feelings took over the world. *The Guardian*, [online] 8 September 2018. Available at: https://www.theguardian.com/books/2018/sep/08/high-anxiety-how-feelings-took-over-the-world

Digital Policing Portfolio (2018) Written evidence submitted to the Home Affairs Committee inquiry Policing for the future [online]. Available at: http://data.parliament.uk/WrittenEvidence/CommitteeEvidence.svc/EvidenceDocument/Home%20Affairs/Policing%20for%20the%20future%20changing%20demands%20and%20new%20challenges/written/47182.html

Di Tella R. and Schargrodsky E. (2013) Criminal Recidivism after Prison and Electronic Monitoring, *Journal of Political Economy* 121(1) pp. 28-73. Available at: https://www.hbs.edu/faculty/Publication%20Files/JPE-Electronic%20Monitoring_e3fc1f85-dabe-409a-a028-0b1443e70d16.pdf

Dyn (2016) *Read Dyn's Statement on the 10/21/2016 DNS DDoS Attack | Dyn Blog*,[online] 22 October. Available at: https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

The Economist (2018a) Violent Crime is Down in Chicago. *The Economist*, [online] 5 May Available at: https://www.economist.com/united-states/2018/05/05/violent-crime-is-down-in-chicago

The Economist (2018b) *Technology Quarterly, Data Detectives*, 2 June 2018. Available at: https://ukshop.economist.com/products/technology-quarterly-data-detectives?redirect=International

The Economist(2018c) Crypto money-laundering. *The Economist,* [online] 26 April. Available at: https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

The Economist (2018d) Body-worn cameras are spreading beyond the police. *The Economist*, [online] 28 July. Available at: https://www.economist.com/britain/2018/07/28/body-worn-cameras-are-spreading-beyond-the-police

Edmonton Police Service (2015) *Body worn video: considering the evidence (Final Report of the Edmonton Police Service Body Worn Video Pilot Project*). Edmonton, AB, Canada: Edmonton Police Service.

F-Secure Cyber Security Research Institute (2018) *Pinning Down the IoT*. *Cyber Security Research Institute report into the Internet of Things*. Available at: https://fsecurepressglobal.files.wordpress.com/2018/01/f-secure_pinning-down-the-iot.pdf

Ferguson, A. (2017) Policing Predictive Policing., *Washington University Law Review* 94(5), pp.1156-1157.

Financial Action Task Force (FATF) (2015) *Emerging Terrorist Financing Risks*. Paris: FATF. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

Foley, S, Karlsen, J. R. and Putnins, T. J. (2018) Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *SSRN e-journal* 14 December. Available at: http://dx.doi.org/10.2139/ssrn.3102645

Franklin-Wallis, O. (2017) If we're living in a simulation, this UK startup probably built it. *Wired Magazine*, [online] 11 May. Available at: https://www.wired.co.uk/article/improbable-quest-to-build-the-matrix

Gayle, D. (2018) Police may need AI to cope with huge volumes of evidence. *The Guardian*, [online] 8 February. Available at: https://www.theguardian.com/uk-news/2018/feb/08/police-may-need-ai-to-help-cope-with-huge-volumes-of-evidence

Gilbert, P. (2015) Dubai's smart policing pilot shows promise for crime fight. *IT Web,* [online] 11 December. Available at: https://www.itweb.co.za/content/WPmxVE7Kgle7QY85

The Guardian (2018) Police Trial AI software to help process mobile phone evidence. The Guardian, [online] 27 May. Available at: https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

Greenberg, A. (2017) Monero the drug dealer's cryptocurrency of choice, is on fire. *Wired.com,* [online] 25 January. Available at: https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

Hitchens, P. (2018) We're all still suffering from Enoch's craziest, cruellest idea. *Mail Online,* 2 December. Available at: https://hitchensblog.mailonsunday.co.uk/2018/12/were-all-still-suffering-from-enochs-craziest-cruellest-idea.html

House of Commons Home Affairs Committee (2018) *Oral evidence: Policing for the future, HC 515 Tuesday 5 June 2018.* House of Commons. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future/oral/84322.pdf

House of Lords Artificial Intelligence Committee (2017) *AI in the UK: ready, willing and able?* Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm

Information Commissioner's Office (2018) *ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws.* [online]. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/

Isaac, W., and Dixon, A. (2017) Why big-data analysis of police activity is inherently biased. *The Conversation*, [online] 10 May. Available at: http://theconversation.com/why-big-data-analysis-of-police-activity-is-inherently-biased-72640

Jaguar News (undated) *Jaguar Land Rover to start real-world tests of innovative connected and autonomous vehicle technology.* Available at: https://www.jaguar.co.uk/news/connected-autonomous-vehicle-technology.html

Kupper, C. (2018) Deep Web, Deeper Faith. *Focus on the family,* [online] April 2018. Available at: https://www.focusonthefamily.com/socialissues/citizen-magazine/deep-web-deeper-faith

Lartey, J. (2017) Man suspected in wife's murder after her Fitbit data doesn't match his alibi. *The Guardian*, [online] 25 April. Available at: https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate

Liptak, A. (2017) Sent to Prison by a Software Program's Secret Algorithms. *New York Times*, 1 May. Available at: https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html

Marinus Analytics (2018) *AI for Good: A Spinoff Success Story,* [online] 8 June. Available at: https://www.cs.cmu.edu/news/ai-good-spinoff-success-story

Marr, B (2018) How Blockchain Could End the Trade in Blood Diamonds., *Forbes*, [online] 14 March Available at: https://www.forbes.com/sites/bernardmarr/2018/03/14/how-blockchain-could-end-the-trade-in-blood-diamonds-an-incredible-use-case-everyone-should-read/#2215f89a387d

McGuire, M. (2018) *Into the Web of Profit.* Available at: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

Melendez, S. (2017) *Machine Learning: A New Weapon in the War Against Forced Labor and Human Trafficking* [online], Fast Company.Available at: https://www.fastcompany.com/3068128/machine-learning-a-new-weapon-in-the-war-against-forced-labor-human-traffic

Mayor's Office for Policing and Crime (MOPAC) and the Metropolitan Police Service (MPS) (2017) *Public Access Strategy*, [online]Available at: https://www.london.gov.uk/mopac-publications/public-access-strategy

Moore, M. H. with Braga A. (2003) *The "Bottom Line" of Policing. What citizens should value (and measure!) in police performance.* Washington DC: Police Executive Research Forum. Available at: https://www.policeforum.org/assets/docs/Free_Online_Documents/Police_Evaluation/the%20bottom%20line%20of%20policing%202003.pdf

Morrison, S. (2018) Senior officer Sara Thornton: Police must tackle burglaries and violence and not waste time on hate crimes. *Evening Standard,* [online] 1 November. Available at: https://www.standard.co.uk/news/crime/hard-stretched-police-should-focus-on-core-offences-and-not-deserving-issues-like-hate-crimes-top-a3977401.html

Muir, R. (2017) *What do we want the Police to do? It's time for an honest debate* The Police Foundation, [online] 25 October. Available at: http://www.police-foundation.org.uk/2017/10/want-police-time-honest-debate/

National Audit Office (NAO) (2018) *Financial sustainability of police forces in England and Wales 2018* London: NAO. Available at: https://www.nao.org.uk/wp-content/uploads/2018/09/Financial-sustainability-of-police-forces-in-England-and-Wales-2018.pdf

National Crime Agency (NCA), Metropolitan Police Service (MPS) and National Police Chiefs' Council (NPCC) (2018) *Written submission to Home Affairs Committee Inquiry into Policing for the Future, 4 September, 2018.* Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future/written/88580.pdf

National Crime Agency (NCA) (2017) *Written evidence to the Home Affairs Select Committee Inquiry into Policing for the Future, 21 February, 2017*. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future-changing-demands-and-new-challenges/written/47206.pdf

National Police Chiefs' Council (NPCC) (2017) *Better Understanding Demand: Policing the Future* London: NPCC. Available at:https://www.npcc.police.uk/2017%20FOI/CO/078%2017%20CCC%20April%202017%2024%20Better%20Understanding%20Demand%20Policing%20the%20Future.pdf

National Police Chiefs' Council (NPCC) and Association of Police and Crime Commissioners (APCC) (2016) *Policing Vision 2025.* Available at: https://www.npcc.police.uk/documents/Policing%20Vision.pdf

New Indian Express (2018) Police to launch blockchain technology for better data management. *The New Indian Express*, [online] 2 August. Available at: http://www.newindianexpress.com/cities/thiruvananthapuram/2018/aug/02/police-to-launch-blockchain-technology-for-better-data-management-1851911.html

New York State Governor (2017) *Governor Cuomo Announces Major Facial Recognition Technology Milestone with 21,000 Fraud Cases Investigated* [online]. Available at: https://www.governor.ny.gov/news/governor-cuomo-announces-major-facial-recognition-technology-milestone-21000-fraud-cases

Office for National Statistics (ONS) (2019) *Crime in England and Wales: year ending September 2018* [online]. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018

O'Leary, R. (2017) Europol Warns Zcash, Monero and Ether Playing Growing Role in Cybercrime*. Coindesk,* [online] 3 October. Available at: https://www.coindesk.com/europol-warns-zcash-monero-and-ether-playing-growing-role-in-cybercrime

Oswald, M. Grace, J. Urwin, S. and Barnes, G. (2017) *Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'Experimental' proportionality.* Information and Communications Technology Law. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3029345

Owens, C. and Finn, W. (2018) Body-Worn Video through the Lens of a Cluster Randomized Controlled Trial in London: Implications for Future Research. *Policing* 12(1), pp.77-82.

Palmer, D. (2018) *An Internet of Things Crime Harvest is Coming Unless Security Problems are Fixed*', ZDnet, [online]. Available at: https://www.zdnet.com/article/an-internet-of-things-crime-harvest-is-coming-unless-security-problems-are-fixed/

Policemediablog.com (2017) *Not everyday you get a feature in Police Professional. – Policing by content.* Available at*:* https://policemediablog.com/2017/02/08/not-everyday-you-get-a-feature-in-police-professional/

Ramey, C. (2018) The Crypto-Crimewave is Here. *Wall Street Journal*, [online] 26 April. Available at: https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366

Reuters (2017) Police and Military Security Agencies are beginning to see blockchain as a potential solution to securing data. *Reuters*, [online] 3 December. Available at: https://www.firstpost.com/tech/news-analysis/police-and-military-security-agencies-are-beginning-to-see-blockchain-as-a-potential-solution-to-securing-data-4239465.html

Rodrigues, V. and Urban, R. (2018) The Startup is Using Blockchain to Fight Art Forgers. *Bloomberg*, [online] 23 March Available at: https://www.bloomberg.com/news/articles/2018-03-23/art-forgers-find-a-new-enemy-in-verisart-s-blockchain-startup

Schuba, T. (2018) CPD expands predictive policing technology, deploys 86 new officers. *The Chicago Sun Times*, [online] 3 April Available at it: https://chicago.suntimes.com/crime/cpd-expands-predictive-policing-technology-deploys-86-new-officers/

Searcy, B. (2017) Tapping into the Internet of Things will Help Police Departments Turn Smart Cities into Safe Cities. *Police Chief Magazine,* [online] 15 March. Available at: http://www.policechiefmagazine.org/tapping-internet-things/

The Seattle Times (2011) Diaz on DOJ report: 'Department is not broken'. *The Seattle Times*, [online] 16 December. Available at: https://www.seattletimes.com/seattle-news/diaz-on-doj-report-department-is-not-broken/

Sherman, L.. and Neyroud, P.(2012) *Offender-Desistance Policing and the Sword of Damocles* London: Civitas.

Spencer, D. and Cheshire, R. (2017) Ten Years of Body Worn Video in Northamptonshire Police. *Policing* 12(1), pp. 116-119.

Symantec (2016) *Mirai: what you need to know about the botnet behind the recent DDoS attacks* [online]. Available at: https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Tech UK (2017) *Policing and the Internet of Things*. London: Tech UK.

Thomson, A. (2015) *Using the Blockchain to Fight Crime and Save Lives* [online]. Available at: https://techcrunch.com/2015/09/27/using-the-blockchain-to-the-fight-crime-and-save-lives/

Thorn (2018) *Impact One Pager* [online]. Available at: https://27l51l1qnwey246mkc1vzqg0-wpengine.netdna-ssl.com/wp-content/uploads/2018/01/Thorn_Spotlight_Impact_Infographic_V2.pdf

Thorn (2017) *Impact report* [online]. Available at: https://www.wearethorn.org/impact-report-2017/

Vaas, L. (2013) *Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking* [online] 22 October. Available at: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

Volpicelli, G. (2017) How the Blockchain is Helping Stop the Spread of Conflict Diamonds. *Wired*, [online] 15 February. Available at: https://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger

Watkins, J. (2017) *The Future of Crime in the Blockchain Economy*[online]. Available at: https://www.ozy.com/fast-forward/the-future-of-crime-in-the-blockchain-economy/81435

White, D., Gaub, J.D., and Todak, N. (2017) Exploring the Potential for Body-Worn Cameras to Reduce Violence in Police Violence in Police-Citizen Encounters. *Policing* 12(1), pp.66-76.

Wilkins, D. (2017) It's a fair cop. Residents furious as 'stretched' police filmed riding on dodgems at fairground despite being on duty. *The Sun,* [online] 17 October. Available at: https://www.thesun.co.uk/news/4699766/humberside-police-officers-dodgems-hull-fair/

Wright, R. Police Force Uses Data to Assess Risk and Predict Crime. *Financial Times*, [online] 19 July. Available at: https://www.ft.com/content/81af2e14-7fb9-11e8-bc55-50daf11b720d

The Police Foundation
The Foundry
17 Oval Way
Kennington
London SE11 5RR
020 3752 5630

www.police-foundation.org.uk

ISBN 0 947692 71 1

Charity Registration Number: 278257

THE POLICE FOUNDATION

The UK's policing think tank