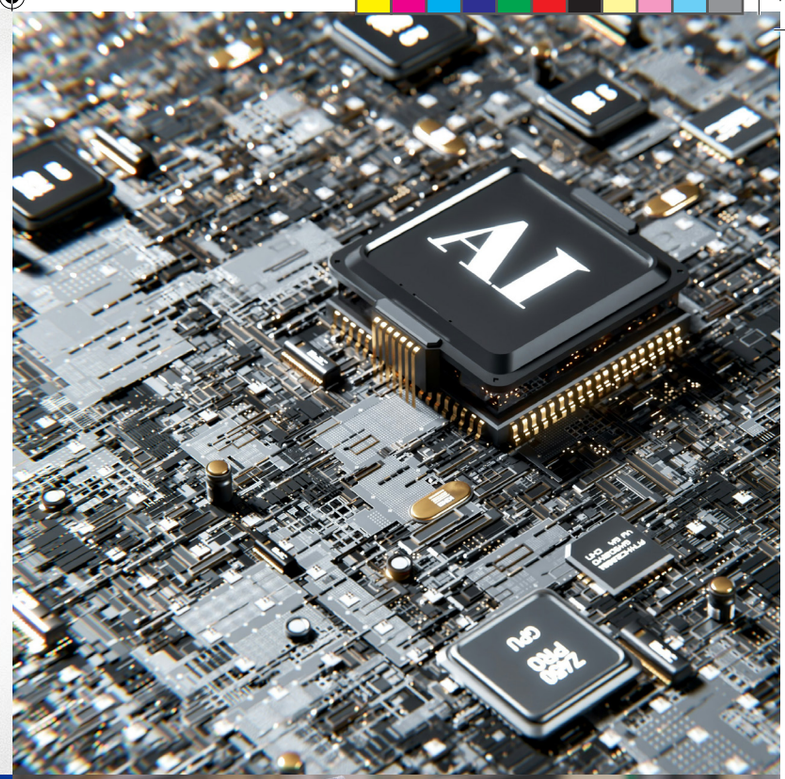

POLICING AND ARTIFICIAL INGELLIGENCE

THE POLICE FOUNDATION
The UK's policing think tank

RICK MUIR
FELICITY O'CONNELL

FEBRUARY 2025

POLICING AND ARTIFICIAL INTELLIGENCE

Rick Muir and Felicity O'Connell

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. Our mission is to generate evidence and develop ideas which deliver better policing and a safer society. We do this by producing trusted, impartial research and by working with the police and their partners to create change.

Dr Rick Muir is Director of the Police Foundation.

Felicity O'Connell is a Researcher at the Police Foundation.

The authors would like to thank Steve Rick, Chief Executive of Forensic Analytics, for contributing to the writing of the report.

Forensic Analytics

Forensic Analytics is a leading provider of digital forensics software, training and consultancy services. Over 90% of crimes now involve digital elements, often encompassing vast amounts of digital data, and Forensic Analytics helps investigators and analysts solve these cases more efficiently. The company was founded in 2013 by three committed engineers and expert witnesses and has since grown to a team of seventy professionals, drawn from backgrounds in law enforcement, telecoms, software development and RF engineering.

Cover: istockphoto/Pexels/Unsplash

CONTENTS

1. INTRODUCTION

Emily is on the phone to a 999-call handler. She is worried because a man who has been stalking her has been seen by a neighbour in a nearby street. While the call handler is talking to Emily and trying to reassure her, the call is being automatically transcribed into an artificial intelligence (AI) system that can search police databases. When Emily mentions the man's name and address, the AI software discovers that the man has a firearms licence and alerts the call handler that the police need to get to Emily's house straight away.

Police Constable Tony Williamson[1] has come across an elderly woman of British Pakistani heritage seemingly distressed in the street. He asks her if he can help, but she does not speak English. PC Williamson turns on the live translation tool on his mobile device and he asks her again. As she speaks, the woman's words are translated in real time into his earpiece. She says that she is worried because her son Mohammed did not come home from school. This was three hours ago, and she has been trying to look for him. She says her son has a history of mental health problems and often goes missing.

PC Williamson types 'what's your son's name and date of birth?' into the translation app on his phone and intuitively the keyboard is offered in Urdu. The woman types in the answer. The officer can run an immediate search across police databases for any information about her son. A full profile of her son Mohammed Iqbal[1] is generated, including a list of addresses with which he is associated. The officer calls the case in and escorts Mrs Iqbal home while reassuring her that officers are now looking for her son.

These are just two examples of the way AI powered technology could enhance the way that the police are able to serve the public. Policing is at its heart a complex information business, but it has struggled to make full use of the data stored on its many often outdated systems. AI could be transformative in policing because it can turn this wealth of data into actionable intelligence at the touch of a button.

However, the AI revolution poses a whole set of legal and ethical questions for the police and society. How far should the police go in using AI to keep communities safe? Could these technologies make the police *too* effective, in that they may be able to know much more about us and pry into our private lives to an unprecedented degree? How can we be assured of the reliability and accuracy of the AI tools being deployed? How do we feel about machines making or guiding decisions as to whether a crime should be investigated, or someone should be charged with a criminal offence? Which policing decisions ought to be reserved for human beings?

There are important technical, organisational and cultural questions too. Is the data the police hold ready for the AI revolution? Do police leaders understand the technology they are using? Are there the skills in the police workforce to properly exploit the potential of AI? Is the police service organised in such a way that it can properly make use of these new technologies?

In this report we explore these and other questions in the following ways:

1. We set out a brief history of the development of AI and define some of the terms used to describe its different forms.
2. We describe some of the ways in which AI is currently being used by UK policing and explore how it might be used in the future.
3. We identify eight challenges for the more widespread use of AI for policing purposes.
4. We make a number of recommendations for policymakers and police leaders intended to help policing make the most of the AI revolution, while maintaining public trust and confidence and protecting rights and freedoms.

1 This is a fictitious name.

The report is based on research undertaken between March and September 2024. This included a review of relevant academic and grey literature, interviews with 18 operational and strategic police leaders, policy makers, industry and civil liberties representatives, and a survey of chief information officers in English and Welsh police forces.[2]

2 With the support of the National Police Chiefs' Council we sent an online survey to chief information officers in 43 police forces in England and Wales. We received nine responses. Because we cannot be certain this sample is representative we have not analysed the survey results quantitatively. Instead, we have analysed the substantive free text responses as a source of qualitative data.

2. CONTEXT AND CONCEPTS

In this chapter we put the later discussion in context by setting out a brief history of the development of AI. We then go on to discuss what is meant by AI and define other key concepts such as machine learning, deep learning and neural networks that are distinct components of AI but are often used interchangeably.

2.1 A BRIEF HISTORY OF AI

The birth of AI dates back to the 1950s following Alan Turing's milestone paper *Computing machinery and intelligence* which explored the question 'can computers think?' (Turing, 1950). The term 'artificial intelligence' was coined by John McCarthy who hosted a famous workshop at Dartmouth in 1955 where the first artificial intelligence system 'Logic Theorist' was presented by Allen Newell, Cliff Shaw, and Herbert Simon.

From the 1950s to the late 1970s the development of AI faced both advances and setbacks. Computer storage capacity was increasing, and computers were becoming cheaper, faster, and overall, more accessible. However, limitations in computational power and processing speed and a lack of investment saw a decrease in AI development in academia and industry (Delipetrev et al., 2020).

The 1980s were considered an 'AI boom' with a big increase in funding and interest following advances in research (Anyoha, 2017). However, this was relatively short-lived, and it wasn't until the 1990s and early 2000s that major progress was made. Notable milestones included the defeat of the world champion and chess grand master Gary Kasparov by IBM's 'Deep Blue' AI decision making programme; speech recognition software being released by Microsoft Windows; and the development of the first robot, known as Kismet, that could display human emotions.

The following years saw a rapid growth in the use of AI by the social media, mobile phone and video streaming giants for advertising, user experience algorithms, and virtual assistants. Then came major breakthroughs in the mass use of AI with the launch of generative AI applications i.e., systems and algorithms that create new content or data such as text generation (for example GPT-3) and image generation (for example DALL-E2), targeted at the lay person or general user.

AI has enormous transformative potential for most sectors of the economy, as well as major implications for how we as individuals interact and use technology. Some have likened its disruptive impact to that of the industrial revolution (Jones, 2023). However, the growth of AI technologies has also come with a number of serious ethical, safety, moral, and societal risks, some of which we discuss later in this report.

2.2 SO, WHAT IS AI?

There is currently no universally agreed definition of AI. This is partly due to the difficultly in defining the abstract and subjective concept of human intelligence (Kaplan, 2016). The majority of definitions of AI refer to *"computers or machines that can perform like humans or are able to perform tasks that require intelligence"* (Samoili et al., 2020).

While technical, the definition of AI provided by The High-Level Expert Group (HLEG)[3] on Artificial Intelligence is comprehensive and includes the different facets of AI (including *"perception, understanding, interpretation, interaction, decision making, adaptation to behaviour and achievement of goals"*; Samoili et al., 2020, p.8):

> *"Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the*

3 See https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

Table 1. A taxonomy of AI (Samoili, 2020).

AI taxonomy		
Core	AI domain	AI subdomain
	Reasoning	Knowledge representation
		Automated reasoning
		Common sense reasoning
	Planning	Planning and scheduling
		Searching
		Optimisation
	Learning	Machine learning
	Communication	Natural language processing
	Perception	Computer vision
		Audio processing
Transversal	Integration and interaction	Multi-agent systems
		Robotics and automation
		Connected and automated vehicles
	Services	AI services
	Ethics and philosophy	AI ethics
		Philosophy of AI

physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions."

Samoili et al. (2020) developed a taxonomy that characterises what they describe as the core and transversal (or intersecting) domains of AI. As shown in their taxonomy in Table 1 above, AI covers many domains including technology, science, ethics and philosophy. This broad spectrum of domains may be one of the reasons why we lack a consensus around a single definition.

There is general confusion around AI associated terminology, with many distinctive sub-components of AI being used interchangeably. It is better to see AI as an overarching concept while machine learning, deep learning and neural networks are subsets of AI, each encompassing the next.

Machine learning involves algorithms that learn from experience and improve their decision-making or predictive operations over time. Machine learning can be supervised i.e., when the machine is trained (by a person) using data that is well labelled (data matched with the correct answer/classification). The input data is then paired with the desired output and once this relationship is learned, the trained machine can then make predictions on new unlabelled data. Examples of supervised machine learning include linear and logistic regressions, classifications, and support vector machines.

With unsupervised machine learning the machine learns from unlabelled data. As such the machine discovers relationships, patterns, and processes in unlabelled and uncategorised data with no predefined output.[4]

4 See https://www.ibm.com/think/topics/reinforcement-learning

Deep learning is a subset of machine learning which uses a complex layered structure of algorithms or 'artificial neural networks' to analyse data. Deep learning automates a great deal of feature extraction, recognising similar patterns and using decision boundaries to cluster inputs appropriately. The benefits of deep learning include the ability to handle large and unstructured data at high speed with high accuracy in addition to automatic pattern recognition. Examples of deep learning applications include computer vision (e.g., self-driving cars and facial recognition); automatic speech recognition such as virtual assistants (e.g., Siri, Alexa, Cortana and Google); Chatbots for customer queries, feedback and complaints; translation (e.g., language and images to text and vice versa); and generative AI (e.g., text, audio and image generation).

Artificial Neural Networks are the backbone of deep learning and are made up of input, hidden, and output layers, mimicking the neurons of the human brain. Neural networks tend to provide single outputs or results such as a word or action whereas deep neural networks (deep learning) provide a global output based on all the input data supplied.

Having described the development of AI over time and distinguished between its different components, the next chapter focuses on how it is being used in policing.

3. THE USES OF AI IN POLICING

While public debate and media discourse around policing and AI naturally focus on the most contentious areas of operational police work (particularly the use of technologies such as Live Facial Recognition for example), many of the most transformative areas in which AI could play a role are much more mundane. We describe a number of these in the use cases set out below.

In considering how AI technologies may be put to use in policing, it is important to consider the public value they may add. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) breaks down the public value generated by policing into three domains, which provide a useful starting point. Can AI make policing more or less *effective* in keeping the public safe, investigating crime, responding to incidents and so forth? Can AI make policing more or less *efficient* in the way it spends public money? And can AI make the police more or less *legitimate* in the eyes of the public, as seen through levels of trust and confidence in the police? We will consider these different dimensions of public value as we look at the use cases below.

It is also important to distinguish between four different types of technology in which AI may have an impact on policing and public safety: there is the technology the police use to store and exploit information (what was traditionally known as 'police IT'), there is the technology that offenders use to commit crimes, there is the technology that the police use to stop people committing crimes and there is the technology the police use to investigate crime. In this paper we focus on the first, third and fourth of these types of technology.

3.1 CURRENT USES OF AI IN UK POLICING

It is hard to quantify the degree to which AI technologies are currently being used in UK policing. Fundamentally there is a lack of information in the public domain around the availability of these tools, their use and how they are implemented in practice (Zilka et al., 2022).

Freedom of information requests to explore the use of algorithmic decision aids across all UK police forces have confirmed that around 15 per cent of forces use these tools, although the proportion has no doubt increased since that research was conducted (Couchman, 2019; Oswald and Grace, 2016).

More recently, the National Police Chiefs' Council (NPCC) has stated that all police forces use data analytics and at least one third of forces use advanced data analytics (NPCC, 2023). According to the NPCC, the majority of AI applications are used for organisational effectiveness and workforce planning (e.g., triage of 999/101 calls and automation of data administrative tasks (NPCC, 2023).

Our survey respondents from nine English and Welsh police forces listed the following areas where their forces are either currently using or considering using AI technologies:

- Back office/business support functions
- Risk management of warrants
- Facial recognition
- Redaction
- Forensic analysis of data
- Intelligence and demand forecasting
- Resource allocation (officer and vehicle)
- Intelligence (facial recognition, uncovering hidden links, mapping)
- Performance optimisation (optimising investigative timelines)
- Risk reduction
- Data bias

- Model drift (or the degradation of a model's prediction power due to changes in the environment, and thus the relationships between variables)
- Health warnings
- Lie detection
- Automated triage
- Early identification of exploitation and routes to criminality

In what follows we distinguish between three broad uses of AI technologies in policing: first, to make routine processes more efficient through Robotic Process Automation (RPA), second, to help the police prevent and investigate crime and third, to improve the quality of contact between the police and the public. Below we look at some cases in depth, exploring how they may impact on effectiveness, efficiency and legitimacy.

3.1.1 Robotic Process Automation

According to IBM, Robotic Process Automation (RPA) uses intelligent automation technologies to perform the repetitive office tasks of human workers, such as extracting data, filling in forms, moving files and more. Given the level of law and regulation around operational police activity, RPA has the potential to make a significant contribution to policing by enhancing efficiency, reducing the chances of human error and freeing up time so that the police can focus on their core (and their uniquely human) responsibilities.

It may also contribute to improving the wellbeing and retention of police officers and staff, by allowing them to spend less time filling out forms and more time directly serving the public.

Disclosure of evidence

The Crown Prosecution Service (CPS)[5] has said that proper disclosure is vital for a fair trial but admits the criminal justice system has "*struggled to get it right*". It launched a National Disclosure Improvement Plan with the NPCC in 2018 and said it had led to significant improvements. Disclosure of evidence has been a significant challenge for policing and other parts of the criminal justice system. The Serious Fraud Office averages around five million documents[6] an investigation and those investigations take around four and a half years. Most of that time is spent reviewing vast amounts of data much of which has no bearing on the investigation. RPA has the potential to revolutionise the approach to disclosure by cataloguing relevant information far more efficiently than humans and finding that needle in a thousand haystacks.

There is already an independent review underway chaired by Jonathan Fisher KC, to consider how the disclosure regime is working in the digital age and whether fraud law meets the challenges of modern offending, including whether the penalties are proportionate to the impact of the crime.

In his preliminary report published in April 2024 Jonathan Fisher[7], makes the point that

> *"The proliferation of digital material and the progressively complex nature of offending in both volume and serious crime means that disclosure is an increasingly time and resource intensive process for all parties, which has the impact of slowing down case progression in the criminal courts. This is acutely felt in the prosecution of 'disclosure heavy' crime types such as fraud and also rape and serious sexual offences cases (RASSO) where digital evidence is frequently found. The volume of material generated and gathered in criminal cases continues to rise".*

Fisher has already identified the need to explore the full range and capabilities of the technological and AI solutions which might be available.

Digital redaction tools

The Policing Productivity Review (2023) highlights that approximately 770,000 hours are used to manually redact data by officers and police staff

5 Jonathan Fisher KC, 2018

6 Home Office, 2024

7 Home Office, 2024

whereas the use of digital redaction tools could free up at least 618,000 hours of staff time. Using this data, we can extrapolate it to show a saving of 82 per cent. The cost saving, if based on a Detective Constable on a base salary of £27,000 and paid £13.85 per hour, would in this example result in a saving of £8.5 million. The Productivity Review recommends that the Police Digital Service and the Policing Productivity Team should prioritise the implementation of redaction technology in police forces by September 2024.

Bedfordshire Police has pioneered the use of DocDefender to auto redact documents (personal and metadata or information that describes other data such as how it was collected, who collected it etc) before they are sent to the Crown Prosecution Service. Bedfordshire police told the authors that the redaction burden across policing is enormous and manually undertaking this task is *'morale destroying'.*

Bedfordshire Police provides an example of how much time can be saved by using this tool: one officer was able to redact an 800-page document in one hour which would have previously taken 15 hours to complete manually. The force estimates that once the tool is embedded, more than 9,500 officer and staff hours will be saved per year (Bedfordshire Police, 2023). The force told the authors that it has saved time equivalent to 10 people per year, which can be reallocated to more important and public facing tasks.

Automation of requests for authority

Bedfordshire Police has similarly developed an automated approach to requests for authority i.e., where a chief officer must provide authorisation before an operational deployment. Such reports have until now required officers to manually search through multiple police systems and read through lots of different intelligence reports.

The force pointed to examples such as authorities for the deployment of firearms or directed surveillance, which used to involve an officer manually compiling a report over four hours per authority. This can now be done by RPA in one minute.

3.1.2 Crime prevention and investigation

AI technologies are also being used to help the police become more effective in the prevention and investigation of crime, examples of these are outlined below.

AI imaging

Some forces are using counter proliferation IOT (Internet of Things) device forensics, whereby software can analyse images and determine the location of a potential victim of human trafficking or a missing person.

Predictive policing

Predictive policing uses algorithms and data analytics to predict the geographical areas where future crimes may occur (to direct policing resources) or to make individual risk assessments to predict who is likely to commit an offence or become a victim of crime. Originally, police forces were using commercial software programs however, some of these proved to be too costly to sustain (Couchman, 2019). For instance, Kent Police used PredPol (software developed by a US firm to predict where and when crimes would occur) for five years until 2018 when its £100,000 per year costs were deemed too high and subsequently withdrawn. Some forces are now designing and implementing 'in house' predictive software programs (Robinson et al, 2016).

From 2016 to 2021, Durham Police used the Harm Risk Assessment Tool (HART) which was a form of supervised machine learning (random forest forecasting) to classify arrested individuals at low, medium, or high risk of committing a violent or non-violent offence in the next two years. Those considered low or medium risk were eligible to participate in a 'Checkpoint' rehabilitation programme, which if completed would allow them to avoid charge and prosecution. Durham Police ceased use of the HART tool in 2021. Various flaws were identified in the HART tool such as over-estimation of the likelihood of re-offending and discrimination in the data (see Fair Trials, 2022).

Another predictive tool in development is the Domestic Abuse Risk Assessment Tool (DARAT). This tool uses information gathered by the

attending officer at a domestic abuse case as well as any available historic data relating to the people involved to predict the likelihood of further harm occurring in the year following the incident. The prediction falls into three categories: standard risk, medium risk, and high risk. While not yet implemented, piloting and evaluation of the tool appears promising (College of Policing, 2022).

One force that is relatively advanced in its use of predictive policing software, especially in relation to individual risk assessments of victims and perpetrators, is Avon and Somerset. For instance, programmes are used that can predict the likelihood of an individual's victimisation and vulnerability, of their being reported missing, of them being a victim of stalking and harassment, of them being a victim of a serious domestic or sexual violence. Tools can also estimate the likelihood of a suspect re-offending and perpetrating burglary, stalking and harassment, serious domestic or sexual violence.

The force created more than 40 apps that can be used to conduct searches of their entire dataset, based on features such as a suspect name, an address, or a number plate. This overcomes a common problem facing many police forces, which is that they 'do not know what they know', because up until now it has been too time consuming and costly to run a manual check across multiple databases. 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 or individuals where they may need to focus their resources, and they can alter force deployment decisions, strategy and even operational tactics as a result of that insight.

Facial Recognition technology

Facial Recognition (FR) is used by a number of forces in the UK. There are three types of this technology in use or development:

- Live Facial Recognition (LFR) which involves a camera scanning a scene and checking facial images against a database of wanted individuals.
- Retrospective Facial Recognition (RFR) which involves looking over images or videos taken from CCTV, dashcams, mobile phones, social media, and video doorbells. These images are compared to arrested individuals to verify identity or help to identify the missing and deceased.
- Operator Initiated Facial Recognition (OIFR) which allows officers to photograph a person of interest to verify their identity.

The use of facial recognition by police is increasing, and in 2023 the Policing Minister urged forces to double the number of retrospective facial recognition searches in 2024.

LFR cameras are now deployed routinely by the Metropolitan Police Service (MPS). The MPS told the authors of this report that they are deployed to high crime areas, identified by their crime harm severity score (a measure which indicates crime levels multiplied by their severity, using sentence length from the government's Sentencing Guidelines). They are typically used to identify persons wanted for homicide, rape and serious violence, as well as persons wanted by the courts. So far in 2024, the use of LFR by the MPS has resulted in the arrest of around 250 wanted persons. The MPS found that areas deploying LFR are three times more efficient at identifying wanted persons than those using traditional methods, such as just deploying Territorial Support Group officers.

Operator Initiated Facial Recognition is used when an officer wants to confirm the identity of an unknown subject. An image will be taken on an officer's mobile phone and submitted via an app to be checked against police databases. South Wales Police told us that the technology has a 100 per cent true identification rate.

However, the deployment of automated facial recognition technology has been challenged by academics, charities, civil liberties organisations, and the Home Office Biometrics and Forensics Ethics Group. These groups have contested the legal basis for the use of the technology and have raised concerns about privacy and bias (Purshouse and Campbell, 2022). 2020 saw the world's first successful legal challenge to the police

use of live facial recognition technology where it was held that use of the technology by South Wales Police was unlawful (Court of Appeal in *R (Bridges) v Chief Constable of South Wales Police and Others* [2020] EWCA Civ 1058). Indeed, the European Parliament in June 2023 banned the use of live and most retrospective facial recognition systems in public places. A number of US States have also banned the use of facial recognition.

The accuracy and bias of the technology has been a core concern and the MPS and South Wales Police have worked with the National Physical Laboratory (NPL) to try to deal with this. Recent tests by the NPL found no bias in the use of Retrospective and Operator Initiated Facial Recognition technology. They found some racial and gender bias in the use of Live Facial Recognition technology, but they said that accuracy can be preserved by setting the equipment to only make identifications at a higher threshold for image quality (Mansfield, 2023).

3.1.3 Public contact

Chatbots

The potential for AI to reduce the time and effort that citizens need to expend during police interactions is considerable. Chatbots are being used to provide automated and semi-automated responses to many simple or transactional enquiries that arrive in police contact centres.

In Bedfordshire for example, chatbots are used to handle issues such as property claims and animal welfare issues that would otherwise take up the time of call handlers who can better be deployed on the more serious incidents. 20 per cent of queries to Bedfordshire Police are now answered by chatbots.

Translation and natural language technologies

Instantaneous translation between multiple languages makes it easier for non-English speakers to access services. Natural Language technologies that can sort, triage, direct and provide initial responses to either free-text or voice content – or even identify stress, fear, or other relevant sentiment in callers' voices – are being trialled, and clearly hold potential to help many people get what they need from the police more quickly and easily.

There are concerns about the use of AI in police contact management that ought to be noted. In particular, there could be a clash between the desire for effort reduction (making the interaction as frictionless as possible for the caller), and the need to ensure police-citizen interactions accord to the principles of procedural justice. Procedural justice is about ensuring that citizens feel they have been treated fairly and with respect during encounters with the police. It has been shown to be a big driver of police legitimacy. The concern is that procedural justice requires a recognition of shared group status between the citizen and the police, which may be lacking if the citizen is speaking with a robot. This is an area that merits future research.

However, in principle there should be opportunities here: if chatbots and other automated tools can be used to deal with transactional requests more efficiently, human call handlers should be able to spend more time dealing with people who are vulnerable, in crisis or generally in need of support (see Higgins, 2024 for a more in depth discussion of this question).

3.2 FUTURE USES

We asked our interviewees and survey respondents for examples of future use cases for AI in policing. The following is a summary of the ideas they suggested:

- **Video redaction:** facial recognition technology could be used to blur faces so footage can be used publicly or in court.
- **Prioritising and assisting with emergency calls:** AI assistants could help to triage calls and offer advice and assistance to the call handler by bringing up relevant data as the call is in progress, helping to identify threat, harm, risk and vulnerability. Sentiment analysis could also be used to detect emotion in someone's voice. Ultimately, we could see fully automated call handlers, but this would obviously need to be handled with an eye to which calls really do need a human response.

- **Early warning signs to flag wellbeing issues with officers and staff:** AI could offer automatic advice and support to officers or call handlers who have just dealt with a traumatic incident.
- **Investigation case files and case management:** AI could help guide investigators through the different orders or evidence they might need. Automated case file production could save huge amounts of police time.
- **Identifying internal employee threats:** AI could monitor patterns of digital behaviour by officers and staff and may be able to flag up warning signs for unusual or concerning behaviour.
- **Edge processing:** building in sensors and other devices into an officer's uniform and kit should help them to operate more effectively and access systems on the go. For example, live language translation for officers operating in communities where many people do not speak English as a first language.
- **Dynamic situational awareness:** a large language model could generate a read out for officers on a situation they are being deployed to, with key things they will need to know.
- **Synthetic police data:** developers need data to build useful tools, but generally it is inappropriate to share personal data and involves going through lengthy data sharing processes. What if AI could create fake cases and fake individuals based on real ones, which could then be shared with the development community?

4. THE CHALLENGES FOR THE POLICE USING AI

Based on our interviews and survey responses, we have identified eight key challenges for the police in making the most of the AI revolution.

4.1 CULTURE

The first challenge is that the culture and mindset of policing is not geared towards embracing technological change. One aspect of this is that policing is an overwhelmingly reactive business, responding to current demand rather than looking ahead and thinking strategically about the future. As our interviewees said:

> *"They are permanently fighting fires in policing."*
>
> *"Policing is always fighting the last war."*

This lack of strategic foresight means that insufficient thought is given to how policing can harness AI and other leading-edge technologies.

> *"AI and how it can be used hasn't really been thought about enough by policing."*

There is also a tendency for police leaders to think tactically rather than strategically about new technology. One of our interviewees described a 'Magpie syndrome' whereby police leaders go after *"shiny new things"* rather than thinking about how a better harnessing of data could impact the whole of their business. Others described how the police tend to focus on the technology rather than the problem they want to solve, or indeed to think about equipment over information, which ultimately is what the technology is helping to exploit.

A number of interviewees highlighted a lack of technological and data literacy among senior police leaders, as well as a reluctance to change:

> *"There are some chief officers that are really fantastic and want to innovate and want to do some really great stuff, but we still have a culture… in senior policing of Bobby on the beat, and they got to their position because they're fantastic at what they do, but actually they're coming to the end of their careers. Are they really thinking that far ahead?"*

4.2 DATA READINESS

Machine learning tools are trained on both structured and unstructured data, but one of the big problems in policing is that the quality of the data the police hold is often poor (some of our interviewees used more colourful language), meaning that there is a risk, as one person put it, of *"putting garbage in and getting garbage out".*

There are a lot of erroneous entries in police data and a lack of standardisation across the 43 forces in the way data is entered and coded. This makes it hard to share data and it is also an obstacle to developing AI tools, because these tools need to be trained on large databases and good quality data. As one interviewee told us:

> *"They have tried certain types of data analytics and concluded that they just don't have enough data to do it…. because they're only using police databases…. Also, they've realised through doing some of this modelling that a lot of the data is really, really bad quality in terms of it being all messed up with the names wrong, and things in the wrong boxes."*

Another stressed the importance of building the right foundations before progressing with AI:

> *"I think forces are still a bit overexcited, but I think what policing needs to focus on first before they can really start adopting AI is the data quality, data standards, standardised interoperability piece and really getting the nuts and bolts right in policing."*

4.3 ORGANISATION

The way in which the police service is organised is an obstacle to the diffusion of new technologies like AI. There are two aspects to this organisational challenge that on one level seem contradictory. First, the fragmented nature of the system, with 43 police forces, means that the information is locked into different legacy systems that vary from place to place and do not speak to each other.

Moreover, there is no central testing and validation of AI tools, with every force instead doing its own thing:

"The gap that I think needs to be filled is that I don't think you can have 43 forces independently testing so actually what we need is a central test and assurance function and probably a network of test houses."

"The challenge is trying to get 43 police forces (to move in the same direction) and if you haven't got some power or mandate, then people just go off in different directions. So, I think that's the risk. And, if you had an AI application and you required it to be validated….. then for every police organisation to do that individually, to me that would be bonkers".

However, there is a second aspect to the organisational challenge, which is that innovation may slow if forces must wait for big national programmes. Bedfordshire Police has made big strides with Robotic Process Automation because the force told us that they take a "*sapling approach"* to innovation and "*do not wait for national solutions*."

From the other side of the marketplace, we were told by suppliers that the fragmentation of the system can be a good thing for startups trying to enter the market. We were told that most large mature organisations tend to have a bias towards the big incumbent providers, because even while they tend to cost more and are less innovative, they seem less risky. So, startups find the best way of accessing the system is to build a relationship with a smaller force that can act as a proof of concept for the rest of the system.

As one interviewee put it:

"What we find …with forces is they sort of know what they want to buy and they kind of know which supplier they're going to use and the safe option is to go OK, well, this one force is using this particular tool, so I'm just going to use that… and the startups … are developing some really innovative tools, but they just don't get a look in because the forces just go back to the same old suppliers over and over again."

So, there is a tension here between the need for sufficient local autonomy to enable innovation, while not allowing fragmentation to prevent data sharing and interoperability, nor to block national solutions where it makes sense to do something once not 43 times. We return to how to resolve this organisational dilemma in the next chapter.

4.4 ETHICS

There are a whole series of ethical questions that arise from the police use of AI.

First, there is the problem of bias. Police data is not an objective picture of the real world, but rather data that is skewed towards people, places and incidents that are reported to the police or that the police come across in the course of their work. This means there are some inherent biases in the data that can skew the results. Moreover, there is the potential for algorithmic amplification of latent data biases, and of the risks of an exponential expansion of errors that accompany powerful AI applications. Ensuring that issues of bias are addressed through initial testing is therefore critical before the deployment of AI in operational policing contexts.

Our survey respondents suggested some ways to mitigate the problem of bias

"AI poses massive risks, it learns faster than us, which is great when it works, but it also means that it goes wrong faster, and the effects of its errors are far more serious. It is essential that all AI is subject to rigorous governance, both in terms of ethics and appropriateness checks in the planning phase, and through continued ethical governance throughout its implementation and use. Technical and architectural oversight is also essential, especially when solutions are being created in house. When models are being built it is essential that they are checked for concept drift, data bias, model drift, interpretation bias, imperfect distribution across protected characteristics, and that those using the output are not becoming blindly compliant to the suggestions of the AI.'

"The central risk is through statistical prejudice and the disproportionate targeting of certain ethnic groups e.g. through FR [facial recognition] software. This can be mitigated through a combination of the tolerance levels being directly controlled and of manual/human elements and safeguards being built into the systems."

Others emphasised the importance of officers and staff not being over reliant on these tools and of maintaining the so-called 'human in the loop':

> *"Generative AI…needs human oversight. A risk would be the automatic acceptance of what the AI has produced but through training and compliance with defined acceptance criteria this could be mitigated."*

> *"As long as it is not the only method to reach a decision and simply a contribution or a prompt then any risks should be mitigated."*

Second, there is the question of privacy. One of the major issues with the use of LFR cameras is about the spread of police surveillance in public space. As a representative of a civil liberties group told us:

> *"I think one of the main problems with live facial recognition is that anybody who falls into the zone of recognition has their biometrics scanned and processed. So, from a privacy perspective, and from a kind of broader perspective of what kind of society do we want to live in, (it is problematic) when the state has access to that type of data and can identify and track you."*

It should be noted there is strong public support for the use of LFR, with 70 per cent of the public supporting the use of LFR in police investigations (Ada Lovelace Institute, 2019). However, in the same study this was qualified by support for appropriate safeguards and a view that LFR should be reserved for identifying the most serious criminals.

One of our survey respondents also highlighted the importance of limiting how long personal data will be stored by the police:

> *"It is a matter of building public trust and confidence in AI solutions.Trusting that data will be deleted when no longer required also needs to be demonstrated by the AI providers"*

Third, there is the question of transparency. Given the powers the police have, it is essential that the public can hold them to account. However, many of the new technologies and practices have been implemented without significant public consultation and debate (Bradford et al., 2020; Grimond and Singh, 2020). This is concerning given the public's lack of awareness of the use of new technologies.

For instance, a survey conducted by the RSA in 2018 found that only nine per cent of the public were aware that automated decision-making systems were being used in the criminal justice system.

Research into the public's understanding and awareness of AI is limited and conflicting. Some surveys have reported that 85 per cent of respondents have heard of AI (Cave et al., 2019), whereas others have found that only nine per cent of respondents have heard of Machine Learning (RSA, 2018). In order to make effective and informed decisions and to increase trust in the use of AI, many scholars have suggested the need to open the 'black box' of AI and provide transparency around justifications of use (de Fine Licht and de Fine Licht 2020).

In response to calls for increased transparency around the use of algorithms and data driven technology across the public sector, the UK government recently (November 2021) introduced the draft 'Algorithmic Transparency Standard' to *"promote trustworthy innovation by providing better visibility of the use of algorithms across the public sector, and enabling unintended consequences to be mitigated early on"* (Domagala, 2021).

Oswald et al. (2022) carried out a qualitative study to explore the implications for police forces of participation in the Transparency Standard, to identify benefits, risks and challenges for the police, and areas where the Standard could be improved. Participating in the Standard was found to help the police demonstrate competent implementation of technology-driven policing and that this can enhance trust. Participating in the Standard also increased the opportunity for sharing best practices (and pitfalls) across police forces. While Oswald et al. (2022) highlight several areas where there could be improvement and amendments to the Standard, overall, it appears that using the standard as part of reflective practice could help secure public trust around the police use of technology.

4.5 LAW

There is currently no specific legislation or law regulating AI in the UK (Bhatnagar and Gajjar, 2024,). As one interviewee said:

> *"We need a government that is…helping and supporting, because otherwise innovation will be thwarted. We'll be in the courts for years….I think the government does need to play more of a leading role because 43 forces doing it 43 different ways without any legislation, we could be tied up in the courts"*

There are various laws pertaining to the restriction of AI use in practice (e.g., Data Protection Law; Equality, Privacy and Common Law – including Human Rights and Intellectual Property Law). The EU implemented the AI Act which is the first ever dedicated regulation of AI. The Act sets out different rules or obligations for providers and users depending on the risk of the AI being used: unacceptable risk which will be prohibited (e.g., manipulative or deceptive AI, social scoring and biometric categorisation systems; live and remote biometric identification systems); high risk which include systems that negatively impact safety, fundamental rights or the environment (e.g., critical infrastructure; education; emotion recognition systems; law enforcement; migration and asylum etc); limited risk AI systems that meet certain transparency obligations for instance where people are informed if they are interacting with an AI chatbot to enable them to decide whether to continue or request human engagement instead; minimal risk includes AI systems that are already widely used such as spam filters and AI-enabled video games.

In 2023, the UK government published a white paper detailing how it intends support the development of AI technology as well as regulate the use of AI. The framework focuses on five areas: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance and contestability and redress.

In response to the government's white paper, 30 civil society groups signed a statement detailing key principles for an alternative AI white paper which includes: mandatory transparency; clear mechanisms for accountability at all stages of development, ownership, and deployment of AI tools; public consultations around automated decision making tools before deployment; a specialist regulator for enforcement and accountability and the prohibition of AI tools that threaten fundamental rights.[8]

In the absence of dedicated legalisation, the National Police Chiefs' Council (NPCC) published the Covenant for Using Artificial Intelligence in Policing (NPCC, 2023) which provides a set of principles for how AI will be used in policing to ensure it is responsible, proportionate, and accountable. Endorsed by UK police forces and all members of the NPCC, the principles include:

- All uses of AI in policing should be **lawful.**
- All uses of AI should be **transparent**, which will involve the public being made aware of forces using AI and forces publishing their algorithms and training data limitations. Where this is not possible (due to operational/security constraints) independent assessors will examine the AI tool. Third parties must also be able to scrutinise the data and algorithms from an 'adversarial perspective'.
- AI outputs should be **explainable**.
- AI should be used **responsibly** i.e. intentions are defined before use to enable tracking of outcomes and impact. This principle also states that procedures are put in place to prevent users from accepting outputs uncritically.
- There should be clearly identified individuals who are **accountable** for the use of AI both operationally and for the AI outputs. These individuals must be suitably trained to use the specific AI tool.
- The data used in AI (training data and data that is analysed by AI tools) must be **robust** and reliable. This will require *"assessing, tracking and reporting on the quality of the data, by way of recognising that the quality of the data dictates the quality of the analysis."*

8 See https://publiclawproject.org.uk/content/uploads/2023/06/AI-alternative-white-paper-in-template.pdf

4.6 WORKFORCE

Exploitation of AI in policing will also require an appropriately skilled workforce.

On a general level, as we have already noted, there is a perceived lack of awareness and understanding of AI and other leading-edge technologies within policing. As one survey respondent told us:

> *"Data literacy is not sufficiently high to use all the tools let alone create them."*

An interviewee from private industry said:

> *"The police don't know enough about what the technology is capable of and where it's going."*

There was a concern about whether police officers and staff using these tools have a good enough understanding of the outputs and how they have been arrived at:

> *"There isn't really an understanding that it's…a probabilistic tool, so it's giving you effectively an intelligence that's a statistical probability of something being right. It's not giving you a sort of factual thing and there isn't that understanding I think generally about the way AI systems work and the underlying statistical methods that are used to produce the output…But you need to understand how it works underneath the box."*

Interviewees also highlighted a need for specialist skills, particularly data engineering and data science skills:

> *"Our team includes data engineers, and you very definitely do need data engineers, but I would suggest that data science is a lot more than the coding. So…you do need to be able to code various things, because you're coding to build the models. But the knowledge of what it is that you're supposed to do, given the question and the nature of the data, that requires knowledge that isn't coding related, it's stats, it's machine learning related, data science related stuff. So, finding those skills is important."*

4.7 RESOURCES

A number of our interviewees stated that additional investment is key, not just in the technology but in the specialist staff and organisational support structures required:

> *"Forces need more funding to be able to take advantage of AI. Technology never gets cheaper! Pay structures (are needed) that enable competitive pay for specialist tech skills."*

> *"We lack the funds to acquire expensive staff or the equivalent in consultancy. The main challenges are thus low levels of data literacy, lack of staff, lack of funds"*

> *"I think funding (is one of the biggest issues), I mean obviously we always want more money, but I think money spent…on the right areas and I'm quite a supporter of the idea of some kind of centre of excellence…that has reach into forces or areas of the system that are doing particular things particularly well and which is driving consistency and doing …rapid innovation and applied research."*

4.8 ABSTRACT POLICING

We need to consider how a more automated police service will affect the relationship between the police and the public. This is not just about avoiding the problems of inaccurate or biased tools discussed above, but it is also about making sure that as more of policing is done by machines, we do not put at risk the basic Peelian model of policing with the consent of the public.

For example, can encounters between citizens and machines maintain the quality of procedural justice? Without a deep sense of social affirmation and moral connection, will citizens continue to view encounters with the police as fair or legitimate?

Research indicates that the quality of procedural justice may be hard to sustain when human representatives are substituted by technology, such as chatbots and online reporting forms (Aston et al., 2021; Bradford, et al., 2022; Wells et al., 2023). The evidence on this is still emerging, but this is clearly an area of risk as policing innovates around AI and public contact.

In this chapter we have identified eight key challenges for policing if it is to make best use of AI technologies. In the next chapter we discuss what might be done to tackle these challenges.

5. WAYS FORWARD

In this chapter we turn to the ways in which the police could respond to the challenges identified in our research.

5.1 TECHNOLOGICAL AND DATA LITERACY

We were told how too often senior police leaders view technology as risky or as a '*bolt on*' rather than as part of core delivery of service. Developing greater technological and data literacy among senior police leaders could be achieved through:

- Making technology and data literacy a much more important element of senior leadership development programmes in policing, such as the Executive Leadership Programme.
- Encouraging secondments for police leaders in industry.
- Ensuring that senior leadership teams contain sufficient technological expertise.
- Holding forces to account for their data readiness and use of technology, such as through HMICFRS thematic inspections or by making it a stronger component of the PEEL process.

5.2 DATA READINESS

It is clear that one of the major barriers to the adoption of AI in policing is the condition of police data. Because it is often inconsistent, incomplete and contains many errors, it cannot provide a workable training ground for machine learning. It is therefore of vital importance that police forces accurately collect and cleanse their data as the first steps in enabling maximisation by AI tools.

A nationally coordinated approach to data quality in police 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.
- Greater use of automated checklists to ensure officer compliance with data input rules.
- A common set of mandatory data standards and data entry codes to be used across the country.

5.3 A STRONGER NATIONAL FRAMEWORK FOR DELIVERY

In addition to having to work with 43 operationally independent Chief Constables and a similar number of Police and Crime Commissioners, the national landscape when it comes to delivering police technology programmes is weak and fragmented.

There are currently four bodies involved in delivering technology programmes at the national level. There is the NPCC Data, Digital and Technology Coordination Committee, which leads on coordinating work on digital technology across the 43 forces. There is the Office of Chief Scientific Adviser to policing, which seeks to exploit the opportunities of new science and technological innovations. There is the Police Digital Service, which runs several national programmes and recommends technology and data standards. And there is the Home Office which hosts and maintains some of the major systems.

To take a truly strategic approach to taking advantage of AI, it would be far better to bring all these bodies together into a single home for national leadership around police technology. Elsewhere, the Police Foundation has called for a national police headquarters or agency, which would be a legal entity with the ability to host strategic, operational and enabling capabilities as well as to set a single national technology strategy. A new national delivery framework should be led by a full-time national lead for digital technology, with powers to set mandatory standards in areas like data quality and interoperability.

This body could also provide a central test and assurance centre for AI technologies, working

with a network of regional test centres. Local forces should be innovating with new technologies and should not have to wait for permission to do so. However, rather than all 43 forces having to validate new technology themselves, this could be assured centrally, which would speed up the pace of adoption. It could also provide advice and guidance and be responsible for a clear national framework around ethics, law, and security, so forces do not have to go through all of these processes themselves every time.

We need a system where local forces can innovate at pace, but within a clear framework of standards set nationally so that data can be shared and be made available for innovation and so that local innovations can be tested and assured for use by the wider system.

5.4 A NATIONAL ETHICAL FRAMEWORK FOR THE USE OF AI IN POLICING AND A NATIONAL POLICE TECHNOLOGY ETHICS COMMISSION

In the absence of dedicated legislation governing the use of AI by police forces, it is important that a single national framework for the ethical use of AI in policing is put in place. Our survey respondents flagged the importance of doing this centrally rather than locally:

> *"(We need) a nationally led ethical AI policy (which is) not… the responsibility of the individual force Chief Constable who may not have the reassurance or knowledge to own that public facing assurance."*

> *"(We need) investigation and resolution of legal and privacy issues at the centre and not individually by forces."*

This can build on the work of the many local ethics commissions or panels that have developed in areas such as London and the West Midlands.

It can also build on the principles set out in the *Covenant for Using Artificial Intelligence (AI) in Policing* (NPCC, 2023). One way of doing this would be to establish a National Police Technology Ethics Commission which would issue guidance for police forces around different use cases and technologies. This would provide greater clarity around the rules of the game and could be buttressed by mechanisms for public, as well as expert, participation and deliberation.

5.5 WORKFORCE TRANSFORMATION

It is clear that policing requires more specialist skills to make the most of the AI revolution. This includes a need to recruit more data engineers, data analysts, technical architects and data scientists. Policing will need to be willing to pay competitively to attract people into these roles. It may need to consider a clearer national offer to attract these skills, such as by establishing common job descriptions for these roles and clearer progression pathways.

There should also be more porous boundaries between the police service and industry, with more police leaders spending time on secondment in industry. Programmes to recruit specialist volunteers into policing with data and technology backgrounds, such as the NPCC Cyber Specials Programme, should be expanded.

5.6 INVESTMENT

New AI technology can be expensive, as are those with the skills to make best use of it. The government needs to shift the emphasis in police funding away from 'officer numbers' and towards maximising effectiveness, efficiency and legitimacy through police spend. Over the course of the next two Spending Reviews the government should raise the proportion of the police budget spent on science and technology.

6. CONCLUSION

Policing is a complex information business and makes countless routine decisions based on the intelligence it has received and the incidents it has recorded on its databases. Until now it has struggled to make best use of that information, which has been locked into legacy systems and insufficiently shared.

AI potentially enables policing to do a lot more, and more quickly, by rapidly putting actionable intelligence in the hands of police officers and staff. It could also rid policing of considerable labour-intensive form filling and bureaucratic work, enabling the police to focus their human resources on where they are needed most: speaking with victims, reassuring communities, and interviewing suspects. It could mean that the police can get to complex calls more quickly because they can deal with transactional matters automatically.

At the same time, work is needed to lay the foundation for AI powered policing. There is a need for a proper framework of national standards in terms of ethics, technology and data. This almost certainly requires a new national policing body with the power to mandate where national solutions are in the public interest. Police forces need to be data ready; by cleaning up their databases so they are ready for AI applications. Police leaders need to be technologically and data literate, so they don't see 'IT' as something that is done by one part of the organisation, but as a core part of everything the police do. And the police service needs to recruit those with the expertise to help them make the most of the latest phase of the technological revolution.

The good news is that none of this is impossible and that if policing takes the next steps set out in this report it should be able to use AI to provide a better service to the public, while commanding public trust and confidence and protecting citizens' rights and freedoms.

REFERENCES[9]

Ada Lovelace Institute (2019) *Beyond face value: public attitudes to facial recognition technology*. London: Ada Lovelace Insititute. Available at: <https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf>

Anyoha, R. (2017) *The history of artificial intelligence*. Science in the News, 28.

Aston, E., O'Neill, M., Hail, Y., Wooff, A. (2021) Information sharing in community policing in Europe: Building public confidence. *European Journal of Criminology*, 20(1), pp.1349-1368. Available at: <https://journals.sagepub.com/doi/10.1177/14773708211037902>

Babuta, A. (2022) *Independent Report on the West Midlands Police RFSDi Harm Score and Integrated Offender Management Model*. Available at: <https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2023/01/3.0-RFSDi-IOM-Evaluation-Report-vFINAL-1.pdf?x59042>

Bedfordshire Police. (2023) *Auto-redaction of text for transfer to the Crown Prosecution Service.* Available at: <https://www.college.police.uk/support-forces/practices/auto-redaction-text-transfer-crown-prosecution-service>

Bhatnagar, A., and Gajjar, D. (2024) *Policy implications of Artificial Intelligence (AI)*. London: Parliamentary Office of Science and Technology (POST). Available at: <https://researchbriefings.files.parliament.uk/documents/POST-PN-0708/POST-PN-0708.pdf>

Big Brother Watch (2020) *Big Brother Watch briefing on Algorithmic Decision-Making in the Criminal Justice System*. London: Big Brother Watch. Available at: <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/02/Big-Brother-Watch-Briefing-on-Algorithmic-Decision-Making-in-the-Criminal-Justice-System-February-2020.pdf>

Bradford, B., Aston, E., O'Neill, M., and Wells, H. (2022). 'Virtual policing', trust and legitimacy. In J. Terpstra, R. Salet, and N. R. Fyfe (Eds.), *The Abstract Police: Critical reflections on contemporary change in police organisations* (pp213-238). Eleven International Publishing.

Bradford, B., Yesberg, J. A., Jackson, J., and Dawson, P. (2020) Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. *The British Journal of Criminology*, 60(6), pp.1502-1522. Available at: <https://doi.org/10.1093/bjc/azaa032>

Cave, S., Coughlan, K., and Dihal, K. (2019) "Scary Robots": Examining Public Responses to AI. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society (AIES '19)*. Association for Computing Machinery, New York, USA, pp.331–337. Available at: <https://www.repository.cam.ac.uk/items/70d00e4c-51f9-4615-b767-486e44e5946f>

College of Policing (2022) *Domestic Abuse Risk Assessment (DARA) Information for stakeholders* Ryton-on-Dunsmore: College of Policing. Available at: <https://library.college.police.uk/docs/college-of-policing/Domestic-Abuse-Risk-Assessment-2022.pdf>

Couchman, H. (2019) *Liberty's briefing on police use of live facial recognition technology.* London: Liberty. Available at: <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIBERTYS-BRIEFING-ON-FACIAL-RECOGNITION-November-2019-CURRENT.pdf>

de Fine Licht, K., and de Fine Licht, J. (2020) Artificial intelligence, transparency, and public decision-making. *AI and Society*. 35 (4), pp.917-926. Available at: <https://doi.org/10.1007/s00146-020-00960-w>

9 Accessed 1 October 2024

Delipetrev, B., Tsinaraki, C., and Kostic, U. (2020) *Historical Evolution of Artificial Intelligence.* Joint Research Centre, European Commission. Available at: <https://op.europa.eu/en/publication-detail/-/publication/6264ac29-2d3a-11eb-b27b-01aa75ed71a1/language-en>

Domagala, N. (2021) *What is our new Algorithmic Transparency Standard?* Gov.uk, [blog] 29 November. Available at: <https://dataingovernment.blog.gov.uk/2021/11/29/what-is-our-new-algorithmic-transparency-standard/>

Fair Trials (2022) FOI reveals over 12,000 people profiled by flawed Durham police predictive AI tool. *Fairtrails.org*, [online] 15 August. Available at: <https://www.fairtrials.org/articles/news/foi-reveals-over-12000-people-profiled-by-flawed-durham-police-predictive-ai-tool/>

Fisher, J. (2018) *Independent Review of Disclosure of Fraud Offcences: Preliminary findings and direction of travel.* London: Home Office. Available at: <https://www.gov.uk/government/publications/independent-review-of-disclosure-and-fraud-offences-preliminary-findings/preliminary-findings-and-direction-of-travel-accessible>

Grimond, W., and Singh, A. (2020) *A force for good? Results from FOI requests on artificial intelligence in the police force*. London: RSA. Available at: <https://www.thersa.org/globalassets/reports/2020/a-force-for-good-police-ai.pdf>

Higgins, A. (2024) *Blueprints: Designing local policing models for the 21st Century*. London: The Police Foundation. Available at: <https://www.police-foundation.org.uk/publication/blueprints-designing-local-policing-models-for-the-21st-century/>

Home Office (2024) *Independent Review of Disclosure and Fraud Offences.* Available at: <https://www.gov.uk/government/publications/independent-review-of-disclosure-and-fraud-offences-preliminary-findings/preliminary-findings-and-direction-of-travel-accessible>

Jones, K. (2023) *AI governance and human rights: Resetting the relationship*. London: Chatham House. Available at: <https://www.chathamhouse.org/sites/default/files/2023-01/2023-01-10-AI-governance-human-rights-jones.pdf>

Kaplan, J. (2016) *Artificial Intelligence: What Everyone Needs to Know*. New York: Oxford University Press.

Mansfield, T. (2023) *Facial Recognition Technology in Law Enforcement Equitability Study*. Teddington, Middlesex: National Physical Laboratory. Available at: <https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf>

NPCC (2023) *Covenant for using Artificial Intelligence (AI) in Policing*. London: NPCC. Available at: <https://science.police.uk/site/assets/files/4682/ai_principles_1_1_1.pdf>

Oswald, M., Chambers, L., Goodman, E. P., Ugwudike, P., and Zilka, M. (2022) *The UK Algorithmic Transparency Standard: A Qualitative Analysis of Police Perspectives.* SSRN. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4155549>

Oswald, M., and Grace, J. (2016) Intelligence, policing and the use of algorithmic analysis: a freedom of information-based study. *Journal of Information Rights Policy and Practice*, 1(1). Available at: <https://jirpp.winchesteruniversitypress.org/articles/10.21039/irpandp.v1i1.16>

Purshouse, J., and Campbell, L. (2022) Automated facial recognition and policing: a Bridge too far? *Legal Studies*, 42(2), pp.209–227.

Robinson, A.L., Myhill, A., Wire, J., Roberts, J., and Tilley (2016) *Risk-led policing of domestic abuse and the DASH risk model*. Ryton-on-Dunsmore: College of Policing. Available at: <https://library.college.police.uk/docs/college-of-policing/Risk-led-policing-2-2016.pdf>

RSA (2018) *Artificial Intelligence: Real Public Engagement*. London: RSA. Available at: <https://www.thersa.org/globalassets/pdfs/reports/rsa_artificial-intelligence---real-public-engagement.pdf>

Samoili, S., Lopez Cobo, M., Gomez Gutierrez, E., De Prato, G., Martinez-Plumed, F., and Delipetrev, B., (2020) *AI WATCH. Defining Artificial Intelligence*. Publications Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/83838dbc-3d1f-11ec-89db-01aa75ed71a1/language-en>

The Policing Productivity Review (2023) *Improving outcomes for the public.* Available at: <https://assets.publishing.service.gov.uk/media/655784fa544aea000dfb2f9a/Policing_Productivity_Review.pdf>

Turing, A.M. (1950) Computing Machinery and Intelligence. *Mind*, 59(236), pp.433–460. Available at: <https://doi.org/10.1093/mind/LIX.236.433>

Wells, H. M., Aston, E. V., Bradford, B., O'Neill, M., Clayton, E., and Andrews, W. (2023) 'Channel shift': Technologically mediated policing and procedural justice. *International Journal of Police Science and Management*, 25(1), pp.42-52. Available at: <https://journals.sagepub.com/doi/full/10.1177/14613557221132962>

Zilka, M., Sargeant, H., and Weller, A. (2022) *Transparency, Governance and Regulation of Algorithmic Tools Deployed in the Criminal Justice System: a UK Case Study*. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (AIES '22). Association for Computing Machinery, New York, USA, pp.880–889. Available at: <https://doi.org/10.1145/3514094.3534200>

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE POLICE FOUNDATION

The UK's policing think tank