



Cumberland Lodge Police Conference 2024

CONFERENCE REPORT



THE
POLICE
FOUNDATION
The UK's policing think tank

POLICING AND THE FOURTH INDUSTRIAL REVOLUTION

NOVEMBER 2024

About Cumberland Lodge

Cumberland Lodge is an educational charity and social enterprise that exists to empower young people to lead the conversation around social division – providing them with the skills, perspective, and confidence to question, challenge, and understand some of the most complex social issues of our time.

Day-to-day our buildings and facilities operate as a social enterprise, hosting conferences, meetings, and similar events on a commercial basis. We use the profits to support our educational programme, promoting progress towards more peaceful, open, and inclusive societies since 1947.

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.

About the Cumberland Lodge Police Conference

For more than 40 years, the annual Police Conference held at Cumberland Lodge has provided an inclusive and collaborative space for police leaders, practitioners, academics, civil society groups and others to discuss the pressing policing issues of the day. Since 2023 the conference has been organised by the Police Foundation, under the guidance of the Conference Steering Committee.

Contents

Foreword	4
Jason Hogg	
Conference speakers	5
Key themes from the 42nd Cumberland Lodge Police Conference: 14th -16th June 2024	6
Andy Higgins and Ruth Halkon	
How to operationalise ethical use of policing technology	9
Giles Herdale	
How the Fourth Industrial Revolution can enhance productivity, public service, and police training: from 'just-in-case' to 'just-in-time' and 'just-for-me' learning	11
Ellie Pyemont	
Who you gonna call?	12
Professor Louise Westmarland	
Reflections on the Cumberland Lodge Police Conference 2024	13
Rt Hon Alun Michael	
Increasing public support for Live Facial Recognition in policing	14
Michelle Weller	
How to do AI accountability – and why it's worth the effort	16
Professor Babak Akhgar OBE and Professor Petra Saskia Bayerl	
Policing and the Fourth Industrial Revolution	18
Ruth Halkon	

We are entering a phase of technological development with such radical potential to transform human society, that it has been dubbed the Fourth Industrial Revolution. Alongside the incredible opportunities offered by this new age, profound questions are emerging about its implications for public safety and security, and the changes that will be required to our policing arrangements to contend with the new challenges it will bring.

The 42nd Cumberland Lodge Police Conference, held over a long weekend in June 2024, provided an immersive opportunity for senior police officers, practitioners, academics, technologists and representatives from non-profit and private sector organisations, to gather, hear expert testimony, and engage in focused conversations about the critical issues we now face.

This report is an attempt to capture the key content and spirit of those discussions, and to share it with a wider audience. Bookended by a summary of key conference themes and a copy of the pre-event briefing paper (both provided by the Police Foundation), the report's core consists of six personal reflections on the weekend's proceedings, contributed by conference delegates. These summarise and explore key material from the presentations, develop ideas sparked in the conference

margins, and present individual perspectives on some of the issues raised. As a collection these combine to create a rich and vibrant distillation of the conference's core content, while also standing as an excellent example of the high-quality and diverse thinking that will be needed if policing is to successfully adapt to the technological and social changes ahead.

I would like to thank all of the contributors for taking the time and effort to commit their post-conference thoughts to paper. I'd also like to offer my thanks to Cumberland Lodge and the Police Foundation, along with the Conference Steering Committee, for convening such a high-quality and absorbing event. Finally, as I take over as Chair of the Steering Committee, I'd like to express my sincere gratitude, first to Canon Dr Edmund Newell, who is standing down as Chief Executive of Cumberland Lodge and whose support for the Police Conference over many years has been invaluable, and second to my predecessor, Olivia Pinkney CBE QPM, whose energy and wisdom has helped to secure the Cumberland Lodge Policing Conference as a unique and invaluable fixture of the policing policy calendar.

Jason Hogg

Chair of Cumberland Lodge Police Conference Steering Committee and Chief Constable of Thames Valley Police

Conference speakers

Olivia Pinkney CBE QPM DL – former Chief Constable, Hampshire and Isle of Wight Constabulary. Outgoing chair of the conference steering committee

Canon Dr Edmund Newell – Chief Executive, Cumberland Lodge

Carl Miller – Research Director CASM, Demos

Professor Paul Taylor – Chief Scientific Adviser for Policing

Andy Doran – Enterprise Account Executive, Salesforce

Professor Lawrence Sherman – Chief Scientific Officer, Metropolitan Police Service

Gillian Routledge – Chief Operating Officer, Lancashire Constabulary and National Police Chiefs' PCC Robotic Process Automation lead

Professor Ben Bradford – Professor of Global City Policing at the Department of Security and Crime Science, University College London

Martin Taylor – Deputy CEO, Content Guru

Tony Blaker – Chief of Staff, Cumbria Police and Digital, Data and Technology Coordination Committee

Professor Suzanne Shale – Chair of the London Police Ethics Panel

Lindsey Chiswick – Director of Intelligence, National Police Chiefs' Council Lead for Facial Recognition and Metropolitan Operations and Performance, Metropolitan Police Service

Dr Susan McKeever – Head of Data Science and Artificial Intelligence, Technological University, Dublin

Dr Christina Thorpe – Head of Cybersecurity, Technological University, Dublin

Rt Hon Alun Michael – Former Police and Crime Commissioner for South Wales and former Policing Minister

Imogen Parker – Associate Director, Ada Lovelace Institute

Professor Babak Akhgar OBE, FBCS – Director CENTRIC

Professor Petra Saskia Bayerl – Head of Research, CENTRIC

Sir Mark Rowley QPM – Commissioner, Metropolitan Police Service

Bernard Rix – Publisher, Policing TV/Policing Insight

KEY THEMES FROM THE 42ND CUMBERLAND LODGE POLICE CONFERENCE: 14TH -16TH JUNE 2024

Andy Higgins and Ruth Halkon

1. Policing and the Fourth Industrial Revolution

We are standing in the shallows of a new age of technological development that will radically alter the course of human history. Just as steam, electricity and computing power transformed societies in the late 18th, 19th and 20th centuries, so the Fourth Industrial Revolution, powered by the fusion of Artificial Intelligence (AI), biotechnology, advanced robotics and the Internet of Things, will bring barely imaginable changes to the way we live, work and interact in the 21st century.

As we look towards that horizon, profound questions about our safety and security are moving into view:

- What threats will emerge from this new phase of the digital revolution?
- How should governments and police agencies contend with the new crimes it will unleash?
- How can these technologies be harnessed to improve the effectiveness and productivity of policing and law enforcement?
- What are the implications for the police workforce as traditional tasks are increasingly performed by machines?
- And what of the wider democratic policing mission: the intricate balancing of freedom with safety, surveillance with privacy, control with legitimacy, and independence with accountability, which – since the birth of modern policing during the first industrial revolution – have been core to the British ideal?

These were the questions confronting delegates and speakers at the 42nd Cumberland Lodge Police Conference held in June 2024.

In the foreground, a set of present-day challenges loomed large: the threat of international dark-web criminality, the deluge of child sexual abuse imagery produced by generative AI, and the step change in response to gender violence demanded from our resource-constrained police services. Alongside these,

numerous examples were offered of how innovations such as Robotic Process Automation, Natural Language Processing and Live Facial Recognition are already reshaping modern police delivery. While surrounding all, swirled a nebulous array of concerns, needs, points of view and gut-reactions, that are a long way from forming consensus.

These contemporary threats, applications and contexts form the testbed for the new policing age. They expose gaps in existing arrangements, test the adequacy of long-held wisdom, upset established orders, and disrupt the dynamics of social relationships in complex and unexpected ways. They challenge us to act quickly but also wisely. How and what policing learns from them will prove crucial for securing public safety and cooperation in the turbulent decades ahead.

In this volume we bring together personal reflections, inspired by the conference, from six attendees. As a collection, it brilliantly captures the rich mix of ideas and emotions generated by the weekend's discussions: the sense of terrifying exposure mixed with incredible opportunity, a realisation of the deep entanglement of technological and social domains, the surfacing of new ethical and governance challenges, and an appreciation of the dynamic wisdom – the ability to do the right things at pace – that will be needed by our police leaders to navigate the next phase of the technological revolution.

Before handing the stage to our delegate contributors, we briefly set the scene by summarising some of the conference's key insights around these five thematic markers.

2. Terrifying exposure

There is good reason for unease at the dawn of the fourth industrial revolution, and not just about the way bad actors – some of whom may have had few criminal opportunities, or been deterred by the risk of detection in more analogue times – are exploiting new technologies, at scale, and in harmful and corrosive ways. The sense of exposure also comes from realising the deep maladaptation of our public safety systems

to the new profile of threats. Under-resourced for transformation and facing unfamiliar challenges, like safeguarding ‘truth’ in the age of disinformation and deep-fakery, UK law enforcement finds its hands tied by jurisdictional boundaries and with limited channels for international cooperation, while sophisticated criminality flows unchecked across borders, sometimes enabled by permissive hostile states.

There is also cause for scepticism about the potential for corporate regulation to curtail emerging online harms when (for instance) requirements for age verification on social media platforms, and content moderation on widely used image generation sites, seem easy to circumvent. The blunt suggestion from one expert that protecting children from online harm might involve taking the ‘social guns’ of camera-enabled smart phones from their hands, implies little faith in regulation or corporate responsibility to create a safe online world.

Against these challenges policing can seem worryingly – infuriatingly – hidebound by perennial, mundane problems like poor data quality, closed-system IT architecture, a lack of workforce readiness, and the reluctance of some in leadership to confront the inevitability of technological change. We are facing, as one speaker put it, *“21st century problems, with 20th century thinking and 19th century legislation”*, and while the public discourse remains stubbornly fixated on police officer numbers, the pace of technological change quickens, and our police services, often with antiquated IT systems, risk being left further and further behind.

3. Incredible opportunity

At the same time, however, the conference heard numerous examples of how technological and analytical innovation is already providing transformative opportunities for policing to become more effective, productive and precise. While some agencies have been hesitant about letting ‘the machines’ into police data, others are embracing and exploring *“the art of the possible”*.

For example, Robotic Process Automation – the automatic replication and repetition of human keystrokes – is already being used to redact disclosure files, producing considerable savings in officer and staff time. Natural Language Processing is being used in police control rooms to capture caller information prior to connection, produce call transcripts, and assist with triage and risk-assessment, reportedly taking

minutes off the time spent processing each call. New analytic techniques, joining up disparate data systems, are improving the identification of children in homes where domestic abuse occurs. Live Facial Recognition is helping to arrest wanted criminals in public spaces and has potential to reduce human bias and ‘collateral damage’, while new analytical approaches are enabling precision targeting of high-harm offenders.

These are, it was noted, transitional steps, more properly located within the Third Industrial Revolution than the Fourth, but future advances – many already within the realms of realistic possibility – will soon take us to and beyond that threshold. Smart Dust, for instance (a system of many tiny micro electro-mechanical systems (MEMS)), could be deployed to gather comprehensive information about crime scenes; biometric analysis could replace forensic DNA techniques; remote knife detection (using millimetre waves and AI to differentiate knives from other objects) could reduce the need for divisive stops and searches, and advances in quantum computing could substantially increase the analytic and predictive capabilities available to law enforcement.

There are, of course, crucial questions about what *should*, as well as what *can* be done, and – as Giles Herdale discusses in the first of our delegate reflections – more work is needed to operationalise high-level commitments to ethical technology use into police practice. But delegates heard how the environment for responsible, systemic innovation is beginning to take shape. National coordination committees have been formed to provide governance, consistency and shared learning; the funding pipeline to support innovation is beginning to flow; and those breaking new ground in pioneering forces are sharing practical learning about the team structures and working approaches (*“start small and build trust”*) that can help bring leaders and colleagues along.

The waters ahead may seem daunting but British policing is (as one speaker put it) already *“quite a long way from the shore”*.

4. Technological and social entanglement

Perhaps the single most important learning to emerge from the conference was about the way technological and social dimensions of evolving police practice are intrinsically intertwined. As one speaker put it, we need to consider the *“sociotechnical ripples”* of new tools and

processes: it is not just a matter of building “*robocops*”, but understanding how technology affects the way we think, act and interact as humans – both within police agencies and at policing’s interface with citizens and society.

Internally, the oft repeated message was that using AI and similar innovations to eliminate dull, time-consuming tasks like form-filling, data cleaning and redaction, can (and should) be used to free-up officers and staff to concentrate on “*the good stuff*” – the things that only humans can do, like being compassionate, attentive, creative, reflective and supportive. There are important policy implications here about the need to reinvest (rather than cash-out) the efficiency saving made through automation, back into the essentially *relational* core of good policing.

There are also significant workforce implications. Alongside the challenge of bringing technical skills into the service, a less bureaucratically shackled workforce may also be one in which those ‘human’ qualities become more intensively in demand. Technology can assist here too. For instance, as an indefatigable listening ear, AI can be used to identify and provide information in real time, that officers and staff need to make better decisions. It can also monitor operatives’ processes, alerting them to possible oversights, and provide individualised feedback data, enabling workers to review and refine their own performance. In short – as Ellie Pyemont explores in our second delegate reflection – AI holds promise for optimising the ‘human’ capabilities of the police workforce as well as freeing it from administrative drudgery.

There is also careful thinking to be done about how a more technologised police service interfaces with the public. It seems likely (and experiments appear to confirm) that elements of procedural justice – the deep sense of social affirmation and moral connection that citizens look for during dealings with the police – are more difficult to convey when human representatives are substituted by technological ones such as chatbots and online reporting forms. Whether this may change as younger and future generations become habituated to interacting with, and relating to, intelligent machines, remains to be seen, but for the present – as Louise Westmarland makes plain in Reflection 3 – imperatives around automating police/public contact to improve efficiency appear in tension with the task of improving public trust.

5. Ethical and governance challenges

Powerful technology with profoundly disruptive social consequences, demands renewed attention to questions of responsible use – particularly given policing’s susceptibility to “*mission creep*” and tendency for pragmatic boundary-pushing. Delegates were warned about the potential for algorithmic amplification of latent data biases, and of the risks of “*exponential expansion of errors*” that accompany powerful AI applications. Questions were also raised about policing’s relationship with the private sector: the need for algorithmic transparency and the way public sector purchasing power might be leveraged to incentivise ethical corporate practice.

New contexts, in which more is known (and potentially knowable) about us, also require new ways for thinking about concepts like privacy – which one speaker suggested might usefully be reframed as “*the right to the appropriate flow of personal information*”. Understanding and codifying ‘appropriateness’, however, requires clarity about the purposes to which, and values with which, information is being processed and technology deployed, characteristics that – as Alun Michael argues in Reflection 4 – are too often recessive in current debate.

The conference also heard how public deliberation exercises, exploring informed citizens’ views on the bounds of appropriate public-sector AI use, indicate qualified public support for innovation, contextualised by the specifics of individual use-cases and (significantly) by existing trust relationships – but also caveated with doubts about the competency of government agencies to use technology well. Citizen panels were also concerned about the “*social chilling*” effect of heightened surveillance and the algorithmic extension of existing biases, and made strong calls for clearer rule setting, algorithmic transparency and for mechanisms for challenge and redress. The current public preference for maintaining a ‘human in the loop’ may prove a point of tension, as the ability of machines to out-perform human decision makers becomes increasingly clear. The task of engaging the public in constructive dialogue around controversial innovation is considered by Michelle Weller in Reflection 5.

Debate surrounded the extent to which existing, multi-layered police oversight systems can provide adequate accountability in these new contexts. Does the way law enforcement deploys AI and related technology need

new and additional governance frameworks – potentially utilising principles such as legality, transparency, explainability, enforceability and learning/adaptability, as described by Babak Akhgar and Petra Saskia Bayerl in Reflection 6 – or would additional processes add unnecessary friction and delay? What seems clear is that policing needs good “brakes” (as one delegate put it will) to allow it to move at speed, while maintaining the consent and confidence of the public.

6. Dynamic wisdom

The pre-conference briefing paper (appended to this collection) opens with the myth of Scylla and Charybdis, a pair of closely aligned classical shipping hazards that tested many a Greek hero and have since been evoked to convey the perils that governments and legislators must navigate as technological progress shapes and reshapes our world. Reflecting on the 42nd Cumberland Lodge Police Conference, the metaphor seems apt and multilayered.

At the dawn of the Fourth Industrial Revolution, policing faces multiple paired and proximate risks: of over-caution and over-reach; of inaction and blunder; of failure to imagine the future and of losing sight of its enduring values; of jeopardising public trust and

neglecting public safety; of failure to predict and of stifling social flourishing.

The margins between these hazards often seem perilously fine, and safe navigation will require both wisdom and dynamism; learning fast and listening hard; brave innovation and shrewd investment. Steering that safe course is perhaps the greatest challenge facing policing’s current and future leaders.

But the metaphor might also apply in another way. As a nation, we ask a lot of our police. We charge them to bringing safety to multiple domains of our lives, we turn to them for redress, demand high standards, and are rightly critical when they let us down. But the reality is that investment in the service has not, and will not, keep pace with the expanding breadth of the task or complexity of the job. So, between the Scylla of public expectation and the Charybdis of limited resources, AI and technological innovation may represent the *only* available vessel that can carry our police through the uncharted waters ahead.

Andy Higgins is the Research Director of the Police Foundation.

Ruth Halkon is a Researcher at the Police Foundation.

REFLECTION 1:

How to operationalise ethical use of policing technology

Giles Herdale

The Cumberland Lodge Police Conference 2024 addressed the challenges and opportunities posed by technology and highlighted the rapidly developing environment both technically and socially. There was broad consensus from participants that policing needs to be better and more agile at harnessing the potential of technology in order to maintain efficiency and effectiveness in the face of highly constrained resources, as well as addressing new challenges such as the growth in generative AI enabling and scaling new criminal threat. Equally, however, it is clear that there is a trust deficit faced by both policing and technology companies, that necessitates considerable care as to how new technology is developed and deployed.

So, the question is: how can policing operationalise ethical use of new and emerging technology? Central

to this is the current absence of a playbook for what this involves. In recent years we have had a succession of high-level statements around the centrality of ethics to policing, from the promulgation and revision of a Code of Ethics by the College of Policing,¹ to a range of commitments in national plans, including the national data and digital strategy.² However, we are yet to see what this looks like at a granular, operational level, consistently applied – as evidenced by the ongoing controversy over the deployment of emerging technologies such as Live Facial Recognition (LFR) by the Metropolitan Police.

1 See: <https://www.college.police.uk/ethics/code-of-ethics>

2 National Policing Digital Strategy 2020-2030 – Police Digital Service (pds.police.uk) See: <https://pds.police.uk/national-policing-digital-strategy-2020/national-policing-digital-strategy-2020-2030/>

It is therefore timely to consider four elements that might be included in future guidance:

- 1. Central register of what is happening.** Such a list of high impact technology deployments doesn't currently exist in UK policing, although an equivalent is mandated in the EU by the new AI Act which addresses deployments of 'high risk' AI systems, including for law enforcement purposes.³ While the UK isn't subject to the Act, the principles will have considerable market influence and could be a useful central point of reference for policing technology deployments. The College of Policing could maintain such a list in the same way as they maintain a research map in policing.
- 2. Focus on who is most affected by policing use cases.** In recent years we have seen challenges to police use of technology, including mobile phone extraction from victims and survivors of sexual violence,⁴ as well as concerns that technology (such as LFR) will exacerbate underlying disproportionate use of police powers.⁵ Such controversies have had a direct impact on public trust and confidence: addressing them will require better engagement with community interest groups. This is not currently commonplace but could be (e.g. joint IAG and data ethics engagement).
- 3. High level principles are necessary but not sufficient.** These need to be followed through into consistent processes and backed up by a commitment to transparency (see above). The increasing commitment to scientific evaluation, such as commissioning the National Physical Laboratory to assess the performance of algorithms used in LFR,⁶ is welcome but not sufficient on its own. As things stand, the guidance that exists is largely reactive (e.g. the College of Policing's Authorised Professional Practice on data extraction⁷ and LFR⁸ appeared only after scandal and legal challenge) and is not aimed at the innovation and procurement stages of early product development and pre-deployment testing. Working with innovation bodies such as Accelerated

Capability Environment⁹ could be a way to build these considerations into early innovation pilots and proof of concept activities.

- 4. Encourage good practice in industry.** The same considerations around the need to democratise oversight and engagement apply, not just in policing, but also in industry. More could be done to require industry to show engagement on these issues as a condition of public procurement. Some suppliers are already doing this (e.g. Trilateral Research with the independent review of Cesium,¹⁰ or Axon with their Ethics and Equity Advisory Council (EEAC) engagement on new product development.¹¹) Working with industry bodies such as techUK could be a way to see such practice become the norm rather than the exception.

There are capabilities within the system both locally and nationally that could support and operationalise such a system (e.g. the pre-existing expert advice and scrutiny offered by bodies such as the Biometrics and Forensics Ethics Group (BFEG)¹² and West Midlands Police ethics committee¹³) but these need to be supported with consistent leadership and prioritisation. Policing has the ability to take a lead on these issues with support from partners in industry, academia and civil society. Such approaches will support the much-needed innovation and adoption of new technologies within policing while bolstering public trust and confidence.

Giles Herdale is an independent expert on digital investigation and has been involved in ethical oversight and review of police technology projects for many years, as a member and co-chair of the Independent Digital Ethics Panel for Policing between 2014-20 and more recently in advising national law enforcement bodies on data ethics. He is an associate fellow of RUSI, a member of BFEG and sits on the Axon EEAC.

3 See: <https://artificialintelligenceact.eu/article/26/>

4 See: <https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/>

5 See: <https://www.bbc.co.uk/news/technology-48222017>

6 See: https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

7 See: <https://assets.college.police.uk/s3fs-public/2020-12/APP-extraction-data-from-personal-devices.pdf>

8 See: <https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition>

9 See: <https://www.gov.uk/government/organisations/accelerated-capability-environment>

10 See: <https://www.gov.uk/ai-assurance-techniques/trilateral-research-ethical-impact-assessment-risk-assessment-transparency-reporting-bias-mitigation-and-co-design-of-ai-used-to-safeguard-children>

11 See: <https://www.axon.com/community-impact/eeac>

12 See: <https://www.gov.uk/government/organisations/biometrics-and-forensics-ethics-group>

13 See: <https://www.westmidlands-pcc.gov.uk/governance/ethics-committee/>

REFLECTION 2:

How the Fourth Industrial Revolution can enhance productivity, public service, and police training: from 'just-in-case' to 'just-in-time' and 'just-for-me' learning

Ellie Pyemont

The rapid deployment of generative AI into police training, learning, and development presents an unparalleled opportunity to enhance productivity, improve service to the public, and support the police in tackling crime. This transformative approach can shift police learning from a static, one-size-fits-all model to a dynamic, personalised system that is timely, efficient, and highly relevant. Insights from this year's Cumberland Lodge Police Conference underscore the importance of embracing these advanced technologies.

1. Efficiency through AI-driven learning

Integrating generative AI into police training is an efficiency aggregator, promising significant improvements in learning outcomes and operational effectiveness. Traditional training methods often follow a 'just-in-case' approach, where officers are inundated with information that may not be immediately applicable. Generative AI, however, enables a shift to 'just-in-time' and 'just-for-me' learning models. This means training can be tailored to individual officers' needs, delivered precisely when needed, and customised to their roles.

AI learning coaches can play a pivotal role in this transformation. These virtual coaches can assess an officer's current knowledge base, identify areas of strength and weakness, and fast-track learning in areas where retention and understanding are already high. This personalised approach keeps officers engaged and accelerates their progress, ensuring they spend time learning what is most relevant to their duties.

Moreover, AI learning systems can adapt to additional needs, such as situational language requirements or specific learning preferences. This adaptability ensures that all officers receive the support they need to excel, regardless of their background or learning style. The result is a more competent and confident police service, better equipped to serve the public and tackle crime

effectively, with the added benefit of cost savings due to increased efficiency.

2. Harnessing publicly accessible learning resources

A significant advantage of using generative AI in police training is leveraging the extensive range of publicly accessible, non-contentious learning materials. Most police learning content falls into this category, making it an ideal candidate for AI-driven enhancement. By utilising these resources, AI can provide targeted, personal learning experiences that drive up knowledge and proficiency in a focused manner.

The benefits extend beyond individual development for every hour an officer spends engaged in AI-driven learning. Enhanced knowledge and skills translate into improved job performance, leading to better service for the community. This aligns with the broader goals discussed at the conference, emphasising the societal benefits of advanced training methods.

3. Building capacity for future challenges

Implementing generative AI in police training also offers strategic advantages in preparing for future challenges. By starting with AI-driven learning initiatives, police forces can build their technological capabilities and gain valuable experience managing AI systems. This foundational knowledge is crucial as they prepare to confront more sophisticated uses of AI by offenders and harm-doers.

Engaging with AI in a controlled, supportive environment allows police forces to 'cut their teeth' on the technology, experimenting and refining their approaches in a sandbox setting. This process frees up time for officers to focus on pressing tasks and builds organisational capacity and resilience. As forces become more adept at using AI for training, they will be better positioned to tackle the more complex challenge of countering AI used for criminal purposes.

The widespread and rapid deployment of generative AI into police training is a non-contentious, efficiency-aggregator that can revolutionise learning and development in the public sector. By shifting from ‘just-in-case’ to ‘just-in-time’ and ‘just-for-me’ learning models, AI can provide personalised, adaptive training that keeps officers engaged and progressing quickly.

4. "Education is not the filling of a pail, but the lighting of a fire."

The benefits of this approach are significant: enhanced productivity, improved service to the public, and a more capable, confident police force ready to tackle crime in the digital age. Embracing generative AI in police training is not just an option but a strategic boon that promises significant returns for police and the communities they serve—after all, as is often attributed

to Yeats, "Education is not the filling of a pail, but the lighting of a fire."

Reflecting on the discussions at Cumberland Lodge, it is evident that we are at a pivotal moment. Just as in Percy Bysshe Shelley's warning (duly noted in the excellent briefing materials), harnessing new technologies thoughtfully is essential to promoting human flourishing. In this Fourth Industrial Revolution, the police and government are responsible for navigating the complexities of technological advancement and ensuring that progress benefits all members of society while maintaining ethical standards and public trust. Learning, skills and training do not just light that fire but provide the roadmap to that flourishing.

Ellie Pyemont is a Consultant at Enlighten Training and Consultancy Ltd

REFLECTION 3:

Who you gonna call?

Professor Louise Westmarland

This year's annual police conference at Cumberland Lodge, focusing on the topic, 'Policing and the Fourth Industrial Revolution', was approached with a degree of scepticism by some delegates. The conference was organised by the Police Foundation, and as usual was bristling with senior police officers, Police and Crime Commissioners (PCCs), academics, and this year, representatives of a number of high-tech commercial companies. One of the main topics of discussion was the growing influence of AI and how these commercial companies can provide new technology that can help the police become more efficient.

The discussions are held under the Chatham House Rule, but I think I can reveal that I was one of the sceptics in the room. I am always worried about any aspect of police information gathering and practice, but the idea of giving some very personal details to a chatbot filled me with extreme trepidation. One of the examples given was that of an experiment where a person is calling the police, hiding in a cupboard, with a disabled child, while listening to their home being ransacked by burglars. I feel that in that situation I'd definitely want to speak to a real live police officer, however efficient a chatbot was shown to be. Another example was the way the details of a burglary could be taken by a chatbot. We were assured that very soon we wouldn't know if we were talking to

a machine or a human being, but the line "please just concentrate on the important details" by the chatbot version, gave it away. If you've been burgled, depending on the circumstances, what is important to you might not seem so to a machine.

Finally, to the ethical issues which are my main concern. If the old claim, in answer to the question 'What are the police for?' is to be answered in the Fourth Industrial Revolution I think we need to be careful about trust, belief in the police as our guardians of peace and civilization, and the people who, as their bottom line, protect us from harm. As others have asked – and I paraphrase – *when-something-is-happening-that-shouldn't-be-happening-and someone-needs-to-do-something-about-it*, who you gonna call? Do you want a chatbot operated by a private tech provider or would you like, as a taxpayer and citizen, to speak to the police and for them to be there when we call? The even older question, 'Who guards the guards?' is another ancient ethical dilemma – just who does guard the chatbot and who will make sure they act in our best public interests, when they become, as the tech companies allege, smarter than humans?

Louise Westmarland is Professor of Criminology at The Open University

REFLECTION 4:

Reflections on the Cumberland Lodge Police Conference 2024

Rt Hon Alun Michael

The excellent Cumberland Lodge Police Conference this year demonstrated the breath-taking complexity of police decision-making.

- It underlined the urgency of harnessing technology for policing and justice.
- It highlighted the scale of threats and opportunities posed by “Artificial Intelligence”.
- And it demonstrated the vital importance of two things that are often undervalued...
 - **Clarity of purpose**
 - **Good governance**

The wise words of Leonardo da Vinci – *“everything is connected to everything else”* – don’t just apply to the environment, but to policing more than most other human activities.

Clarity of purpose starts and ends with Peel’s two key principles. Application of technology will go wrong unless policing has a laser-like focus on its prime purpose – to prevent crime and harm – and remembers that unless *“the Police are the Community, and the Community are the Police”* policing will not be trusted.

As I step down after 12 years as Police and Crime Commissioner (50 years in elected offices) it’s clear to me that ever-increasing complexity in policing can prevent that clarity reaching every nook, cranny and silo of policing. Narrower priorities can distort direction and delivery, and that’s particularly true with technology.

Remember the Panda car? It increased police productivity, getting police quickly to where they were needed. Understandably it led to demand for more cars – faster and better cars – and is seen as the moment Dixon of Dock Green became Barlow from Z Cars.

When officers stop being in the community – and stop listening – the disconnect grows. Unless technology and productivity serve the overall purpose and receive fair but unrelenting scrutiny through good governance, it will be like following the instruction on my daughter-in-law’s coffee mug: *“Drink more coffee – it helps you do stupid things more quickly”*.

Live Facial Recognition (LFR) provides a rich case study. It helps enforcement, justice and prevention. Legitimacy has been tested in the courts. Fairness tested by the National Physical Laboratory. Authorised Professional Practice is spelt out in detail by the College of Policing.

Great, but that doesn’t deliver community confidence. It doesn’t tackle fears or perceptions – however unfair – that the police service is intrinsically oppressive. Neither rules nor statistics alone deliver public confidence. Slogans from opponents of LFR continue to have salience, except where the public *do* trust ‘their’ police. So, sensible developments in police application of technology and AI must not be delivered in isolation. And there’s a need to focus prevention on the big drivers of harm – domestic violence and abuse, drug misuse and the business model that exploits children, online fraud and the dark side of the internet and social media. Here’s Sir Andy Marsh’s challenge to those who met to plan use of the governments’ £10m for a focus on police productivity.

Centre for Police Productivity

The College of Policing is setting up a Centre for Police Productivity (CPP) so that forces can harness the full potential of data-driven technologies to transform the speed and accuracy of policing activities across the board. Getting this right will free up frontline officers and staff to improve delivery of their core mission of engaging with the public to prevent crime and disorder in our communities.

CC Sir Andy Marsh, College of Policing

That clarity must be built into the DNA of policing and the dynamics of the new Centre and embraced by police enthusiasts for technology – not just national strategic leaders.

So, there are two key tests of whether the application of Technology and AI is appropriate and successful:

- Does it improve the efficiency and effectiveness of policing? And....
- Does that lead to more time being spent on the ‘core mission’?

Why? Because it's vital for communities to see the police as 'their' police.

That's why the intervention of Suella Braverman, telling the Met how to police a demonstration, was politically dangerous and constitutionally illiterate, so the firm push-back by the Metropolitan Police Commissioner had enormous significance.

It's why concerns over Orgreave have not gone away in the decades since the Miners' Strike and must be addressed.

The key is in the vital day-to-day work of police, engaging with every local community and above all *listening*.

Much press and political commentary is ill-informed. A recent Lords' report talked about LFR as if the technology is the issue and as if more legislation is what's required. My favourite quote is "*Laws rarely prevent what they forbid*" so it makes sense to focus first on clarity of overall purpose, values and good governance, with legislation where needed, designed to support all three.

Police in oppressive regimes do use technology as an instrument of oppression but not because of a lack of legislation. Many laws in the old Soviet Union set out high democratic ideals but were ignored by those in power.

The drive for 'police productivity', and applying technology and AI to police work, is vital, considering the ruthlessness with which organised and international crime will exploit the very same technology, as they drive fresh pathways to profit and harm. But we are not the same. That's why we require such clarity of purpose, good governance and public confidence.

The Rt Hon. Alun Michael is the former Police and Crime Commissioner for South Wales, the former Vice Chair of the Association of Police and Crime Commissioners and Leader of the Labour Group. He was Deputy Home Secretary and Minister of State for Policing 1997-98 before joining the Cabinet as Secretary of State for Wales.

REFLECTION 5:

Increasing public support for Live Facial Recognition in policing

Michelle Weller

The use of Live Facial Recognition (LFR) technology in policing has generated significant debate and controversy, primarily due to concerns over privacy, data security, and the potential for misuse, at a time when public confidence and trust in policing is low. To increase public support for LFR, we need to address these concerns by positively engaging the public through well-designed interventions. The COM-B model,¹⁴ which focuses on Capability, Opportunity, and Motivation as key drivers of behaviour, provides a robust framework for developing such interventions.

1. Capability

To gain public support for LFR, it is essential to increase the public's understanding and knowledge of the technology. Furthermore, ensuring that the public has direct, hands-on experience with LFR technology can help to demystify it and reduce apprehension. This can be achieved through:

- **Educational campaigns:** Develop comprehensive materials that explain how LFR technology works, its intended benefits, and the protections in place to safeguard privacy. These materials should be disseminated through various media channels, including videos, infographics, articles, and social media platforms, to reach a broad audience.
- **Community workshops/training:** Conduct workshops/training sessions for community leaders, influencers and educators to deepen their understanding of LFR. These sessions should cover the technical aspects of LFR, the ethical considerations, and the legal frameworks governing its use. Empowered with this knowledge, these leaders can act as informed advocates within their communities, helping to dispel myths and misinformation.
- **Public demonstrations:** Organise live demonstrations of LFR technology in action. These events should allow attendees to see first-hand how LFR is deployed, how it processes data, and how

¹⁴ COM-B Model developed by S. Michie, Maartje van Stralen and Robert West (2011)

safeguards are implemented to protect individual privacy. Providing opportunities for the public to ask questions and interact with the technology can help build trust, confidence and transparency.

2. Opportunity

Creating environments and opportunities where the public can access reliable information and engage with the technology is essential to increasing trust and confidence in police usage of LFR. To build a supportive pro-LFR social environment requires collaboration and positive media representation: Key strategies to achieve this may include:

- **Public access to information:** Establish dedicated areas online where the public can access comprehensive information about LFR. This should include detailed reports on its deployment, effectiveness, and oversight mechanisms. Regular updates and easy-to-navigate interfaces will encourage public engagement and trust.
- **Community events:** Host regular community events such as town hall meetings, open forums, and Q&A sessions where the public can engage directly with the police, technology experts and policymakers. These events should facilitate open dialogue, allowing the public to voice their concerns ensuring they feel informed and involved.
- **Stakeholder collaboration:** Engage with a broad spectrum of stakeholders, including community leaders, civil liberties organisations, privacy advocates, and the public. Collaborative efforts can help develop balanced policies that address both security needs and civil liberties, fostering a sense of shared purpose and mutual understanding.
- **Positive media campaigns:** Work with the media to ensure balanced and accurate coverage of LFR. Highlighting success stories where LFR has positively impacted public safety can help shift public perception. Media partnerships should focus on presenting both the benefits and the safeguards of LFR, ensuring a nuanced and informed discourse.

3. Motivation

Increasing public motivation/desire to support LFR usage involves addressing the public's rational concerns and demonstrating the responsible use of LFR. Positive reinforcement and addressing emotional concerns can also further enhance public support. This can be accomplished by:

- **Transparency and accountability:** Implement clear policies and procedures for the use of LFR, emphasising transparency and accountability. This includes regular publication of reports, detailing the use of LFR, its successes/failures, and any instances of misuse. Establishing independent oversight bodies to review and audit LFR usage can further build public trust.
- **Evidence of effectiveness:** Regularly publish independent evaluations and audits that demonstrate the effectiveness and fairness of LFR technology. Sharing data on how LFR has helped solve crimes, locate missing persons, or prevent incidents can provide tangible evidence of its benefits.
- **Positive reinforcement:** Recognise and celebrate instances where LFR has significantly contributed to public safety. Public acknowledgments, awards, and positive media stories can create a favourable perception of the technology. Personal testimonials from individuals who have directly benefited from LFR can be particularly impactful.
- **Addressing fears and misconceptions:** Use targeted messaging to address common fears and misconceptions about LFR. Clear, factual communication that debunks myths and provides reassurance about data security and privacy protections can help alleviate public anxiety. Public commitments to ethical standards and the protection of civil liberties can help mitigate fears and build trust.

4. Conclusion

If policing wishes to gain public support and acceptance of its use of LFR technology, it needs interventions that engage the public, rather than relying on merely 'telling' the public about its usage. Using behavioural frameworks such as the COM-B model can help with this, providing a structured approach to designing interventions that aim to influence behaviour – in this case, public support for the use of LFR technology. By enhancing capability, creating supportive opportunities, and positively influencing motivation, the police can foster behaviours that lead to public acceptance of LFR.

Michelle Weller is an independent business change expert who specialises in culture and behaviour change. She works with police organisations to drive, deliver and embed change.

REFLECTION 6:

How to do AI accountability – and why it’s worth the effort

Professor Babak Akhgar OBE and Professor Petra Saskia Bayerl

Accountability is at the core of AI discussions and frameworks, including the National Police Chiefs’ Council AI Covenant,¹⁵ the UK’s National AI Strategy, as well as international efforts such as the EU high-level expert group and the ongoing G7 Hiroshima Process. More generally, accountability is at the core of policing – or as Markham and Punch succinctly phrased it “*policing is accountability*”.¹⁶

As discussions during the conference have shown, the public is not generally against AI use by the police. However, the public is against AI use by the police if its purpose is opaque, if it leads to negative consequences and if they have the impression that mistakes and misuses are not dealt with appropriately, or at all. Our own public citizen consultation¹⁷ demonstrates that citizens expect accountability for AI use by the police:

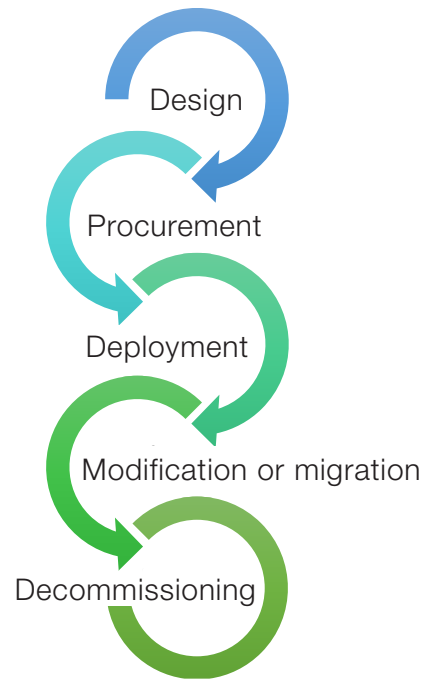
- 88 per cent of respondents want the police to be held fully accountable for the consequence of their AI use, and
- 90 per cent of respondents want the police to be held fully accountable for the manner in which they use AI.

This makes accountability a vital concern for responsible AI use.

1. The scope of AI accountability

Accountability, in its simplest form, is the “*acknowledgement and assumption of responsibility for actions, decisions, and their consequences*”.¹⁸ In the context of AI, this refers to the acknowledgement that a police force has to act in accordance with legitimate expectations of its stakeholders and accept the consequences – legal or otherwise – if it fails to do so. We argue that this responsibility extends across the full

AI Accountability across the AI Lifecycle



AI lifecycle, that is, not only during design, procurement, and deployment but also during system modifications, migrations and decommissioning. It also extends to outcomes and impacts across the plurality of involved and affected stakeholder groups.¹⁹

2. A hands-on approach to AI accountability

To make AI accountability actionable and useful police forces – and their stakeholders – need to be able to assess and evidence it. That is, it needs a practical, hands-on approach. We are currently developing an online tool for police forces that allows them to assess and evidence AI accountability for concrete AI capabilities and usage situations.

The assessment is based on 12 principles which, taken together, establish AI accountability.²⁰ Each of the 12 principles is further operationalised into a small number of questions. One question, for instance, which seeks

15 See: <https://science.police.uk/delivery/resources/covenant-for-using-artificial-intelligence-ai-in-policing>

16 See: https://www.researchgate.net/publication/31226598_Embracing_Accountability_The_Way_Forward_Part_One

17 See: https://www.ap4ai.eu/sites/default/files/2023-10/AP4AI_International-Citizen-Consultation_October2023%28online-version%29.pdf

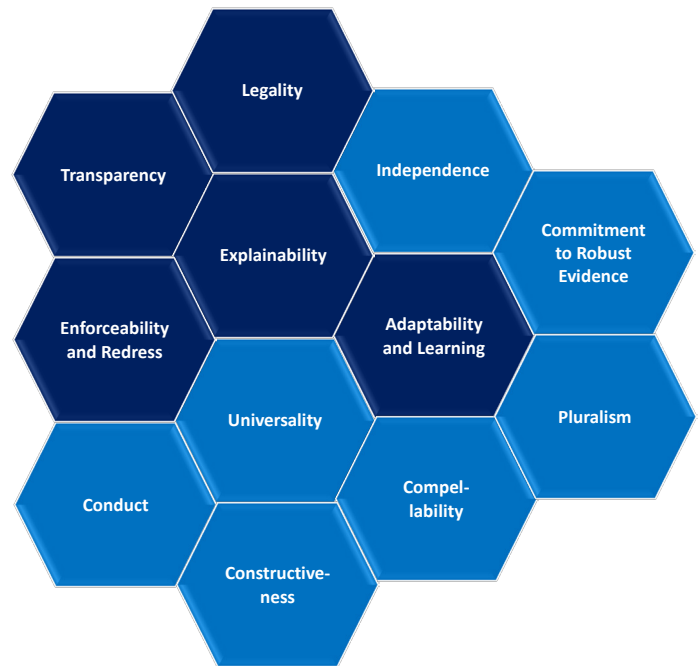
18 See: <https://ssrn.com/abstract=3087771>

19 See: <https://www.ap4ai.eu/reports/2022/02/ap4ai-framework-blueprint>

20 See: <https://www.ap4ai.eu/reports/2022/01/summary-report-expert-consultations>

AI Accountability Principles

1. **Legality:** AI use is entirely in line with the law
2. **Transparency:** all information to assess AI use and to enforce consequences is easily and fully accessible to groups that judge police use of AI
3. **Explainability:** all AI practices, systems and decisions can be fully explained to the public and oversight bodies
4. **Enforceability and Redress:** it is possible to compel police to comply with all requests to improve their AI practices
5. **Adaptability and Learning:** police are continually willing to change their current AI practices based on new knowledge and insights
6. **Independence:** the people and groups that monitor police and enforce consequences are totally independent from police and organisations that design AI systems
7. **Universality:** every aspect of AI use without exception can be monitored and assessed
8. **Pluralism:** every group involved in and affected by AI use, without exception, has a voice in monitoring and assessing police use of AI
9. **Commitment to Robust Evidence:** police are committed to providing evidence that is so robust that their AI use can be judged with confidence
10. **Constructiveness:** police and groups that assess police use of AI always have a constructive attitude in their negotiations with each other
11. **Compellability:** it is possible to compel police to provide access to all necessary information, systems or individuals to judge their use of AI
12. **Conduct:** all police uses of AI strictly follow professional standards



See: <https://www.ap4ai.eu/reports/2022/01/summary-report-expert-consultations>.

to capture the *Enforceability and Redress* principle, requests information on whether “*measures are in place for affected stakeholders to complain/request redress*”.

The tool collects information on whether components of the AI accountability principle have been completely or partially completed or have not been fulfilled at all. Conducting the assessment thus provides a comprehensive view about how far AI accountability has been achieved and provides concrete recommendations on how and where procedures, infrastructures and resourcing could be improved. Importantly, our approach encompasses **proactive and reactive** accountability,²¹ i.e., it improves forces’ ability to prevent negative events, be aware of and manage known risks, and react to negative events more effectively.

3. Why it's worth the effort

AI accountability seems an abstract concept. However, done well, AI accountability is in fact a very practical instrument: It helps to think through the **why, what, how, who** and **for whom** of AI deployments, and it does so proactively. It supports police forces to:

- Understand risks and strengths before each AI procurement, deployment or change.

- Know up-front what to do if something goes wrong.
- Understand which areas of accountability are achieved or need addressing.
- Have evidence ready, in case they get challenged and have to prove adequate AI procedures.

Having gone through the AI accountability process, police forces thus have evidence of their infrastructures, resources, risks, decisions, etc., as well as clear, agreed procedures for how to react to and redress actual failures.

We do not claim that assessing and evidencing AI accountability is a quick and easy process: it takes time, commitment and resources to understand, establish and evidence. However, we argue that it is worth investing in an AI accountability process, as it gives the opportunity to ensure that adequate practices and infrastructures are set up, before things go wrong (i.e., aiming to prevent failures) and to support appropriate reactions if they do.

Babak Akhgar OBE is Professor of Informatics and Director of CENTRIC at Sheffield Hallam University.

Petra Saskia Bayerl is Professor for Digital Communication and Security and Head of Research at CENTRIC.

²¹ See: <https://doi.org/10.1007/s00146-023-01635-y>

Policing and the Fourth Industrial Revolution

Ruth Halkon

Writing in 1821, at the height of the first industrial revolution, the poet Percy Bysshe Shelley warns about the danger of relentlessly pursuing progress without properly considering how modern technologies might be best harnessed to promote human flourishing. He argues this failure to anticipate change has meant that technological progress has been left in the hands of self-interested technocrats who are using it for their material gain, such that: “the rich have become richer, and the poor have become poorer.” State actors who should have intervened to ensure everyone benefited, have instead been slow to react, reduced to steering the country on an uncertain course between two equally unpleasant outcomes: “the Scylla and Charybdis of anarchy and despotism” – when had they taken anticipatory action, they could have avoided both extremes entirely¹ Shelley, 2006).

Two hundred years later, we are facing a similar moment of flux and change and there is a similar necessity for legislators to understand and shape the development of new technologies before they themselves are controlled. The First Industrial Revolution used water and steam power to mechanise production, the Second used electric power to create mass production and the Third used electronics and information technology to automate it. Now, experts such as the World Economic Forum chair Klaus Schwab are hailing the current age as a Fourth Industrial Revolution (Schwab, 2016). As Carl Miller writes in the *Death of the Gods*, the fusion of technologies such as artificial intelligence, biotechnology, advanced robotics and the Internet of Things (IoT) means we are “hurtling into a new social reality.” It is hard to see whether this future will be “a new dawn of knowledge and opportunity, or a nightmare of ignorance and oppression” (Miller, 2019, p.xv). Modern technologies are already bringing about long-term gains in efficiency and productivity, which is driving economic growth, and “lowering the costs associated with human thinking and reasoning” (Dell’Acqua, et al.,

2023, p.23). However, as well as new opportunities for businesses, digital technologies are bringing new prospects for crime that does not respect geographical borders and therefore threatens the rule of law (Muir, 2016). Moreover, although the technologies are very different, the risks of entering a “winner takes all economy” where the “rich get richer and the poor get poorer” are as stark as during early 19th century – with those owning the technologies getting richer, while low-skilled workers find themselves again displaced by machines (Schwab, 2016; Brynjolfsson and McAfee, 2014). This growing inequality risks bringing with it not only discontent, but a potential rise in social tension and violent crime (The Police Foundation, 2020).

As with Shelley two centuries ago, writers are returning to the idea of the Greek myths to make sense of the current turmoil. Floridi and Taddeo (2016) return to the myth of Scylla and Charybdis to describe the challenge of “fostering the development and applications of data science while ensuring the respect of human rights and of the values shaping open, pluralistic and tolerant information societies” in order to reach solutions that maximise the ethical value of data science to benefit our societies. The government, and the police, must steer “between the Scylla of social rejection” in which people reject data science because of ethical concerns and fears over threats to privacy and individual liberty; and the “Charybdis of legal prohibition,” in which individuals are overprotected with rigid regulations that cripple innovation. Unlike in *The Odyssey* and Shelley’s interpretation of the myth however, for Floridi and Taddeo (2016) there is a safe course, and it is the role of the police and government to steer us through. This briefing will explore just how our society is changing as part of this Fourth Industrial Revolution and what the implications are for policing and its relations with the public it serves.

¹ In Homer’s *Odyssey*, Odysseus chose to risk having a few sailors picked off by the sea monster Scylla rather steering too close to the whirlpool Charybdis which would swallow the ship whole. But Jason, in Jason and the Argonauts, were able to avoid both dangers because of an expert guide. And in the *Aeneid*, Aeneas seeks advice beforehand and avoids them entirely.

1. What is AI?

Speaking at last year's global AI Safety Summit, hosted by the British government at Bletchley Park, Prime Minister Rishi Sunak said that the "world stands at the inflection point of a generational technological revolution" as greater access to better chips and more computing power have led to unprecedented developments in the space of artificial intelligence. Attendees at the summit agreed these developments bring "unprecedented opportunities" but also risks, such as generative AI spreading false narratives which might, for example, threaten electoral processes, the risk of AI being misused by criminals, and the prospects of increasing inequality and the amplification of biases and discrimination (UK Government, 2023).

So, what is AI? To answer this question, I asked ChatGPT, a chatbot released by Open AI and based on large language models. Its answer:

"Artificial Intelligence, often abbreviated as AI, refers to the simulation of human intelligence processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction. AI encompasses various subfields, including machine learning, natural language processing, computer vision, robotics, and more. The goal of AI is to create systems that can perform tasks that typically require human intelligence, such as understanding natural language, recognizing patterns, making decisions, and learning from experience." (Open AI, 2024).

There is currently no standardised, universally agreed definition of AI. This is partly due to the difficulty in defining the abstract and subjective concept of human intelligence (Kaplan, 2016). Most definitions of AI relate to computers or machines that can perform tasks that require intelligence (Samoili et al., 2020).

AI is the overarching concept while machine learning, deep learning and neural networks are subsets:

- Machine learning involves algorithms that learn from experience and improve their decision-making or predictive operations over time. It can be supervised (trained by a person using clear, well labelled data so that the input data is paired with the desired output) or unsupervised (the machine receives no training and discovers relationships, patterns, and processes in unlabelled and uncategorised data with no predefined output).

- Deep learning is a subset of machine learning which uses a complex layered structure of algorithms or 'artificial neural networks' to analyse data. Examples of deep learning applications include computer vision (e.g., self-driving cars and facial recognition); automatic speech recognition such as virtual assistants; chatbots for customer queries, feedback and complaints; translation (e.g., language and images to text), 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.

The birth of modern-day AI dates to the 1950s following Alan Turing's milestone paper *Computing machinery and intelligence* (1950) which explored whether computers could think. The term 'artificial intelligence' was coined by John McCarthy in 1955 and from then until the 1980s advancements in AI faced several setbacks and successes and faded in and out of public consciousness. Advances in the 1990s and early 2000s, including IBM's 'Deep blue' AI decision making programme defeating world chess champion Gary Kasparov, heralded rapid growth in the use of AI for advertising, user experience algorithms, and virtual assistants. Recent developments to hit the headlines include generative AI i.e., systems and algorithms that create new content or data such as text generation (e.g., GPT-4o) and image generation (e.g., DALL-E2).

Recent research from Harvard University highlights the huge productivity benefits that AI can bring to the workplace, but also the dangers of relying too heavily on it without proper checks and balances. Dell'Acqua and others (2023) carried out randomised controlled field experiments with highly skilled professional workers. The researchers suggested AI created a "jagged technological frontier" where some tasks, such as fast idea generation, writing, persuasion, strategic analysis and creative product innovation, are easily done by AI and boost efficiency and productivity significantly, while other seemingly similar tasks, are outside the current capability of AI. The article draws out a number of risks from overreliance on the technology:

- Wrong answers might not be recognised as wrong by the humans who blindly follow them.
- Mass AI usage might lead to diminished diversity of ideas.
- The black box' problem of AI – humans can struggle to discern how algorithmic predictions are generated

as it is difficult for them to discern how and which connections between data points are made (Waardenburg and Huysman, 2022).

All of these factors can prove problematic for an organisation like the police, who might use it to aid in making decisions that would affect the lives of individuals and communities.

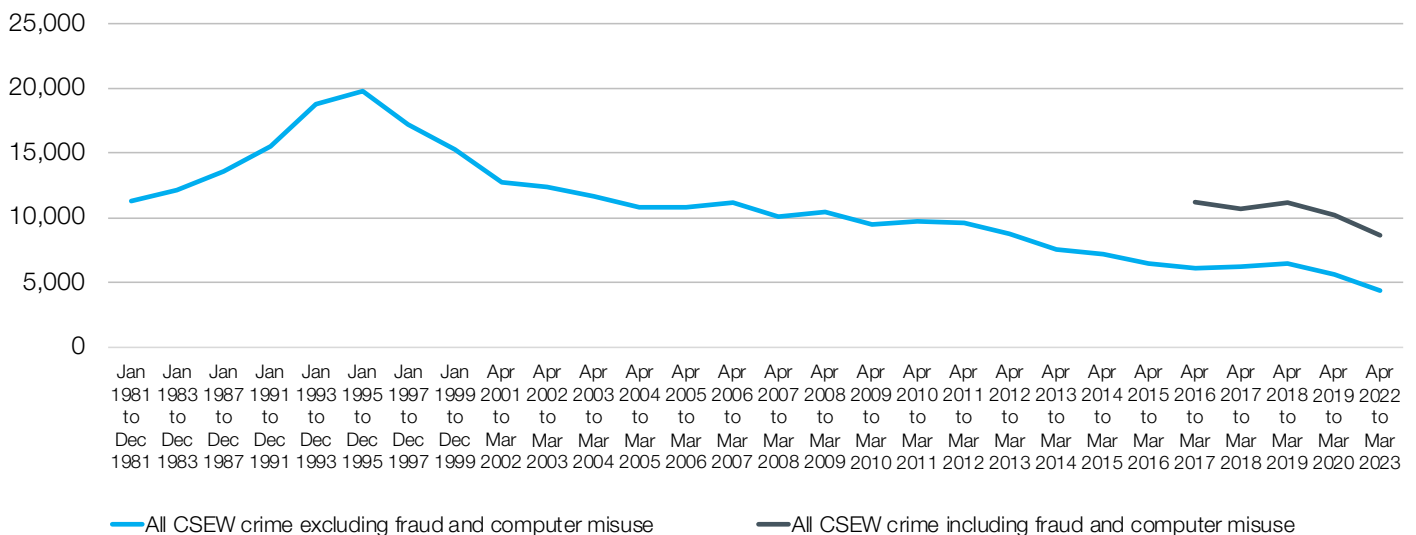
2. Cybercrime

In 2015 figures from the Crime Survey of England in Wales seemed to suggest that crime was at its lowest since records began in 1981, leading the then Home Secretary Theresa May to announce that “families are safer and more secure”. However, the year after, the Office for National Statistics, which delivers the crime

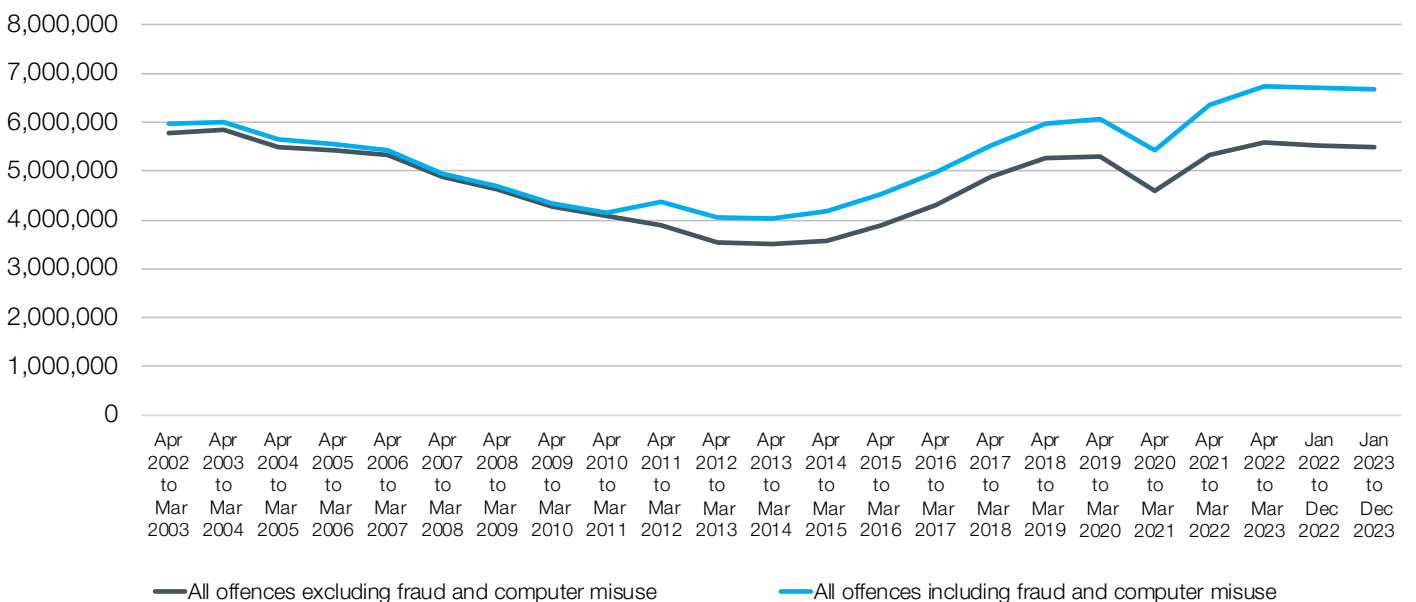
survey, added two new questions on fraud, much of which is cyber-enabled or cyber-dependent, and computer misuse, which covers unauthorised access to computer systems and data. And suddenly crime rates boomed. These two questions “had unearthed around as much crime as all the others combined [...] crime had not really been falling at all; it had been migrating” (Miller, 2019, pp 35-6). There may have been long term reductions in violent crime and theft among other things, but this did not mean that people had turned away from crime. Instead, crime had moved from the streets to behind closed doors, where traditional policing models struggle to penetrate – meaning that “too often those committing fraud and cybercrime believe that they can act with impunity” (The Police Foundation 2022).

Figure 1 Crime rates before and after the inclusion of fraud and cyber crime

Crime Survey of England and Wales – trends in fraud and computer misuse



Recorded crime including and excluding fraud and computer misuse



Cyber offences are committed when someone commits a crime using a computer or other digital technology. There are two main types of cyber offences – cyber-enabled crime and cyber-dependent crime. Cyber-enabled crime is where technology has been used to enhance another crime, like fraud, while cyber-dependent crimes are offences that can only be committed through the use of technology. Some of these technologies are being exploited by existing criminals, such as organised crime groups who are taking advantage of new technologies such as the dark web, virtual currencies and end to end encryption to expand existing drug trading networks (NCA, 2019, 2020; The Police Foundation, 2022).

But there is evidence to show that new types of criminals who might have previously been discouraged by the effort and skill involved, the fear of being caught or reluctance to confront their victims, are being tempted by the opportunities these technologies bring. User friendly computer programmes, easily accessible on the dark web, mean committing cybercrime hardly needs any skill, knowledge, or time. For a little bit of money, criminals can download everything they might need to commit a ransomware attack – which seizes control of victims’ devices until a fee is paid (Miller, 2019). These attacks are also increasingly targeting organisations such as schools and hospitals, which often lack the resources to combat them. Recent figures from the Information Commissioner’s Office (ICO) show a 55 per cent increase in the number of cyber incidents reported by educational establishments between 2022-23 (Standley, 2024). Government data suggests most schools and colleges have identified a cyber-security breach in the past year, and secondary schools and higher educational establishments are more likely to be targeted than the average business (Ell, 2024). The volume and the sheer difficulty of investigating these complex crimes challenges police capability to determine and prioritise which cases they should pursue. It also puts pressure on them to better collaborate across borders to combat criminals who are already using the internet to break down the “traditional criminal investigation triangle of local victim, local offender and local police” (Muir, 2016).

AI and crime

A lot of the debate around AI and crime centres around hypothetical or long-term risks like creation of synthetic viruses, cyber-attacks or, at the extreme, the risks in creating a ‘superintelligence,’ or postulated artificial

general intelligence (AGI) (IWF, 2023). But AI is being used to commit crime in the here and now – and regulators, police and the security services are slow to realise the risks posed by these new technologies, or to ensure manufacturers put safeguards in place to limit their use for crime (*Today*, 2024). Easy-to-use interfaces to large-scale artificial intelligence (AI) models “have enabled an explosion” in ‘synthetic’ content, from sophisticated voice cloning to deepfake imagery – leading the World Economic Forum’s [Global Risks Report 2024](#) to rank misinformation and disinformation as the number one threat the world faces in the next two years (WEF, 2024). Deepfakes are content created using AI which can be used to impersonate real people and can be so lifelike, only a computer can detect they are not the real thing (Torkington, 2024). For example, Open AI announced [GPT-4o](#) in May 2024, its most ‘emotive’ model yet, which communicates via speech rather than text. It could be used to improve translation between languages, but has huge criminogenic potential, such as being used to defraud victims by imitating relatives and friends (Today Programme, 2024).

The potential implications of deepfakes for public trust are profound. They can be used for art or education, but when they are used to misrepresent politicians, civic leaders and heads of industry, deepfakes can erode people’s faith in government, media, justice systems and private institutions, potentially leading to civil unrest. Brown et al. (2024) argue that while conventional devices such as laptops and phones already give abusers a powerful reach, various “smart,” smart’, internet-connected devices – such as home assistants, security cameras, lights, doorbells, and locks – have increased the damage they can do significantly. Their study identified a number of design features which can be exploited by perpetrators seeking to control victims and reduce their agency. The researchers suggested that while abusers had quickly identified the criminological potential of the IoT, “manufacturers and government authorities” had not seen the threat and so had failed to build in the “safety-by design” features that could have prevented abuse occurring (Brown et al., 2024).

Similarly, before the rise of the internet, the availability of child sexual abuse material (CSAM) was limited to all but the most committed offenders, (The Police Foundation, 2022). Now perpetrators are beginning to use generative AI to create indecent images of children (including existing victims, famous children and those known to them). The technology enables perpetrators, with very

basic skills, to legally download everything they need to generate CSAM, and then create the images offline, lowering the threat of detection still further (IWF, 2023).

The problem, as Dame Hall (2023) states, is there is nothing stopping companies from releasing new technology without telling us how safe it is; there is no guidance on how it is tested, what information is being fed into the models and there are no organisations to hold companies to account (Today Programme, 2024). Regulators are catching up, but they have a long way to go, and it is often hard to strike the right balance. There is a risk that some governments will act too slowly, facing a trade-off between preventing misinformation and protecting free speech, or other governments will use enhanced regulatory control as an excuse to erode human rights (WEF, 2024). Currently the United Nations is working on a high-level advisory body on AI, which will bring together diverse voices to “strengthen stakeholder cooperation on governing AI in the face of pressing technical breakthroughs, and thereby contribute to better-governed AI globally.” However, such bodies could take years to bring about real change (UN, 2023).

Box 1: AI Legislation

The UK [Online Safety Act \(2023\)](#) - bans sharing sexually explicit images or videos that have been digitally manipulated where they have intentionally or recklessly caused distress to an individual.

[Criminal Justice Bill 2023-24](#) will criminalise the creation of deepfake sexual images.

In the EU, the world's first comprehensive AI law, the [AI Act](#), will establish obligations for providers and users depending on the level of risk from AI.

3. AI and policing

Policing has always been an information business, but the digital revolution has greatly increased the quantity of data available to police agencies (Rowe and Muir, 2021). Criminals are realising the potential of digital technologies to perpetrate crime on an industrial scale and the police are using the same technologies to combat them. But as Muir (2016) writes, the police use of digital technologies generates pressing ethical questions, including under what conditions police should be accessing and storing our personal data, what should police do about big data that can help predict when bad things may occur, and how can we ensure decision making is transparent when the algorithms governing it often are not (Muir, 2016).

There is potential for AI and robotics to lead to a radical shift in how the police function and investigate crime. In November 2023, National Police Chiefs' Council (NPCC) Chair Gavin Stephens promised a “quantum leap” in policing's use of new technology – including futuristic drones, facial recognition, and new digital forensics (Sweetland, 2024). This quantum leap may not yet have happened, but already there are “tremendous opportunities to automate manual administrative tasks that take officers and staff away from vital work to protect the public, investigate effectively, and catch criminals” (Sweetland, 2024). Already, in some forces, such as Essex Police, data analytics are open to anyone who wants to understand their jobs better, something which the Chief Scientific Officer Paul Taylor calls “democratising the science” (Say, 2023).

The NPCC has stated that all police forces use data analytics and at least one third use advanced data analytics (NPCC, 2021). According to the NPCC, most applications are used for organisational effectiveness and workforce planning (e.g., triage of 999/111 calls and automation of data administrative tasks (NPCC, 2023). For example, many forces are using robotic process automation (RPA) to free-up officers' time by doing tasks which need no “human intervention, cognitive thinking, or any person to add value to it” (Sweetland, 2024). RPA is not machine learning or artificial intelligence, merely recording what a human does on a keyboard and replicates it repeatedly, yet it lays the groundwork for transformative technologies such as AI and machine learning by ensuring they are based on data that is “good, accurate and complete” (Sweetland, 2024).

There are also instances where AI is supporting decision making. For example, Avon and Somerset Police uses

supervised machine learning to assess factors such as whether someone might re-offend, which offence they might commit, or whether an individual is vulnerable to victimisation. Through an app on their mobile devices, neighbourhood officers can instantly access the risk profiles for each offender registered in the force area, which are recalculated daily (NPCC, 2023).

Some forces have highlighted how such tools are enhancing efficiency, reducing chances of human error, and freeing up time to focus on their core responsibilities, as Box 2 shows:

Box 2: How some forces are using AI

Avon and Somerset Police – automates processes across crime (freeing up frontline officer time), vetting (reducing the backlog), data quality and corporate services (improving users' experience). In total, the force automated 44 processes across 4.1 million cases, freeing up 200,000 hours of police time.

Bedfordshire Police – uses DocDefender to auto redact documents (e.g., personal data) before sending them to the Crown Prosecution Service. Approximately 770,000 hours are used to manually redact data by officers and police staff whereas the use of digital redaction tools could free up at least 618,000 hours of staff time.

Kent Police – Evidence-Based Investigative Tool (EBIT) predicts the probability score of a crime's solvability, which enables the police to prioritise cases based on resource and capacity.

Lancashire Constabulary – Uses RPA to enhance data quality and remove duplicate/triplicate records that were creating an ever-increasing risk to the force. It processed 34 years of manual data cleansing in nine months, generating £2 million savings following a £864,000 investment (Pughley, 2023; McFadzien et al., 2020).

It has been argued that the current use of data science in policing is not replacing officers, but rather is freeing them up for the frontline, as they will still be needed to provide oversight (Dechesne, 2019). Yet there are fears around whether the police workforce is ready, able and being supported well enough to take on the challenge, or even whether we need a new police workforce with different skills entirely to meet the challenges of the future (Kearns and Muir, 2019).

Policing controversy

What happens when the data is not “good, accurate and complete” has been shown in the controversy over predictive policing techniques, which use algorithms and machine learning to predict who might commit or be subject to crime and where crime might occur. Predictive policing, which had its origins in the US, has the potential to reduce the social harm associated with crime – which often weighs more heavily on those already experiencing marginalisation and relative deprivation (Rowe and Muir, 2021). Recognising patterns in domestic abuse, for example, might allow for better risk profiling and early intervention.

Yet there are concerns that the same technology may be unable to take all relevant information into account and has potential for “baking in disproportionality and discrimination” (Hobson et al., 2023). Harcourt (2006) argued that in predictive policing, a ‘ratchet effect’ occurred whereby the over-representation of some groups in police practice leads, through actuarial methods, to a spiral of increasing control and disproportionate police attention in ways that do not reflect crime patterns in society. For instance, the human rights organisation Liberty (2019) argues mapping programs direct officers to already over-policed areas, while individual risk assessment programs encourage an approach to policing based on discriminatory profiling. 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' risk of offending in the next two years. It ceased use of the tool after flaws were highlighted such as deliberate over-estimation of the likelihood of re-offending and discrimination in the data such as basing prediction on personal characteristics including age, gender and postcode (see Fair Trials, 2022; Couchman, 2019).

Similarly, the use of facial recognition by police is increasing, despite questions being raised by academics, charities and civil liberties organisations about its lack of legal basis and potential risk to human rights (e.g., right to privacy and freedom from discrimination) (Purshouse and Campbell, 2021). There are also questions over its accuracy and bias. An evaluation of over 189 commercially available facial recognition algorithms showed that accuracy and performance can vary depending on the targets (age, ethnicity, and gender) and the geographical location in which the algorithm was developed (Grother, Ngan and Hanaoka, 2019). Outcomes like this arise because

police data is not an objective reflection of crime and harm in society, since many crimes are not reported to the police and many incidents logged on police systems reflect police decisions to prioritise certain types of crime and particular geographic areas (Rowe and Muir, 2021). But proponents claim the tool is improving rapidly, and can bring huge benefits to policing, with retrospective facial recognition, for example, enabling police to rapidly identify and arrest suspects from CCTV (Home Office, 2023). A recent report from the National Physical Laboratory (2023) suggested trials of operator initiated facial recognition which uses AI to enable officers to photograph a person of interest to verify their identity, was accurate all the time (Mansfield, 2023).

It has been argued that rather than entrenching police bias, some AI technologies can be used to reveal it. For example, body-worn cameras (BWC) are used to record police encounters with the public, as a means of enhancing transparency, accountability and evidence collection in policing. But there are numerous barriers to their effective use such as the volume and complexity of the data they generate and the human labour required to store, manage and review it effectively (see Higgins and Halkon, 2023). It has been posited that AI can be used to extract, classify, and summarise the relevant information from the BWC footage, using a combination of natural language processing (NLP), computer vision (CV), and machine learning (ML) techniques. This information then could be shared with the public with a view to improving public confidence and trust (Lukens, 2024).

AI and police legitimacy

The Metropolitan Police has argued that: “to declare technologies as being ‘off limits’ to policing risks denying law enforcement the tools it needs to keep the public safe whilst leaving these tools easily available for criminals and commercial users to consume and exploit” (Metropolitan Police Service, 2021). Yet public safety is not solely achieved by disrupting criminals, but by ensuring that the police act legitimately and the public feel the institutions that govern them are legitimate. Procedural justice theory has shown that treating people with fairness and respect can enhance police legitimacy and promote compliance with the law (The Police Foundation, 2022). Recent evidence demonstrates that public trust and legitimacy in the police are important predictors for accepting the police use of modern technologies such as live facial recognition (Bradford et al., 2020), and increasing transparency around

the use of facial recognition and education around misinformation can increase support for its use by the police (Bragias et al., 2021).

Yet many of the new technologies and practices have been implemented without significant public consultation and debate (Bradford et al., 2020). Research into the public’s understanding and awareness of AI is limited and conflicting. Some surveys have reported that the majority of respondents have heard of AI, but only around half can explain what it actually does (Cave et al., 2019; Dupont et al., 2023). Where the public are aware of AI, a recent survey showed that they are generally in favour of it if it is used for routine tasks. Within healthcare, for instance, it is thought that algorithmic tools can perform with expert-level accuracy, deliver cost-effective healthcare, and often outperform human actors (Longoni et al., 2019). Yet while respondents believed it could do a good job in diagnosing a condition, they preferred a doctor, fearing AI would not deal with the patient in a sympathetic, caring way. Moreover, they were opposed to AI being used to decide or to advise when it came to detecting guilt and objected to being forced to use it against their will (Dupont et al., 2023). While people perceive police officer decision making as fairer and more appropriate than algorithmic decision making, being exposed to successful algorithm decision making can increase trust in the decision made and police use of algorithms (Hobson et al., 2023). However, Hobson et al. (2023) found this increased trust is not based solely on the algorithm bringing about a successful outcome, but rather the victim’s belief that the successful outcome came about because the police were “more trustworthy and fair” in their decision. Conversely a lack of consultation and transparency around the use of new technologies may damage the public’s trust in law enforcement (Hobson et al., 2023). By contrast, only a quarter of those surveyed by Dupont and others (2023) seemed concerned about the privacy implications of an AI having information about a people’s symptoms in relation to healthcare. It has been observed, that social attitudes to privacy are changing and people no longer expect to have the kind of privacy enjoyed in pre-digital times: “social attitudes towards privacy are changing dramatically with the younger generation willing to disclose an abundance of personal, sensitive information online” (Rabinovich-Einy and Katsh, 2014, pp 64–65). A recent study of public attitudes towards privacy and police use of AI using Q sort methodology suggests that the issue of privacy vs safety is nuanced. It identified

five perspectives, ranging from complete rejection of police use of AI over privacy concerns to a safety-first approach which acknowledged a moral obligation to another's safety over one's own privacy – and found most participants lay between the two extremes (Ezzeddine, et al., 2023). Most individuals did not perceive AI use by police as an either/or scenario but offered differentiated arguments and contextualisation hinting towards situational, demographic, cultural and political factors (Ezzeddine, et al., 2023).

Yet while there has been a small amount of work identifying and publishing the current use of AI and data driven approaches by the police within the UK (e.g., Liberty 2019), there is a significant lack of information and transparency around the availability of the tools, their use and how they are implemented in practice (Zilka et al., 2022). The main problem with big data is its lack of transparency. 'Machine policing' is a fast-developing area which is often opaque and technologically complex (Rowe and Muir, 2021). The software and technology that constitute algorithms tends to be created and owned by private IT companies who might be resistant – on commercial grounds – to external analysis of the coding. Moreover, as Miller (2019) writes, often machine learning means that the decisions generated by algorithms are opaque even to those who have designed them.

Ferguson (2017) found that legislators are unable to penetrate the working of algorithms and the fast-paced development of technology risks making legislation and post hoc legal challenges redundant. All of this makes the question of holding police use of such systems to account a hard one to solve and emphasises the importance of involving the public in the debate around the use of AI and automation in policing. Yet Wells et al. (2023) argue that such public involvement is not happening in the way it should. Wells and colleagues argue the move towards automation and the Single Online Home, which boosts efficiency since people can report crimes without ever speaking to a police officer, may have risked undermining the legitimacy with which policing is provided. Although technologically mediated contacts may still offer procedural justice, there is little evidence that the police have consulted those being affected by the changes. (Wells et al., 2023).

4. Conclusion

The *National Police Chiefs' Council Covenant for Using Artificial Intelligence (AI) in Policing* was agreed in 2023 by all 43 forces in a bid to ensure a "proportionate and responsible use that builds public confidence" (NPCC, 2023). These principles are designed to limit potential damage to civil liberties by ensuring that all use of AI is: "lawful, transparent, explainable, responsible, accountable and robust." While implementing these principles may be "ongoing and evolving" the NPCC hopes through publishing them, to show they are attempting to be transparent from the start (NPCC, 2023).

Many scholars have suggested the need to open up the 'black box' of AI and provide transparency around justifications of use (Licht and Licht, 2020). It is important for us to acknowledge the "complexities and uncertainties brought by novel technologies" in modern-day policing" and to ensure the public are aware of them (Fussey and Sandhu 2022, p.11). The answer then is not to ban these technologies entirely but for governments to develop and implement laws regulating police use of them which consider privacy and victim rights issues and mandate rigorous testing of algorithms – an approach which has public support (Thompson, 2024; Dupont et al, 2023).

Shortly after Shelley made his plea for imagination to take its place in legislation, Sir Robert Peel argued for the foundation of the Metropolitan Police and a "new mode of protection" which uses the trust, confidence and cooperation of the public rather than the exercise of power to keep the peace (The Police Foundation, 2022). Two hundred years later there is a need to think again about how policing can be properly carried out in a world of radical technological change (Muir, 2016). It is worth remembering that AI is designed to achieve the objectives we set it. As Professor Stuart Russell (2021) warned in his 2021 Reith Lecture, any tasks we set it must be carefully defined within a framework that benefits humanity. Otherwise, as in *The Sorcerer's Apprentice*, the command to fetch water can result in an unstoppable flood. This conference will examine what those principles might look like and how they could help the police to make the most of new technologies, while commanding public trust and confidence.

Questions for conference

- How could new technologies help to improve productivity, service to public and support the police in tackling crime?
- How will the next phase of the digital revolution shape the nature of crime and harm?
- To what extent should artificial intelligence lead to the automation of tasks currently carried out by police officers and staff?
- What does the increased capacity for mass surveillance mean for policing and the public in a democratic society?
- How can we ensure that policing remains accountable to the public when it is utilising advanced technologies for public safety purposes?

References²³

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.

Bragias A., Hine K., and Fleet R. (2021) 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research*, 22(6), pp.1637-1654.

Brown, A., Harkin, D., and Tanczer, L. (2024) Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence Against Women*, 0 0:0.

Brynjolfsson, E., & McAfee, A. (2014) *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. New York: W.W. Norton and Co.

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*. New York: Association for Computing Machinery, pp.331-337.

Couchman, H. (2019) *Policing by machine*. London: Liberty.

Dechesne, F. (2019) *AI and Ethics at the Police: Towards Responsible use of Artificial Intelligence in the Dutch Police*. Leiden/ Delft: Universiteit Leiden.

Dell'Acqua, F. et al., (2023) *Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality*. Harvard Business School Technology and Operations Management Unit Working Paper No. 24-013 [online] Available at: <https://www.hbs.edu/ris/Publication%20Files/24-013_d9b45b68-9e74-42d6-a1c6-c72fb70c7282.pdf>

Dupont, J., Wride, S. and Ali, V. (2023) What does the public think about AI? Public First [online] Available at: <<https://publicfirst.co.uk/ai/>>

Ell, M. (2024) *Cyber security breaches survey 2024: education institutions annex*. London: Department for Science, Innovation and Technology [online] Available at: <<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex#:~:text=Of%20all%20the%20educational%20institutions,to%20identify%20breaches%20or%20attacks.&text=Bases%3A%20%2C000%20UK%20Businesses%3B%20185,colleges%3B%2031%20higher%20education%20institutions>>

Ezzeddine, Y., Bayerl, P. and Gibson, H. (2023) Safety, Privacy, Or Both: Evaluating Citizens' perspectives around artificial intelligence use by police forces. *Policing and Society*, 33 (7), pp. 861-876.

Fair Trials (2022) *Equality data in criminal justice*. Brussels: Fair Trials.

Ferguson, A. (2017) *The Rise of Big-Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.

Fussey, P., and Sandhu, A. (2022) Surveillance arbitration in the era of digital policing. *Theoretical Criminology*, 26(1), pp.3-22.

Floridi, L., and Taddeo, M., (2016) What is Data Ethics? *Philosophical Transactions of the Royal Society A*, 374(2083).

Gother, P., Ngan, M. and Hanaoka, K. (2019) *Face Recognition Vendor Test. Part 3: Demographic Effects*. NISTIR 8280. Gaithersburg, MD: National Institute of Standards and Technology.

Hall, W. (2023) *Engineering Responsible AI: Q&A with Professor Dame Wendy Hall FREng FRS*. Royal Academy of Engineering 24 August [blog] Available at: <<https://raeng.org.uk/blogs/ai-blog-series-professor-dame-wendy-hall-freng-frs>>

²³ Accessed 20.05.24

- Harcourt, B. (2006) The Ratchet Effect: An Overlooked Social Cost. In *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. Chicago: University of Chicago.
- Higgins, A. and Halkon, R. (2023) *Contact and confidence in a digital age*. London: The Police Foundation.
- Hobson, Z., et al. (2023) Artificial fairness? Trust in algorithmic police decision-making. *Journal of Experimental Criminology* 19, pp.165–189.
- Home Office (2023) *Police use of Facial Recognition: Factsheet*. Home Office News Team. 29 October [online] Available at: <<https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/>>
- IWF (2023) *How AI is being abused to create child sexual abuse imagery*. Cambridge: Internet Watch Foundation.
- Kearns, I. and Muir, R. (2019) *Data-driven policing and public value*. London: The Police Foundation.
- Kaplan, J. (2016) *Artificial Intelligence: What everyone needs to know*. Oxford: Oxford University Press.
- Licht, K., and Licht, J. (2020) Artificial intelligence, transparency, and public decision-making. *AI and Society* 35 (4), pp. 917-926.
- Longoni, C., Bonezzi A., and Morewedge, C. (2019) Resistance to medical artificial intelligence. *Journal of Consumer Psychology* 46(4) pp.629–650.
- Lukens, P. (2024) Transformation and creativity: How AI can change police services without cutting jobs. *Policing Insight* 17 May [online] Available at: <<https://policinginsight.com/feature/innovation/transformation-and-creativity-how-ai-can-change-police-services-without-cutting-jobs/>>
- Mansfield, T. (2023) *Facial recognition technology in law enforcement equitability study: Final report*. Teddington: National Physical Laboratory.
- Metropolitan Police Service (2021) *Written Evidence to House of Lords Justice and Home Affairs Committee Inquiry: New Technologies and the Application of the Law* (NTL0031). London: Metropolitan Police Service.
- McFadzien, K., et al. (2020). The Evidence-Based Investigative Tool (EBIT): a Legitimacy-Conscious Statistical Triage Process for High-Volume Crimes. *Cambridge Journal of Evidence-Based Policing*, 4, pp.1-15.
- Miller, C. (2019) *The Death of the Gods: The New Global Power Grab*. London: Windmill Books.
- Muir, R. (2016) Robocops: are the police robots coming? The Police Foundation. 30 September [online] available at: <<https://www.police-foundation.org.uk/2016/09/robocops-are-the-police-robots-coming/>>
- NCA (2019) *National Strategic Assessment of Serious and Organised Crime 2019*. Available at: <<https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file>>
- NCA (2020) *National Strategic Assessment of Serious and Organised Crime 2020*. Available at: <<https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file>>
- NPCC (2023) *Covenant for Using Artificial Intelligence (AI) in Policing*. London: National Police Chiefs' Council.
- OpenAI. (2023) ChatGPT (May 13 version) [Large language model] [online] Available at: <<https://chat.openai.com/chat>>
- Pughsley, A. (2023) *The Policing Productivity Review*. London: Home Office.
- Purshouse, J. and Campbell, L. (2022) Automated facial recognition and policing: a Bridge too far? *Legal Studies*, 42(2), pp. 209–227.
- Rabinovich-Einy, O. and Katsh, E. (2014) Digital justice: Reshaping boundaries in an online dispute resolution environment. *International Journal of Online Dispute Resolution*, 1(1), pp. 5–36.
- Rowe, M. and Muir, R. (2021) Big data policing: Governing the machines? in J. McDaniel and K. Pease (eds) *Predictive Policing and Artificial Intelligence*. London, Taylor and Francis, pp. 254-68.
- Russell, S. (2021) BBC Reith Lectures 2021 – *Living with Artificial Intelligence, Lecture 1, 'The Biggest Event in Human History*, BBC Radio 4, 1 December.
- Samoili S., et al. (2020) *TES analysis of AI Worldwide Ecosystem in 2009-2018*. Luxembourg: Publications Office of the European Union.
- Say, M. (2023) *The outlook for science and technology in policing*. UK Authority. 23 November [online] Available at: <<https://www.ukauthority.com/articles/the-outlook-for-science-and-technology-in-policing/>>

- Schwab, C (2016) *The Fourth Industrial Revolution: what it means, how to respond*. World Economic Forum. 14 January [online] Available at: <<https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>>
- Shelley, P. (2006) The Defence of Poetry in Z. Leader and M. O'Neill, ed. *Major Works*. Oxford: Oxford University Press.
- Standley, N. (2024) Pupils miss classes as school cyber attacks rise. *BBC*. 10 May. [online] Available at: <<https://www.bbc.co.uk/news/articles/c2vwz4exq4xo>>
- Sweetland, J. (2024) CC Gavin Stephens: 'I think there's a real opportunity for a policing reset on a number of fronts'. *Policing Insight*. 16 April [online] Available at <<https://policinginsight.com/feature/cc-gavin-stephens-i-think-theres-a-real-opportunity-for-a-policing-reset-on-a-number-of-fronts/>>
- Today* (2024) BBC Radio 4. 14 May. Available at <<https://www.bbc.co.uk/programmes/m001z6hg>>
- The Police Foundation (2020) *Public Safety and Security in the 21st Century: The First Report of The Strategic Review of Policing in England and Wales*. London: The Police Foundation.
- The Police Foundation (2022) *A New Mode of Protection Redesigning Policing and Public Safety for the 21st Century: The Final Report of The Strategic Review of Policing in England and Wales*. London: The Police Foundation.
- Thompson, L. (2024) Facial Recognition for Lead Generation and Lineup Construction. In, E. Pica, Ross, R., and J. Pozzulo, (eds) *The Impact of Technology on the Criminal Justice System: A Psychological Overview*. London: Routledge, pp. 56-74.
- Torkington, S. (2024) The US is drafting new laws to protect against AI-generated deepfakes. World Economic Forum. 27 February [online] Available at <<https://www.weforum.org/agenda/2024/02/ai-deepfakes-legislation-trust/>>
- Turing, A. (1950) Computing machinery and intelligence. *Mind*, 59, pp. 433-460.
- UK Government (2023) *Chair's Summary of the AI Safety Summit 2023*, Bletchley Park. [online] Available at <<https://www.gov.uk/government/publications/ai-safety-summit-2023-chairs-statement-2-november>>
- Waardenburg, L., and Huysman, M. (2022) From coexistence to co-creation: Blurring boundaries in the age of AI, *Information and Organization*, 32(4).
- Wells, H. et al. (2023) 'Channel Shift': technologically-mediated policing and procedural justice. *International Journal of Police Science & Management* (in press).
- World Economic Forum (2024) *The Global Risks Report 2024*. Geneva: World Economic Forum.
- 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. *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*. Oxford: Association for Computing Machinery, pp. 880-889.

© 2024 The Police Foundation

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

Enquiries concerning reproduction should be sent to The Police Foundation.

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE
POLICE
FOUNDATION

The UK's policing think tank