JUSTICE



AI in Policing: international lessons and domestic solutions

A JUSTICE Report

justice.org.uk

December 2025

Joint Foreword

The pace of technological change is relentless. Policing cannot afford to stand still. Artificial Intelligence is already reshaping the world around us: how we live, work, and interact with one another. If policing does not act decisively and collaboratively now, it risks falling behind, leaving gaps that undermine public trust, operational effectiveness, and the very principles of justice.

This report is not just a set of recommendations. It is a call to action. It sets out a clear, practical roadmap to ensure that the use of AI in policing is implemented responsibly, transparently, and in a way that strengthens the rule of law. The urgency is real. Without coordinated standards, legal clarity, and robust governance, we face fragmented approaches and inconsistent safeguards. We will reduce instead of enhance trust and confidence in policing.

This JUSTICE report reflects the collective effort of many, but special recognition must go to the JUSTICE team for their skill, hard work and dedication in analysing and bringing together complex evidence and perspectives into actionable proposals. Their work demonstrates what can be achieved when expertise and commitment align. Equally, the advisory group has been instrumental in shaping the vision, challenging assumptions, and ensuring that every recommendation is grounded in both operational reality and democratic accountability.

This is a pivotal moment for policing. The decisions we make now will define how policing uses AI for at least the next decade. We must act with urgency, clarity, and unity, because we recognise that the cost of inaction is too high. We welcome the recommendations of the report and will seek to work with JUSTICE and partners, to make them a reality.



Lord John Thomas of Cwmgiedd

House of Lords, JUSTICE Council and member of the Advisory group to this report



Alex Murray OBE

National Police Chiefs' Council AI lead and National Crime Agency Director

Contents

Executive Summary 4

Chapter 1: Introduction 8

Chapter 2: International lessons learnt 16

Chapter 3: Learning from these lessons in England and Wales 30

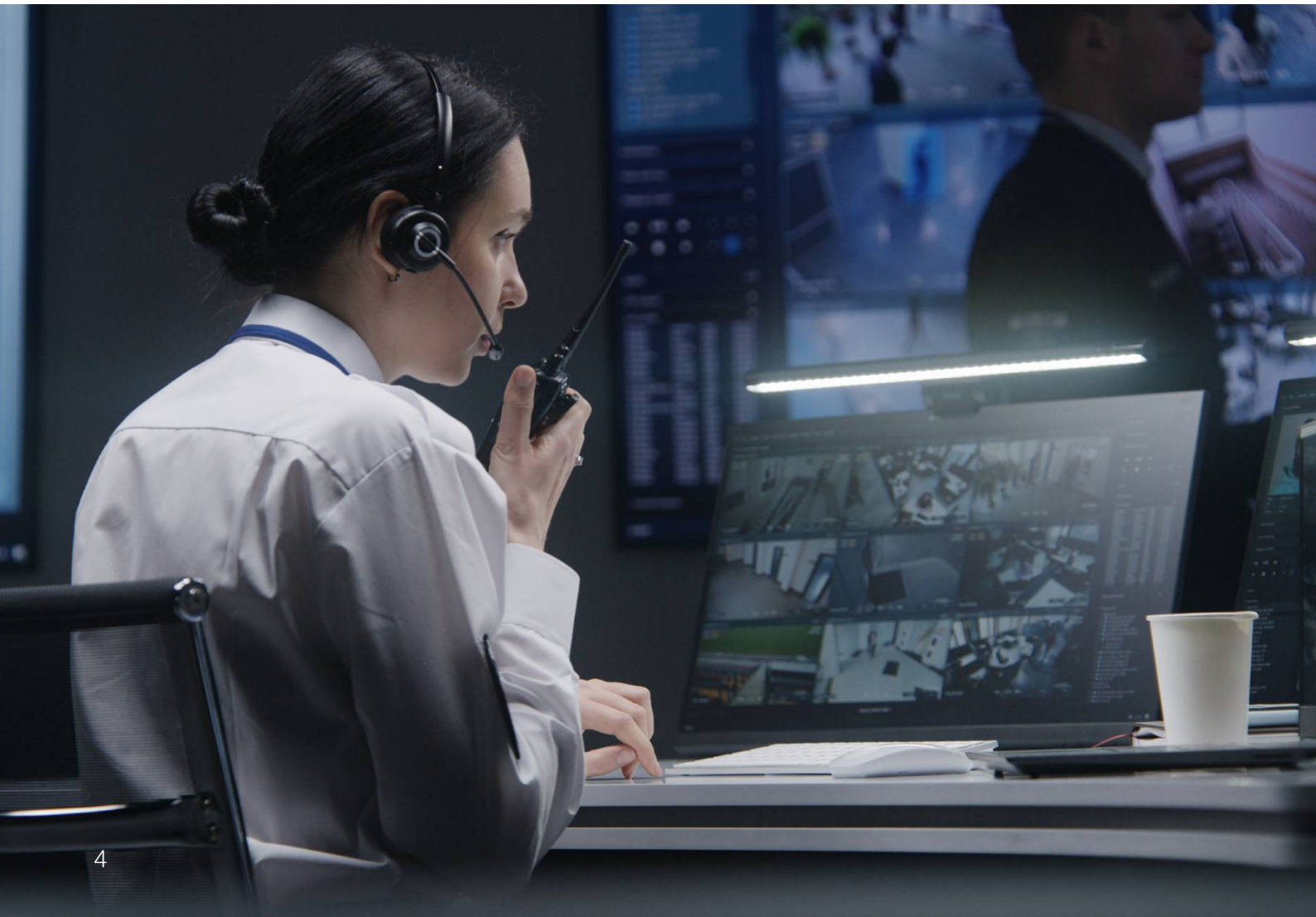
Chapter 4: The way forward – responsible AI in policing that the public can trust 53

Acknowledgements 60

Executive Summary

1. Artificial intelligence ("**AI**") is rapidly reshaping public services, and policing is no exception. The pace of innovation, the scale of private-sector investment, and the UK Government's explicit ambition to "mainline AI into the veins of the nation" mean that AI deployment in policing is not a distant prospect but an accelerating reality. This brings significant opportunities: enhanced investigative capability, faster processing of digital evidence, improved risk assessment, and the potential to intervene earlier to prevent harm. Yet it also carries profound risks for human rights, the rule of law, and public trust. The police occupy a uniquely powerful position in our democratic society; integrating AI into that environment without the right safeguards risks entrenching discrimination, undermining lawful decision-making, and eroding communities' confidence in policing.

2. This report asks a central question: **what must be in place for AI in policing to be trustworthy, value for money, effective in achieving policing goals, and compliant with human rights and the fair administration of justice?** To answer this, JUSTICE carried out international research, examined domestic developments, and convened stakeholders across policing, government, civil society, regulators, academia, and industry. Across this work, five lessons emerged, each of which signals not only what must be done, but the urgency of acting now while the UK remains at a crossroads.



Lesson 1: Fitness for Purpose – AI tools must work, and must work for the context in which they are used

3. Across jurisdictions, we found striking examples of unvalidated, inaccurate or unsuitable AI tools being deployed in policing, from software that did not contain the AI capabilities vendors claimed, to transcription tools with low but disastrous error rates, to predictive tools whose underlying accuracy was misunderstood due to unreliable metrics. These cases demonstrate that AI can fail in ways that create operational inefficiency, serious risks to individual rights and undermine public legitimacy and trust.

4. In England and Wales, the current 43-force structure fosters innovation but generates inconsistency. There is no shared definition of what "good enough" accuracy looks like for different policing contexts, no common standards for testing or validation, and insufficient coordination on procurement. As a result, forces can reach different conclusions about whether the same tool is fit for purpose—some making effective, well-evidenced decisions, others relying heavily on vendor claims or limited in-house expertise.

5. **To ensure tools are genuinely fit for purpose, policing requires national standards, shared testing capacity and a coordinated approach to procurement,** so decisions are driven by policing needs, legal obligations and ethics—not by market incentives.

Lesson 2: Competent, Ethical and Lawful Use – Human oversight must be real, informed and supported

6. When tools have been deployed without proper training or without users understanding their limitations, significant harms have resulted. International examples illustrate how automation bias, over-trust in opaque systems, or pressures of "tough on crime" cultures can distort professional judgement. Human oversight only functions as a safeguard if users understand an AI tool's uncertainties, confidence levels, and appropriate applications.

7. In England and Wales, there is no mandatory training regime for AI-enabled tools outside digital forensics, and no accreditation framework for officers expected to oversee them. Moreover, ambiguous or incomplete legal frameworks – particularly for biometric tools – risk leaving officers to navigate complex rights-interference issues through local policy alone.

8. **Effective human oversight requires clear legal rules, consistent communication of technical limitations, and organisational cultures that value scrutiny over expediency**. Responsibility must be distributed across policing and the tools' design and development; officers cannot be expected to interpret complex AI systems on their own – they need training and well-designed user interfaces which effectively present them with the information they need to exercise scrutiny.

Lesson 3: Understanding Impacts – AI tools must be evaluated both before and after deployment

9. Some of the most troubling examples from overseas involve AI tools that generated discriminatory or rights-violating outcomes for months or even years before intervention. Bias embedded in training data, flawed assumptions within models, and distortive feedback loops can all compound existing inequalities.

10. Yet evaluation is not only about fairness: it is also about whether systems deliver real-world value. Some technologies marketed as productivity tools have shown no measurable efficiency gains when independently assessed. Without ongoing monitoring, forces cannot know whether AI is improving policing or wasting public money.

11. In England and Wales, monitoring capacity is patchy. Academic researchers often cannot access underlying systems; post-deployment evaluations are inconsistent; and incentive structures reward "innovation" more than

ongoing scrutiny. Crucially, no mechanism exists to ensure forces share findings with each other or with the public.

12. **The policing landscape requires ongoing evaluation, shared data and learning across forces, an open culture with independent researchers and a systematic approach to understanding how AI changes skills, behaviour and decision-making.**

Lesson 4: Proportionate and Effective Safeguards – Clear limits, accountability routes and effective redress are essential

13. Safeguards may arise from design choices, legal frameworks, independent oversight or routes for individuals to challenge their treatment. Internationally, we observe that safeguards only function where transparency exists; without it, unlawful or harmful technology can persist in the shadows.

14. The EU AI Act provides one model: tiered obligations based on risk, strict limits on biometric surveillance, and mandatory oversight. By contrast, the UK's regulatory framework for policing AI is fragmented. Important oversight bodies exist—the Information Commissioner, Biometrics and Surveillance Camera Commissioner, Forensic Science Regulator—but their mandates do not cover all relevant tools or all policing contexts.

15. Routes to remedy for individuals affected by AI-driven decisions remain unclear and inaccessible, particularly outside criminal proceedings. Meanwhile, in criminal proceedings, we need to ensure defendants have a fair trial. Access to the disclosure and expertise they need to understand the reliability of tools and adequately challenge them is essential if we want to guard against another Post Office-Horizon scandal in the future.

16. **The UK needs a coherent, proportionate system of safeguards that match the risk of the technology, are enforceable, and ensure accessible routes for challenge when harm occurs.**

Lesson 5: Public Participation – Trust requires visibility, involvement and accountability

17. Public attitudes research shows that while the public does not oppose police use of AI, they are unwilling to write a blank cheque. They demand transparency, fairness, accountability and robust rules. Yet in practice, public engagement in England and Wales remains limited, sporadic and largely informational rather than participatory.

18. International case studies show the benefits of embedding community participation into design and oversight—from Vancouver's collaborative development of predictive tools to Taiwan's radical models of citizen involvement in technology governance. Conversely, secrecy has undermined trust and led to scandal.

19. **To sustain legitimacy, policing must bring the public into the conversation early and often, through transparent AI registers, local ethics committees, and a national participatory mechanism which is ongoing and permanent.**

The Way Forward: A New Independent Central Body for Responsible AI in Policing

20. Across all five lessons, the same structural gap appears: England and Wales lacks a central, independent mechanism to coordinate standards, innovation, oversight, research, procurement, and public engagement. While new structures are welcome, including the National Police Chiefs' Council's AI Portfolio, the Science and Innovation Committee, the Office of the Police Chief Scientific Advisor and the Science Technology Analysis and Research fund, they do not yet provide the full systemwide capability required.

21. JUSTICE therefore recommends establishing **a new independent central body**, which would likely fit well within the Government's future plans for a National Centre for Policing. Its mandate should include:

    (a) **Setting mandatory technical and governance standards** for specific AI use cases.

    (b) **Coordinating oversight,** aligning standards across existing regulators, identifying regulatory gaps, and powers to fill those gaps where needed.

    (c) **Supporting responsible innovation,** including a national AI testing environment, an innovation hub, and ethical/legal/technical advisory services to forces and vendors.

    (d) **Reviewing legal clarity**, through ongoing analysis of how emerging technologies interact with existing law and recommending solutions to Ministers (such as in biometrics, where we conclude current lack of clarity requires legislative action).

    (e) **Enabling national research** enabling access to tools and datasets for independent scrutiny by researchers, a national testing programme, and ensuring systemic and longitudinal evaluations are included in research strategy.

    (f) **Embedding public participation,** through national engagement mechanisms and support for local ethics committees.

22. This body should be independent, expert-led, and transparent. Pending its establishment, existing bodies should adopt elements of these functions. Primary legislation will be required to establish it and give it the powers it needs – for example to set mandatory standards in codes of practice. That legislative process will be a valuable opportunity for society which it has not had so far: a democratic process through which we debate what role we want AI to play in policing.





Chapter

1

Chapter one: Introduction

Chapter one: Introduction

1. The use of artificial intelligence ("**AI**") in policing is no longer the subject of science fiction; it is a reality. AI technologies have the potential to offer new insights, enhanced capabilities, and valuable efficiencies for a service on which there is unrelenting demand, and on which the public depends for public safety and justice. But the risks are many: overreliance and underreliance, opaque systems, unaccountable tools, biased data and systems, and inaccurate outputs influencing harmful, unfair and discriminatory outcomes. Harnessing that potential, while guarding against the risks, is the challenge of our age, and policing is no exception. In fact, it is one of the most important areas that we get it right.

2. Policing is no ordinary public service: it can deprive individuals of their liberty, search and seize their property, investigate and prosecute offences, and surveil public spaces in the interests of public order. AI could improve the way police exercise these powers, or it could drastically worsen it. The latter would be devastating for the rule of law, human rights, the fair administration of justice in this country, and the public's trust and confidence in the police. We need the right conditions, infrastructure and support so the police can innovate responsibly, learn from mistakes honestly, and enhance policing with AI for the benefit of society.

3. This report interrogates those conditions and asks - **what do we need in place for AI in policing to be trustworthy, value for money, successful in achieving policing objectives, while protecting human rights, the rule of law and the fair administration of justice?**

4. This report builds on JUSTICE's flagship report published in January 2025: *'AI in our Justice System'* which addressed the adoption of AI across our whole justice system, from legal services to policing, from civil to administrative law.[1] We proposed a rights and rule of law-based framework for responsible AI use in the justice system, incorporating legitimate goals of AI deployment, management of risks at technical, individual and system levels, and integrating transparency and accountability to the public. We have adopted this framework – of being goal-led, and rigorously analysing risks on technical, individual and system level – throughout our work on this report.

What we mean by "AI in Policing"

5. There is no general definition of AI that enjoys widespread consensus. In *'AI in our justice system'*, we adopted a broad understanding of the term in line with the OECD definition as of May 2024: *"An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."*[2] This aligns largely with the definition used by the UK Government in its Data Ethics Framework,[3] along with its more recent adoption of the two characteristics highlighted by the OECD – adaptivity and autonomy – into its understanding of the distinct functional capabilities of AI.[4]

6. We did not conduct a comprehensive mapping of all policing AI being used or being prospectively developed in England and Wales, but we are aware others are undertaking this work.[5] However, through desktop research and stakeholder engagement we identified several use cases across a range of different applications in policing, which we summarised into four categories.[6]

1 JUSTICE, 'AI in Our Justice System' (January 2025).
2 OECD, 'Recommendation of the Council on Artificial Intelligence' (OECD Legal Instrument OECD/LEGAL/0449, adopted 22 May 2019); OECD, 'Explanatory memorandum on the updated OECD definition of an AI system' OECD Artificial Intelligence Papers No 8 (OECD Publishing, Paris 2024).
3 Government Digital Service and Central Digital & Data Office, Data Ethics Framework: glossary and methodology (2020)
4 Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation' (March 2023).
5 Mapping police AI in England and Wales is one of the work products of the UKRI-funded four year PROBabLE Futures project.
6 We do not suggest these are definitive categorisations, rather they were helpful during our work based on the use cases on which we focused. There were areas of future AI use – such as robotics – which our review did not consider.



Biometric tools: Tools which analyse biometric data to identify, classify or make inferences about individuals. For example:

- Live facial recognition in a public space for identification of those on a watchlist.
- Retrospective biometric identification, of a face on CCTV footage, or of a voice on an audio file, in the context of an investigation.
- Tools used to infer emotions, credibility or the psychological state of a person from their facial expressions, gait or other physical attributes or behaviours.



Text generating tools for summarisation, statement generation and transcription: Tools which generate text to represent a summary or transcription – from audio data or a far larger amount of text – to streamline workload, including generating draft evidential statements. For example:

- Transcription of body worn camera footage or police interview recording into a draft summary or into draft witness statements.
- Summarising content of open-source data, e.g. social media, for intelligence gathering.
- Summarising evidence contained in a mobile phone extraction to inform investigatory directions and maintain a record of evidence for disclosure purposes.



Probabilistic data analysis tools: Tools which analyse large amounts of data to predict risk or likelihood of harm, or to inform and prioritise police interventions, intelligence analysis or criminal investigations.[7] For example:

- Prediction of where and when crime is likely to take place in a geographical area.Analysis of the likelihood of individuals committing a crime/further crime.
- Analysis of mobile phone extraction data in an investigation, e.g. to identify aggressive content of messages, or patterns of communication indicative of stalking.
- Analysis of open-source data in intelligence gathering e.g. to identify indications of social disorder through social media posts.



Public interaction tools: Tools which support or replace police interactions with the public, to improve experiences and prioritise resources. For example:

- Online chatbots to assist victims to make a report.
- Automated triage of calls based on detected severity or vulnerability, based on voice tone and/or transcribed content.
- translation for communication with non-English speaking members of the public.

7 Whilst acknowledging that a lot of the AI systems used in the other three categories can constitute, or incorporate, probabilistic technology. "Probabilistic" meaning AI models which use probability theory and statistical models to incorporate uncertainty and make predictions with an associated confidence score. See Open Data Science, 'Embracing Uncertainty: How Probabilistic AI is Redefining Decision-Making' Medium (29 May 2025).

The current context in England and Wales

7. There have been several previous independent reviews of policing and the wider justice system's use of and algorithms and emerging technologies over the past decade, notably the Law Society's Commission on the Use of Algorithms in the Criminal Justice System in 2019[8]; the Royal United Services Institute's report on '*Data analytics and Algorithmic Bias in Policing'* in 2020, commissioned by the Centre for Data Ethics and Innovation,[9] the Justice and Home Affairs Committee's report '*Technology Rules? The advent of new technologies in the justice system'* in 2022[10], and the Ryder review of biometrics governance in 2022, commissioned by the Ada Lovelace Institute.[11]

8. These reports all have different areas of focus, but some key themes can be identified. They all highlight the need for legal and regulatory clarity, in terms of when technology can be used, the conditions of use, and the rights of impacted individuals and groups. They stress the importance of transparency, between those deploying technology and the public, as well as between private developers and justice system actors. They emphasise the importance of control staying in the hands of justice system actors, not private companies, highlighting the impact design and development decisions can have on bias and discrimination, the right to a fair trial, and the privacy of individuals and their (sensitive) personal data. And those looking at oversight mechanisms highlighted the importance of both proactive guidance and effective enforcement from regulators,[12] and the need for independent oversight.[13]

9. Our work seeks to build on these reviews, taking into consideration several further developments in the technology and the current political, economic and societal context.

10. Firstly, central government policy has crystalised in the last three years. In January 2025, the UK Government made clear its intention to "*turbocharge AI*" and "*mainline AI into the veins"* of the nation, aspiring towards AI-driven economic growth.[14] Its approach is pro-innovation, growth-led and slow to regulate, unlike the neighbouring European Union.[15] It intends to do so through investment in infrastructure; attracting companies making frontier AI to the UK, and public sector adoption.[16] The AI Opportunities Action Plan recommended that public sector employ a "*scan, pilot, scale*" approach; investing in a continually updated understanding of AI capabilities, rapidly developing prototypes and identifying successful pilots to be rolled out beyond organisational boundaries.[17] In September 2025, $31billion investments in the UK were announced from US technology firms including Microsoft, Nvidia and Google, dubbed a "*Tech Prosperity Deal*" with promises including data centres in AI Growth Zones and a supercomputer.[18]

11. Secondly, this growth-led agenda is largely attributable to the advent of general-purpose generative AI.[19] OpenAI's Chat GPT – the "*emblematic product of the AI boom*"[20] – launched as a free to use chatbot in November 2022. Just three years later in November 2025 it has 800 million active weekly users.[21] General-

8 The Law Society of England and Wales, *Algorithms in the Criminal Justice System* (2019).
9 Alexander Babuta and Marion Oswald, *Data Analytics and Algorithmic Bias in Policing* (Royal United Services Institute 2019).
10 House of Lords Justice and Home Affairs Committee, 'Technology Rules? The advent of new technologies in the justice system', 1st Report of Session 2021–22, HL Paper 180 (2022).
11 Matthew Ryder KC, *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales* (Ada Lovelace Institute June 2022).
12 The Law Society of England and Wales, *Algorithms in the Criminal Justice System* (2019), 6-8.
13 House of Lords Justice and Home Affairs Committee, 'Technology Rules? The advent of new technologies in the justice system', 1st Report of Session 2021–22, HL Paper 180 (2022), 76.
14 Department for Science, Innovation and Technology, Prime Minister's Office, 10 Downing Street, The Rt Hon Peter Kyle MP, The Rt Hon Sir Keir Starmer KCB KC MP and The Rt Hon Rachel Reeves MP, 'Prime Minister sets out blueprint to turbocharge AI' (GOV.UK, 13 January 2025).
15 Which has passed the EU AI Act, a comprehensive regulatory framework for AI: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689.
16 Department for Science, Innovation and Technology, 'AI Opportunities Action Plan' (January 2025).
17 Ibid.
18 Zoe Kleinman, Faisal Islam 'Nvidia boss says UK will be 'AI superpower' as tech firms invest billions' *BBC News* (17 September 2025).
19 A model that "can create ('generate') content that is ... complex, coherent, [and] original. For example, a generative AI model can create sophisticated essays or images." See Google, *Machine Learning Glossary: Generative AI* (2024). For a reference list of definitions, see JUSTICE'AI in Our Justice System' (January 2025), 9.
20 Dan Milmo, 'Boom or bubble? Inside the $3tn AI datacentre spending spree' *The Guardian* (2 November 2025)
21 Ibid.

purpose generative AI,[22] particularly that which can generate text, has been predicted to have transformative effects on global economies and productivity.[23] These transformative expectations can be seen to be reflected in the sheer scale of investment in AI as well as the stratospheric valuation of AI companies, alongside some concerns of creating an AI bubble.[24]

12. Thirdly, we now have an emerging understanding of public attitudes to these technologies. Since 2022, nationally representative surveys have revealed the UK public's concern about AI has increased, while perceptions of benefits have remained stable.[25] In response to that concern, there is a growing public desire for rules and oversight: the majority (over 75%) feel it is "*very important*" for the government or independent regulators to have a suite of safety powers, rather than private companies alone having this control, while a majority (72%, up from 62% in 2022/23) indicate that laws and regulations would increase their comfort with AI technologies.[26]

13. Levels of concern can also be seen to vary between demographic groups, particularly in relation to facial recognition use in policing, with higher concern levels from Black and Asian people about false accusations than the general population.[27] Meanwhile, recent public attitudes research through deliberative workshops has painted a mixed picture having explored police AI use *other* than facial recognition with members of the public (AI handling 101 calls, AI summarises evidence, and predictive policing AI).[28] Participants agreed there are clear benefits to police embracing AI, including efficiency gains, keeping human errors in check, and helping police to be more preventative and protective of people's rights and safety, rather than reactive. However, concerns included data security, loss of human interactions between police and the public, bias and inaccuracies, and the lack of transparency, safeguards and oversight. In addition, there was a consistent and strong feeling that AI was inevitable, and was happening without the public's involvement and approval.[29]

22 As opposed to non-generative AI, i.e. "AI which primarily relies on algorithms that draw information directly from vast data sets to detect patterns, forecast outcomes and support decisions. The dominant technique is Machine Learning (ML), and its more sophisticated subset, Deep Learning (DL). This kind of AI employs probabilistic models to predict outcomes and give recommendations. […] The strength of recent non-Generative AI lies in the ability to handle extremely large and potentially unlabelled and unstructured datasets." OECD, *The Impact of Artificial Intelligence on Productivity, Distribution and Growth* (2024), 10.
23 Michael Chui and others, 'The Economic Potential of Generative AI: The Next Productivity Frontier' (McKinsey & Company, June 2023) 50.
24 Dan Milmo, 'Boom or bubble? Inside the $3tn AI datacentre spending spree' *The Guardian* (2 November 2025).
25 Roshni Modhvadia, Tvesha Sippy, Octavia Field Reid and Helen Margetts, 'How Do People Feel About AI?' (Ada Lovelace Institute and The Alan Turing Institute, 2025).
26 Ibid.
27 Ibid. See general finding 4: 39% of the general population expresses concern about its use in policing, this rises to over half among Black (57%) and Asian (52%) people.
28 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025). JUSTICE's Senior Lawyer, Ellen Lefley, sat on the independent oversight group for this project, 2024-2025.
29 Ibid.



14. Fourthly, drivers for adoption of AI in policing have persisted.

    (a) UK police forces continue to look to technology to help productivity, as they experience high demand on their resources,[30] particularly as the reach of a number of other public services has reduced, in a context of tighter resources and rising demand, such as in mental health.[31] The recent police productivity report, published by the National Audit Office in November 2025, records the growing financial pressure on police forces with "*£276 million of financial reserves drawn down by police forces in 2024-2025 to help balance their annual budgets*",[32] and amongst a range of recommendations to improve productivity, highlights the need for "*faster implementation of new technologies and use of AI*".[33]

    (b) The police are increasingly expected to prevent harm proactively, rather than to only retrospectively investigate criminal activity,[34] while policymakers have increasingly focused on public order, expanding police powers and introducing new offences.[35]

    (c) In addition, cybercrime and online offences continue to rise, adding extra pressure to police workloads.[36] Estimates have been made that digital evidence features in 90% of criminal investigations,[37] with digital forensics – both incorporating AI and not – developing at a rapid rate to respond. However, researchers have found the breadth and speed of the development of digital forensics has "*far outpaced*" the national infrastructure necessary to properly utilise it for the detection and investigation of suspected crimes.[38]

    (d) There is a swell behind AI deployment in policing, with the creation of a new AI Portfolio in the National Police Chiefs' Council ("**NPCC**") and several initiatives discussed later in this report. The Police Foundation too has reported on the potential for AI to revolutionise policing, identifying institutional, cultural and data reform needed to seize the opportunity.[39] The area in which there has been the most media attention has been in the swell of adoption in live facial recognition technologies.[40] In September 2025, Metropolitan Police Commissioner Sir Mark Rowley described live facial recognition as a "*game-changing tool*"[41] while the Home Office announced its financial support for the roll out of live recognition vans across England and Wales, beyond their current use by a few early adopter forces.[42]

15. This emerging landscape reflects the pace of change in the last three years. We conclude that there is a window of opportunity now to get the conditions right for incorporating AI technology into policing well, but it is one which will close fast if the pace of change continues, or even speeds up.

30 See for example, London Assembly Police and Crime Committee, *Public Order Policing – the Met's Approach* (April 2025).
31 Home Office, *Policing Productivity Review: Independent Report* (April 2024).
32 National Audit Office, *Police Productivity* (HC 1380, Session 2024–26, 3 November 2025) 23.
33 Ibid, 12.
34 Alexander Babuta and Marion Oswald, 'Data Analytics and Algorithmic Bias in Policing' (Royal United Services Institute 2019).
35 See the new powers and offences in the Police, Crime, Sentencing and Courts Act 2022 and the Public Order Act 2023.
36 Institution of Engineering and Technology, 'Cyber Crisis: Surge in attacks leaves UK public feeling unsafe online' (1 October 2025).
37 House of Lords Science and Technology Select Committee, 'Forensic science and the criminal justice system: a blueprint for change', HL Paper 333 (2019).
38 Cerian Griffiths; Emma Piasecki; Sophie Carr; Philip Anderson; Tim Wilson, *Digital Forensics in the Criminal Justice System: Use, Effectiveness and Impact*. (The Northumbria University Digital Forensics Project, 2024).
39 Rick Muir, Felicity O'Connell, *Policing and Artificial Intelligence* (The Police Foundation, February 2025)
40 Defined by the Biometrics and Surveillance Camera Commissioner as follows: "'live time' […] facial recognition algorithms refers to the deployment of surveillance camera systems by the police with the intention of conducting surveillance upon members of the public so as to capture their images which are then automatically processed in 'live time' so as to extract biometric data, specifically measurements of facial features, which is then immediately compared against biometric data contained on a watchlist which is held within a data base. […] Also in this context, 'near real time' is a term which should be interpreted as being applicable to those circumstances whereby images are analysed by facial recognition technology very shortly (a matter of minutes) after the images are captured as part of a surveillance. It is acknowledged that 'near real time' is a relatively non-specific term which requires a degree of ethical interpretation to be applied by decision makers." See *Facing the Camera, Good Practice and Guidance* (November 2020), 1.5-1.6.
41 'More than 700 arrests this year from live facial recognition' *BBC News* (10 September 2025).
42 Home Office, 'Live Facial Recognition technology to catch high-harm offenders' (News release, 13 August 2025).

This report

16. AI adoption in policing is not a challenge that the UK faces alone. Although the experiences of other countries will never straightforwardly apply here, key learnings from other jurisdictions provide a valuable resource to understand how we should navigate this terrain.

17. To prepare this report, we therefore conducted international research into how AI is used by the police different jurisdictions. From this research we extracted key lessons learnt and applied these to the England and Wales policing context, undertaking desktop research, consultations and a workshop with stakeholders to answer the above question - **what do we need in place for AI in policing to be trustworthy, value for money, successful in achieving policing objectives, while protecting human rights, the rule of law and the fair administration of justice?** Stakeholders included regulators, industry bodies, policing, private developers, Government, civil society, community leaders, academia, Parliamentarians and lawyers.

18. Our review and our recommendations in many areas serve to underline the urgency of solutions already proposed by others in previous reports. In other areas, our report will highlight a need to reconsider the right solution for the world we find ourselves in today.





Chapter

2

Chapter two: International lessons learnt

Chapter two: International lessons learnt

19. We reviewed use cases of AI in policing across several countries, for lessons which have already been learnt about the use of AI in the policing and law enforcement context. Our hypothesis behind this exercise was as follows: we can learn from mistakes which have been made elsewhere and hardwire against them, while identifying good practice which will help us secure responsible AI design, development and deployment.

20. Our review was global, but by far the highest volume of use cases we identified and analysed was from the US – this weighting is reflected in the examples quoted below. We developed our lessons learnt iteratively during our review. Below, we summarise the five core lessons learnt which we identified, and provide several examples of the most useful case studies.

Lesson 1: We need to ensure AI technology is fit for purpose

21. We found examples of technology being used which doesn't work at all; doesn't work well enough in the context it is being used in; or only works for some people and not others, i.e. it is biased in its inaccuracy. When technology isn't fit for purpose, the impacts can vary depending on the context: it can simply make processes more inefficient; it can make communities less safe through the deployment of ineffective technology; or it can expose individuals and groups to arbitrary police powers, surveillance and even make them vulnerable to miscarriage of justice. Our examples below demonstrate some of these potential impacts, as well as demonstrating that reliance on marketing claims alone is an inadequate way to ensure fitness for purpose.

22. **Not fit for purpose at all and the importance of validation in procurement:** A tool used by police in Utah, US – "*Live Time*" marketed by software firm Banjo – is an example of technology that did not do what the vendors claimed. Live Time was marketed as providing live event detection – such as "*child abduction cases, active shooter cases, traffic accidents*" – allegedly by collecting a large stream of data from traffic cameras, CCTV cameras, social media, 911 emergency systems, and using AI to synthesise this data to understand the context of an event.[43] After an investigatory journalist revealed that the CEO had previously been involved in criminal activity as part of a white supremacist group, a state audit was ordered. It was not just issues with the CEO's personal affiliations which were uncovered, however. The audit in fact uncovered that the *"actual capabilities of Live Time appeared inconsistent with Banjo's claims"* and that "*Live Time lacked the advertised AI technology.*"[44] One key criticism arising from this audit was that the Office of the Attorney General – which had procured the tool – did not verify the claims made by Banjo during the procurement process, which had instead been based on claims, not actual capability. To assist with his inquiry, the state auditor convened the Commission on Protecting Privacy and Preventing Discrimination.[45] The Commission issued software procurement principles including that vendors should clearly demonstrate the validity of their marketing claims and that validation of all AI claims should be required, including capability reviews.[46] Although the example of Live Time is unusual, the Utah police department's use of Banjo's software and willingness to invest $20.7 million into the technology[47] serves as a stark reminder of the importance of validating marketing claims during the procurement process.

23. **The importance of context – small error rates can have drastic consequences:** Even when an AI tool uses a valid method, it can have a degree of inaccuracy or

43 Jason Koebler and Joseph Cox, 'Utah Gave $20 Million Contract to AI Surveillance Firm That Didn't Have AI' *VICE* (30 March 2021).
44 Office of the State Auditor (Utah), *Review of Banjo IT Controls* (26 March 2021) 1.
45 Ibid, 2.
46 Ibid, 8 - 10.
47 Jason Koebler and Joseph Cox, 'Utah Gave $20 Million Contract to AI Surveillance Firm That Didn't Have AI' *VICE* (30 March 2021).

unreliability. However, even low levels of inaccuracy can be harmful. Whisper, a transcription software by OpenAI is integrated into platforms including Chat GPT, Oracle and Microsoft, and is advertised by to have "*high accuracy and ease of use*".[48] In fact, a scientific paper available on OpenAI's website states that when "*compared to a human* […] *the best zero-shot Whisper models roughly match*[ed] *their accuracy and robustness.*"[49] While the rate of hallucinations is difficult to assess,[50] one study found that only 1% of Whisper audio transcriptions contained entire hallucinated[51] phrases or sentences. However, 38% of the hallucinations amounted to explicit harms such as perpetuating violence, making up inaccurate associations, or implying false authority.[52]

24. For example, a speaker said:

"*He, the boy, was going to, I'm not sure exactly, take the umbrella*" followed by a pause.

Whisper transcribed as follows:

"*He, the boy, was going to, I'm not sure exactly, take the umbrella.* ***He took a big piece of across. A teeny small piece. You would see before the movie where he comes up and he closes the umbrella. I'm sure he didn't have a terror knife so he killed a number of people who he killed and many more other generations that were […] And he walked away."***

A speaker in another recording described:

"*two other girls and one lady*."

Whisper invented extra commentary on race and transcribed:

"*two other girls and one lady****, um, which were Black***."[53]

25. This example demonstrates that simply measuring inaccuracy 'incidents' does not fully capture the risk: a hallucination of an obviously erroneous random word is qualitatively different to a hallucination which changes the meaning of the text in a plausible, substantive and entirely erroneous way. It also demonstrates the importance of fitness *for purpose* – the above hallucinations may be unacceptable, even if there is only a 1% risk of them occurring, in a policing context, since false allegations or descriptions could impact the reliability of documentary evidence, and even risk impacting the direction of an investigation.

26. **A systems-approach to fitness for purpose – the downstream impact of inaccuracy on the criminal justice process:** Draft One is an AI tool produced by Axon, which drafts police reports based on auto-transcribed body camera audio. It is deployed slightly differently by police departments across the US depending on local policies.[54] The Chief Prosecutor in King County, Washington State, decided last year that the tool was not fit for the purpose of drafting police narratives to be used in prosecutions, due to the "*likely result in many of your officers approving Axon-drafted narratives with unintentional errors in them.*"[55] In the letter to police departments explaining the decision, he cites an example one report which referenced an officer who was not even at the scene.[56] Additional concerns included that Draft One does not keep a draft of what it produces or what the officer fixed or added, and does not track its rate of errors.[57] Although officers must edit the transcript and confirm under penalty of perjury that it

48 OpenAI, 'Introducing Whisper' (21 September 2022).
49 Alec Radford and others, 'Robust Speech Recognition via Large-Scale Weak Supervision' (OpenAI, 21 September 2022) 6.
50 Garance Burke and Hilke Schellmann, 'Researchers say AI transcription tool used in hospitals invents things no one ever said' AP News (26 October 2024). Researchers have found different rates, from "*nearly every one*" of a 26,000 hour sample, to only 187 of a 13,000 audio file sample.
51 Hallucinations are productions of false or inaccurate information by large language models. See Jean Kaddour et al, 'Challenges and Applications of Large Language Models' (2023) arXiv:2307.10169, 19-20.
52 Allison Koenecke, Anna Seo Gyeong Choi, Katelyn X Mei, Hilke Schellmann and Mona Sloane, 'Careless Whisper: Speech-to-Text Hallucination Harms' in *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24)* (Association for Computing Machinery 2024) 1672, 1674.
53 Garance Burke and Hilke Schellmann, 'Researchers say AI transcription tool used in hospitals invents things no one ever said' AP News (26 October 2024), citing examples from Profs Allison Koenecke and Mona Sloane, verified by email correspondence with the authors, October 2025.
54 For instance, in Lafayette, Indiana, officers can use Draft One to generate reports for any kind of case, but in Oklahoma City, Oklahoma, Draft One reports cannot be used on cases which result in arrest. Scripps News, 'Police Officers Are Starting to Use AI Chatbots to Write Crime Reports. Will They Hold Up in Court?' *WRTV* (26 August 2024).
55 Clare Duffy and Emily Williams, 'How AI Is Being Used in Police Stations to Help Draft Reports' *CNN Business* (12 August 2025).
56 Daniel Clark, 'Email to Police Chiefs re: Axon Draft One' (King County Prosecuting Attorney's Office, 20 September 2024; Jeremy Harris, 'AI-assisted police reports not welcome in King County due to potential errors' *KOMO news* (27 September 2024).
57 This issue has also been raised by a digital rights group, Electronic Frontier Foundation, meaning the tool is "*unauditable*" and "*def*[ies] *transparency*": Matthew Guariglia and Dave Maass, 'Axon's Draft One Is Designed to Defy Transparency' *Electronic Frontier Foundation* (10 July 2025).

is accurate, sometimes officers miss certain errors. The Chief Prosecutor expressed concern that if that officer on the stand alleged AI made the error, no draft report would exist to prove it one way or another, with "*devastating […] consequences […] for the case, the community and the officer*."[58]

27. **Measuring "fitness" – the need for a common understanding:** To determine whether technology is fit for purpose it is important to have a clear understanding of how "fitness" is being measured. ShotSpotter, a tool developed by Sound Thinking, Inc. and used in more than 180 cities,[59] "*uses an array of acoustic sensors that are connected wirelessly to ShotSpotter's centralized, cloud-based application to reliably detect and accurately locate gunshots using triangulation"*.[60] Although ShotSpotter claimed that its tool has a 97% accuracy rate, an investigation by the MacArthur Justice Center concluded that "*89%* [of gunshot alerts] *turned up no gun-related crime and 86% led to no report of any crime at all*".[61] An independent report prepared by Edgeworth Analytics commissioned by ShotSpotter clearly states that the 97% accuracy rating from SoundThinking was based on a proxy metric – customer complaints of errors, which in turn "*relies on clients reporting those potential errors to ShotSpotter*".[62] ShotSpotter maintains that its tool is effective and that police agencies and the public approve of the technology's use.[63] The issue is one of measurement: the claim of 97% accuracy is reliant on an implicit assumption, i.e. an output that wasn't complained about must have been accurate. However, its arguable whether this is a suitable metric for accuracy, and whether police can rely on it to understand if the tool is fit for purpose, or value for money. The audit of ShotSpotter demonstrates why it is worthwhile to scrutinise claims made by those marketing AI technology, including the metrics of "accuracy" upon which they are based. We also observe that wildly disparate competing claims of accuracy – such as 3% vs 86-89% inaccuracy above – are likely to undermine public trust and confidence in policing use of AI.

58 Daniel Clark, 'Email to Police Chiefs re: Axon Draft One' (King County Prosecuting Attorney's Office, 20 September 2024; Jeremy Harris, 'AI-assisted police reports not welcome in King County due to potential errors' *KOMO news* (27 September 2024).
59 SoundThinking, 'ShotSpotter Frequently Asked Questions' *SoundThinking*.
60 SoundThinking, 'Gunshot Detection' *SoundThinking*.
61 MacArthur Justice Center, 'ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study' MacArthur Justice Center (3 May 2021); Hannah Cheves, 'ShotSpotter Is a Failure. What's Next?' MacArthur Justice Center (5 May 2022).
62 Edgeworth Analytics, *Independent Audit of the ShotSpotter Accuracy* (28 March 2022).
63 SoundThinking, 'ShotSpotter Public Safety Results' *SoundThinking*.



Lesson 2: We need to ensure AI technology is used competently, ethically and lawfully

28. We found examples of predictive AI tools which are inscrutable to the humans using them, undermining their ability to understand what is behind a prediction and therefore exercise proper analysis of the output. There are also examples of users who are not encouraged or equipped to understand the limitations of what the technology can do and how it can be used, leading to unreliable, incompetent and unethical use. When human police officers make decisions using technology they cannot interpret, or fail to understand the technology's limitations and biases, they risk undermining (not improving) their judgment of what is reasonable, necessary, or proportionate, and may act unlawfully as a result. We also include below a UK example, which demonstrates the importance of legal clarity of the legal frameworks surrounding use, without which there are risks to arbitrariness and unlawful use.

29. **Opaque technology and adequate human oversight:** Predictive risk assessment tools such as COMPAS – which is used to predict the likelihood of recidivism – provide a kind of recommendation which cannot be immediately verified by the human overseer: a prediction of future risk. Decision-making responsibility is still with humans, who are meant to incorporate the prediction into their exercise of judgement, rather than follow it blindly. However, automation bias is a recognised barrier to exercising this judgement well, i.e. when machine information is viewed as inherently trustworthy and above scepticism.[64] Combatting automation bias is hampered when the decision-maker does not understand the limitations of the tool. When the COMPAS risk assessment tool was legally challenged, the Wisconsin Supreme Court mandated that its future use be accompanied by disclosures about its limitations, including: the lack of validation for the state's population; the lack of information about how risk factors were weighed; and the evidence of disproportionate classification of minority offenders.[65] However, the non-profit coalition *Partnership on AI*[66] added that this was insufficient by itself to address the issue, since the disclosures do not help decision-makers understand how they can exercise their scrutiny in light of these limitations. They added that the minimum requirements for human review were that predictions are interpretable, tools produce confidence estimates for their predictions, and there is training on the nature and limitations of the tool.[67] As the US courts recognised with respect to COMPAS, reducing technological opacity is essential to enable meaningful human oversight and involvement.

30. **Training on tool limitations and competent use:** According to a report released in September 2023 by the US Government Accountability Office, only ten of the of the 196 FBI agents who accessed Clearview AI, a facial recognition service from an outside vendor, had completed any training on how to properly use it.[68] This report also identified that although seven law enforcement agencies in the Departments of Homeland Security and the Department of Justice reported using facial recognition services provided by commercial and nonprofit entities, all seven agencies initially used these services without requiring staff take facial recognition training.[69] The purpose of such training is to prevent the likelihood of mistakes by users deploying AI in entirely unvalidated

64 Mary Cummings, 'Automation Bias in Intelligent Time Critical Decision Support Systems' (2004) AIAA 1st Intelligent Systems Technical Conference quoted in Partnership on AI, *Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System* (August 2021) 23; for the opposite phenomenon of tools predictions being ignored, see footnote 44 of the latter, quoting Angèle Christin, 'Algorithms in Practice: Comparing Web Journalism and Criminal Justice' 4(2) *Big Data & Society* (2017).

65 *State v Loomis* 881 NW2d 749 (Wis 2016).

66 A US non-profit organization that convenes a coalition of over 80 members, including civil society groups, corporate developers and users of AI, and numerous academic artificial intelligence research labs, to answer important questions about artificial intelligence policy and ethics.

67 Partnership on AI, *Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System* (August 2021), 25.

68 US Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties* GAO-23-105607 (September 2023) 2, 27.

69 US Government Accountability Office, *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for*

deployments, such as the infamous example of an NYPD officer who once uploaded a photo of actor Woody Harrelson into its facial recognition system to identify a suspect, claiming the individual resembled Harrelson and that the available surveillance footage of the suspect was too blurry to use.[70] By prioritising AI training, police forces decrease the likelihood of such incidents, while increasing accountability to the public.

31. **Leadership and culture shaping the quality of human oversight:** Political or social pressure to act on perceived problems – and the rush to AI as the solution – can lead to messy thinking and rushed decisions. This is especially true in the context of AI, where the stakes and complexity are high. Machine learning algorithms were used in the Netherlands child tax credit scandal, which resulted in tens of thousands of families – often with lower incomes and belonging to ethnic minorities – being wrongly penalised and pushed into poverty. Some victims committed suicide, and more than a thousand children were taken into foster care.[71] The Dutch Parliamentary Inquiry into the scandal named it "*Unprecedented injustice*" and a breach of the rule of law.[72] The scandal also caused PM Mark Rutte's resignation.[73] The machine learning algorithm used to flag possible fraud learnt to profile those with dual nationality and low income as being suspicious.[74] Supposed safeguards were the further checks and demands for documentation,[75] thereby preserving a human in the loop and ensuring no decisions on fraud were taken automatically. However, human fraud investigators worked "*Under the pressure of the clamour of overzealous politicians to deal with fraud, with every [claimant] error being too easily viewed as such*, [...] *result[ing] in parents finding themselves incorrectly branded as deliberate fraudsters*".[76] Issues identified in the Parliamentary inquiry included the fraud teams working to a rule that around 80% of families flagged for further checks would be guilty and 20% would be innocent, even though that ratio was acknowledged to be an assumption rather than being based on any evidence.[77] This example is a stark reminder of the danger of acting under "*pressure […] to deal with*" crime, when it disincentivises scrutiny and individual rights, and the ease with which AI – if not subject to scrutiny – can exaggerate the harm caused by such a culture, automating unlawful discrimination and generalisations about types of people and their propensity to criminality.

32. **Unclear Legal Frameworks:** In the UK, primary legislation does not specifically govern facial recognition technologies. Instead, use is subject to a patchwork of common law policing powers, human rights law, equality law, and data protection law. The Court of Appeal in *Bridges v South Wales Police* found in 2019 that such a patchwork was not a bar to the use of facial recognition technology, provided that the legal use was still made accessible and foreseeable by police, for which purpose public statements of police policy were adequate.[78] Without clear policy statements, however, police officers and the public cannot anticipate how the technology will be used or prevent its arbitrary application. In *Bridges*, the Court of Appeal found South Wales Police's policies insufficient because they failed to provide legal clarity about when the tool would be used and on whom.[79] This meant the use was not "*in*

Civil Liberties GAO-23-105607 (September 2023) 2.

70 Clare Garvie, 'Garbage In, Garbage Out: Face Recognition on Flawed Data' (Center on Privacy & Technology at Georgetown Law, 16 May 2019); Graham Rayman, 'NYPD Uses Celebrity Photos to Track Down Criminals' New York Daily News, republished in Police1 (18 May 2019).

71 Gijs Herderscheê, 'More than 1,100 children of victims of the benefits scandal were removed from their homes' (original Dutch : Charlotte Huisman and Jan Meeus, 'Ruim 1.100 kinderen van gedupeerden toeslagenaffaire werden uit huis geplaatst' *de Volkskrant* (29 October 2021).

72 House of Representatives of the Netherlands, *Ongekend Onrecht [Unprecedented Injustice]: Parliamentary Inquiry into the Childcare Allowance* Parliamentary Document 35 510, no 2 (17 December 2020).

73 BBC News, 'Dutch Rutte Government Resigns over Child Welfare Fraud Scandal' BBC News (15 January 2021).

74 Melissa Heikkilä, 'Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms' Politico (29 March 2022).

75 House of Representatives of the Netherlands, *Ongekend Onrecht [Unprecedented Injustice]: Parliamentary Inquiry into the Childcare Allowance* Parliamentary Document 35 510, no 2 (17 December 2020) 14.

76 Ibid, 7.

77 Ibid, 23.

78 *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

79 Ibid, [91].

accordance with the law" under Article 8 of the European Convention of Human Rights, since the breadth of discretion given to police officers was so broad as to be open to arbitrariness.[80] This case shows that unclear legal frameworks do not support the lawful use of AI tools, and risk creating overly broad areas of discretion which are "*so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself*".[81]

Lesson 3: We need to understand how AI technology is impacting people and systems around it

33. We have found examples of rights-infringing technology going unscrutinised for years. Other examples show a lack of impact assessment beforehand as well as a lack of evaluation afterwards. However, it is only by doing these assessments that we will understand the fairness, value for money, and proportionality of the technology, when it is out of the lab and used "in the wild". Examples also point to limited understanding of the value of independent review and scrutiny. However, errors and unintended consequences won't be identified if those evaluating are only looking for what they want to see. The value is not just to those immediately impacted by the technology but crucially to the wider trust and confidence of the public.

34. **Evaluations of bias and discrimination:** Biased input data, which often reflects societal biases, can create discriminatory outputs of AI tools, while also often creating feedback loops which then further embed discrimination and perpetuate harm to those discriminated communities. Independent academic evaluation has identified this racial bias in predictive policing algorithms.[82] Many forms of machine vision have been found to exhibit biases, from self-driving cars' lesser ability to spot people with darker skin,[83] to the well documented racial and gender biases in widely used facial recognition algorithms in the US between 2002 and 2019.[84] Intersectional discrimination was found in the seminal 2018 study by Joy Boulamwini & Timnit Gebru, who audited commercial systems which classified the gender of facial images and found an error rate for darker-skinned women to be up to 35 times higher than that of white men.[85] Racial bias in risk scores was also famously uncovered by investigative journalists in the individual risk assessment tool, COMPAS.[86] In Queensland, Australia, concerns have been raised about piloting new risk algorithms for domestic violence risk[87] due to established disproportionality of Aboriginal and Torres Strait Islander people subject to domestic violence proceedings,[88] and evidence of discriminatory and inaccurate actuarial risk assessments for Indigenous children used in Queensland.[89] This history of bias and discrimination in data-driven technology highlights the need to proactively evaluate impacts of new technologies, and be

80 Ibid, [210].
81 *In the matter of an application by Lorraine Gallagher for Judicial Review (Northern Ireland)* [2019] UKSC 3 [17].
82 Rashida Richardson, Jason M Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (2019) 94 *New York University Law Review Online* 192.
83 Anthony Cuthbertson, 'Self-driving Cars More Likely to Drive into Black People, Study Claims' The Independent (6 March 2019).
84 As evaluated by NIST, see P Jonathon Phillips, Patrick Grother, Ross Micheals, Duane Blackburn, Elham Tabassi and Mike Bone, 'Face Recognition Vendor Test 2002: Evaluation Report' NIST Interagency Report 6965 (National Institute of Standards and Technology 2003); Patrick Grother, George W. Quinn and P Jonathon Phillips, 'Report on the Evaluation of 2D Still-Image Face Recognition Algorithms' NIST Interagency Report 7709 (National Institute of Standards and Technology, 24 August 2011); Mei Ngan and Patrick Grother, 'Face Recognition Vendor Test (FRVT): Performance of Automated Gender Classification Algorithms' NIST Interagency Report 8052 (National Institute of Standards and Technology, April 2015). Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' NIST Interagency Report 8280 (National Institute of Standards and Technology, December 2019). Sources collated originally in David Leslie, 'Understanding Bias in Facial Recognition Technologies: An Explainer' (The Alan Turing Institute 2020) 19, fn 19.
85 False positives occurred only 0.8% of the time when the technologies were used to identify white men, while error rates for darker-skinned women were up to 34.7%: Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) Proceedings of Machine Learning Research vol 81, 1, 9.
86 Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks' *ProPublica* (23 May 2016).
87 Heather Douglas and Robin Fitzgerald, 'Qld Police Will Use AI to Predict Domestic Violence Before It Happens – Beware the Unintended Consequences' *The Conversation* (16 September 2021).
88 Heather Douglas and Robin Fitzgerald, 'The Domestic Violence Protection Order System as Entry to the Criminal Justice System for Aboriginal and Torres Strait Islander People' (2018) 7(3) *International Journal for Crime, Justice and Social Democracy* 41.
89 The tool was assessed to produce high false positive rates for Indigenous children, and its criteria proved better at predicting race than recurrence of risk: Brian Q Jenkins and Clare Tilbury, 'An Evaluation of the Racial Equity of the Actuarial Family Risk Assessment Instrument Used in Queensland, Australia' (2024) 164 *Children and Youth Services Review* 107891.

transparent about the results. Indeed, the *Bridges* case found the lack of evaluation to be a breach of the duty in England and Wales to proactively promote equality and eliminate discrimination (the Public Sector Equality Duty).[90] But in addition, we observe there is also a need to acknowledge embedded histories of biased treatment, and continuous evaluation to be a real practical commitment not to perpetuate such bias in the future.

35. **Evaluations of efficiency impact:** Even where tools perform their stated objectives, they may not significantly benefit law enforcement agencies. In the United States, many police forces have made use of Draft One, as explained above. However, a randomised control trial at the University of South Carolina showed that, despite vendor claims about the tool's ability to increase efficiency, there was no significant decrease in officers' workloads. The tool did not have a meaningful impact on time saved in officers' administrative responsibilities.[91] These findings underline the importance of impact assessments and real-world testing of the AI technologies used in policework, as they may not be as beneficial to the system as they appear. A rigorous approach to evidence is particularly important given the cost of AI tools to police departments, money which could be spent elsewhere.[92] The cost ultimately is to taxpayers, who would justifiably expect cost benefit analyses to be robustly calculated to ensure that tools are a productive addition to police work, in any procurement and evaluation monitoring processes.

36. **Impact on policing skills and capabilities:** Research on automation over several decades has highlighted reoccurring challenges and unintended consequences of introducing machines into workplace systems. Instead of simply introducing efficiency, automation can paradoxically make the human operator's role more critical and complex.[93] De-skilling may occur when automation stops a human operator from retaining or improving their skills, creating an irony where individuals with potentially diminished skills are expected to oversee complex systems.[94] Meanwhile automation can reduce situational awareness leading to "automation surprises" where operators are caught off guard; or induce complacency, causing operators to be more likely to accept automation outputs without critical evaluation, elsewhere referred to as cognitive offloading.[95] However, such impacts are not inevitable, and policing is a particular context which requires specialist study. For example, while people in general have been shown to offload memory processing tasks to devices, such as cameras, a study on police-worn body cameras have shown police officers *did not* show evidence of cognitive offloading.[96] The study suggests that officer training, for example, may "*mitigate cognitive offloading to some extent, since it encourages officers to attend to and encode a variety of cues in their environment".*[97] How police skills and capabilities are impacted by AI, both on an individual case basis and on a systemic level over time, warrants careful attention and further study. Without such evaluation, it will be impossible to make informed choices about trade-offs, and we risk proceeding on the basis of immediate productivity gains without truly understanding the impact of AI on policing.

90 *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
91 Ian T Adams, Matt Barter, Kyle McLean, Hunter M Boehme and Irick A Geary Jr, 'No Man's Hand: Artificial Intelligence Does Not Improve Police Report Writing Speed' (2024) *Journal of Experimental Criminology*.
92 US examples anecdotally show it can range between tens of thousands and millions of dollars per year. Aaron Sankin and Surya Mattu, 'Predictive Policing Software Terrible at Predicting Crimes' Wired (2 October 2023); Jason Koebler and Joseph Cox, 'Utah Gave $20 Million Contract to AI Surveillance Firm That Didn't Have AI' *Vice* (30 March 2021).
93 Lisanne Bainbridge, 'Ironies of Automation' *Automatica*, 19, 6 (1983), 775.
94 Steve G. Sutton, Vicky Arnold, and Matthew Holt, 'How Much Automation Is Too Much? Keeping the Human Relevant in Knowledge Work' *Journal of Emerging Technologies in Accounting* 15, 2 (2018), 15.
95 Prakash Shukla, Phuong Bui, Sean S Levy, Max Kowalski, Ali Baigelenov, Paul Parsons, 'De-skilling, Cognitive Offloading, and Misplaced Responsibilities: Potential Ironies of AI-Assisted Design' Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26-May 1, 2025, Yokohama, Japan.
96 Brittany Blaskovits, Bryce Jenkins, Andrew Brown, Simon Baldwin and Craig Bennell, 'Misplacing Memory: Examining the Phenomenon of Cognitive Offloading During an Officer-Involved Use-of-Force Scenario' (2022) 37(1) *Journal of Police and Criminal Psychology* 49.
97 Brittany Blaskovits, Bryce Jenkins, Andrew Brown, Simon Baldwin and Craig Bennell, 'Misplacing Memory: Examining the Phenomenon of Cognitive Offloading During an Officer-Involved Use-of-Force Scenario' (2022) 37(1) *Journal of Police and Criminal Psychology* 49.

Lesson 4: We need proportionate and effective safeguards

37. As set out above, we must make sure that we are aware of how AI technology is impacting people and systems around it. However, without acting upon that knowledge, it serves little purpose. We found examples of safeguards which can prevent harm occurring in the first place, through design choice, pre-deployment assessments, and laws which create legal frameworks around use. However, safeguards are also important to ensure contestability and redress after use, so that AI technology which unjustifiably discriminates against people, breaches human rights, or operates at a loss to the detriment of the public purse cannot be allowed to proliferate or do so with impunity. Unfortunately, limited transparency mechanisms, poor access to independent review or complaint mechanisms, and competing interests between commercial providers and public sector, or indeed between state institutions and the public, means that such flawed technology sometimes remains in use.

38. **Safeguards by Design:** Appropriate safeguarding for AI technology starts at the design stage. The Vancouver Police Department, Canada, uses a machine learning location-based algorithmic system called GeoDASH (Geographic Data Analysis and Statistics Hub) APS. GeoDASH APS is a predictive hotspot tool, which uses police data of where theft and burglary crimes have taken place to generate location-based forecasts of where they are likely to occur in the next 24 hours. An important design feature is that crime data is exclusively from cases that were triggered by a complaint from a civilian to police and excludes all police-initiated reports. The purpose of this policy is to reduce both the risk and the perception that police bias influences the training data or algorithms.[98] An additional feature is its use of "*exclusionary zones*". These "*exclusionary zones*" are used for neighbourhoods where there are concerns of over-policing, in an attempt not to replicate feedback loops of over-policing seen in US predictive policing tools. The effect is simply that locations within the exclusionary zones will not be recommended as high risk by the GeoDASH APS.[99] Another example is KIRaPol.5G, a research project between 2022 and 2024 funded by the German state of North Rhine-Westphalia. The project sought to use radar sensor technology for surveillance in certain public places instead of video.[100] The radar software does not take video footage or biometric data, rather radar sensors collect anonymised data and AI was then used to train and detect potential hazards and dangerous situations. No announcement has been made as to whether the technology will be used any further, however it is an example of innovation incorporating safeguards by design, to mitigate the privacy concerns associated with CCTV and facial recognition technology.

39. **Safeguards through pre-deployment assessments and processes:** Several US States have recommended pre-deployment quality checks for AI tools. In California, state agencies aiming to procure new generative AI technology must identify a business need which the proposed technology will meet, understand the implications of using generative AI to solve that problem, and participate in a comprehensive discovery process to ensure that the technology will effectively meet agency needs.[101] Additionally, before deploying a solution that includes generative AI into production, the state entity must "*invest time and resources to prepare data inputs and test models adequately*".[102] Federally, agencies using AI which has been designated "*high-impact*", for example

98 Kate Robertson, Cynthia Khoo, and Yolanda Song, 'To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada' (The Citizen Lab and University of Toronto Faculty of Law, 2020), 42.
99 Ibid, 44.
100 SENTIRE Radar, 'KIRaPol.5G: Artificial Intelligence for Radar Systems to Support Police Surveillance in Public Places and Train Stations' (Radar-Sensor.com).
101 'California Department of Technology, Department of General Services, Office of Data and Innovation and Department of Human Resources, *State of California GenAI Guidelines for Public Sector Procurement, Uses and Training* (March 2024).
102 Ibid.

identification of criminal suspects and forecast of crime, must complete pre-deployment testing and conduct ongoing monitoring for potential adverse impacts.[103]

40. **Safeguards through ongoing monitoring:** The National Institute of Standards and Technology ("**NIST**") in the US provides independent government evaluations of prototype face analysis technologies, including facial recognition. The evaluation programme - which has been running in some form since 1999 - is ongoing, with vendors being able to resubmit new versions every 4 months. It is designed to provide U.S. Government and law enforcement agencies with information to assist them in determining where and how facial recognition technology can best be deployed. It has established benchmarks both for the quality of facial recognition and demographic differences, as well as other "face analysis" technology, such as the effects of masks and age estimation. Its results also aim to help identify future research directions for the facial recognition community.[104]

103 Office of Management and Budget, *M-25-21: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* (3 April 2025) 17, 21.
104 National Institute of Standards and Technology, 'Face Technology Evaluations – FRTE/FATE' (14 December 2016, updated 22 April 2025).



41. **Safeguards through transparency and investigation:** The deployment and investigation of facial recognition tool Clearview AI by the Royal Canadian Mounted Police ("**RCMP**") illustrates how post-deployment investigation by regulators is a safeguard, but only when there is transparency about the use of a tool. Clearview AI's facial recognition software scrapes images from the internet (including social media), creates biometric identifiers for each image, assesses images uploaded by end-users against these biometric identifiers and provides a list of matching images and metadata.[105] On January 17, 2020 following an inquiry from the Canadian Broadcasting Corporation asking whether the RCMP were utilizing Clearview AI, the RCMP responded saying that it "*does not currently use facial recognition software*."[106] However, in February 2020, following freedom of information (**"FOI"**) requests revealing a contract with Clearview AI had begun three months earlier (and reports that Clearview AI's list of clients had been hacked), RCMP publicly announced that they had been using Clearview AI.[107] After the RCMP publicly admitted to using Clearview AI, the Privacy Commissioner of Canada initiated an investigation, during which Clearview AI withdrew from the Canadian market entirely.[108] In February 2021, the Privacy Commissioner found Clearview AI's scraping of images from the internet was unlawful under Canadian privacy law.[109] This investigation illustrates how external oversight by regulatory bodies can hold AI deployers to account, but the importance of transparency in the first place as a gateway to accountability.

42. **Legislative safeguards in the EU AI Act:** The purpose of the EU AI Act is stated to be, amongst other things, to ensure that AI systems protect democracy and the rule of law.[110] It does so by imposing legal requirements proportionate to risk, with high-risk AI systems requiring providers to set up risk management systems, conduct data governance, draw up technical documentation, design automatic record-keeping, provide instructions for use, design the system for appropriate accuracy, robustness and cybersecurity. Providers must equip deployers to use AI systems effectively by offering clear instructions that highlight limitations, designing systems to support human oversight, and establishing quality management processes for ongoing compliance.[111] As regards live biometric, e.g. facial recognition specifically, the Act clearly acknowledges that the "*use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons*".[112] Accordingly, the use of these biometric systems for the purpose of law enforcement is prohibited "*except in exhaustively listed and narrowly defined situations*."[113] More specifically, there is a definitive list of use cases, including identifying victims of human trafficking, terrorism and identifying suspects for certain criminal offences, including such offences punishable for a maximum period of at least four years.[114] Further, each such use "*for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible space*" must be *"subject to a prior authorisation granted by a judicial authority or an independent administrative authority*".[115] This judicial oversight mechanism embedded into the text of the EU AI Act highlights how legislative

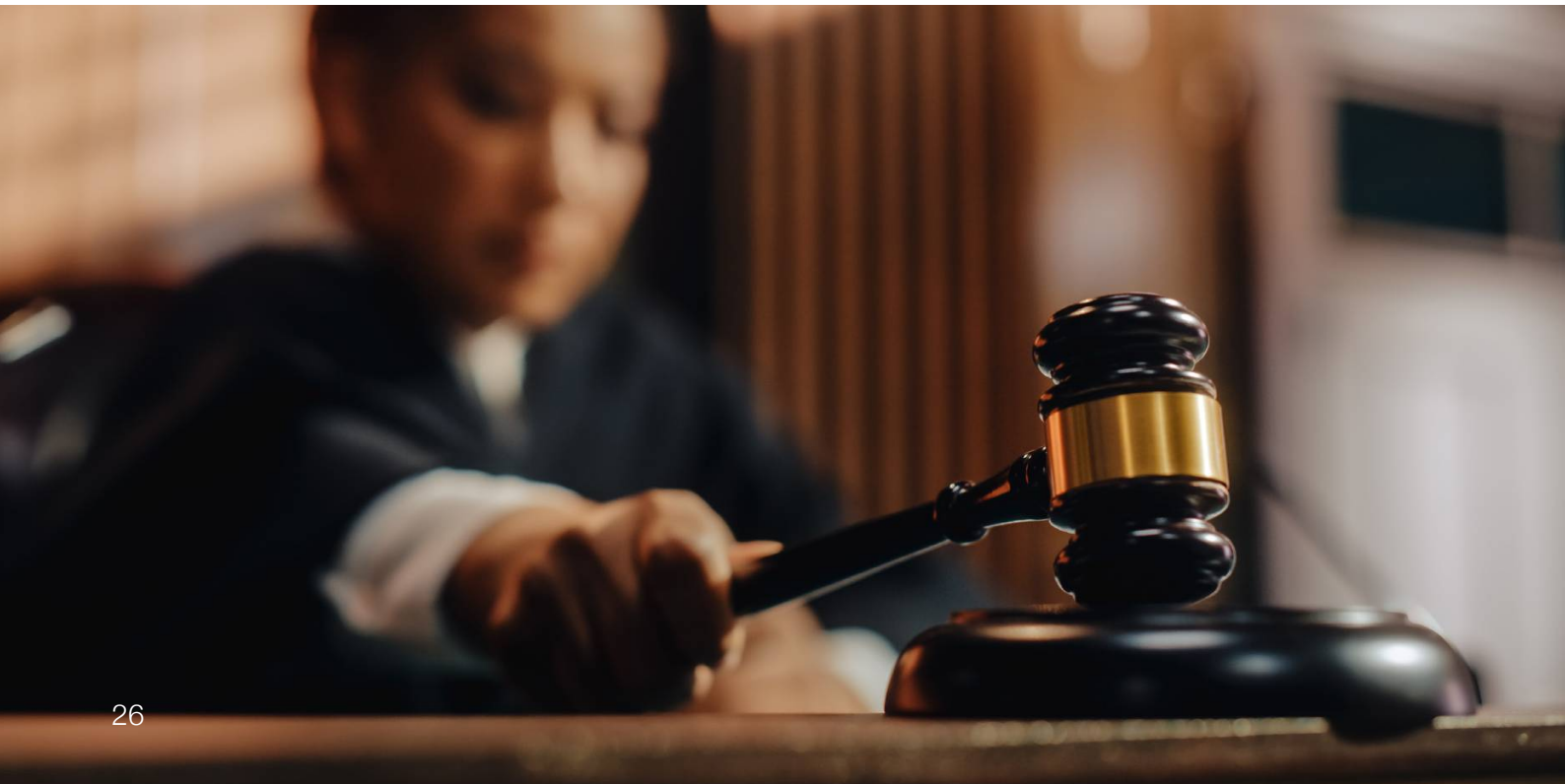
105 Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Information and Privacy Commissioner for British Columbia and Information and Privacy Commissioner of Alberta, 'Joint Investigation of Clearview AI, Inc.' PIPEDA Findings #2021-001 (2 February 2021).
106 Catharine Tunney, 'RCMP Denied Using Facial Recognition Technology - Then Said It Had Been Using It for Months' *CBC News*, (4 March, 2020).
107 Bryan Carney, "FOI Documents Confirm RCMP Falsely Denied Using Facial Recognition Software," *The Tyee* (16 April 2020); Catharine Tunney, 'RCMP Denied Using Facial Recognition Technology - Then Said It Had Been Using It for Months' *CBC News*, (4 March, 2020).
108 Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Information and Privacy Commissioner for British Columbia and Information and Privacy Commissioner of Alberta, 'Joint Investigation of Clearview AI, Inc.' PIPEDA Findings #2021-001 (2 February 2021).
109 Ibid.
110 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, Recital 1.
111 Ibid, arts 8–17.
112 Ibid, Recital 32.
113 Ibid, Recital 33, art 5.
114 Ibid, art 5(1)(h).
115 Ibid, art 5(3).

safeguards may be used to protect the rights of individuals against unlawful AI use in policing.

43. **Fair trial safeguards – New Jersey v Arteaga:** This case illustrates the importance of procedural safeguards in criminal proceedings when AI tools are used in criminal investigations. Following a bank robbery, video footage was processed using facial recognition technology which produced a match. The suspect identified was then included in a photo lineup alongside filler images, and a witness selected him. The defendant requested disclosure about the facial recognition system used, arguing that he needed access to assess the reliability of the match. On appeal, the Superior Court of New Jersey, Appellate Division agreed, finding that the "*Defendant must have the tools to impeach the State's case and sow reasonable doubt*".[116] This case underscores the need for due process safeguards, including transparency about AI systems, to protect the right to a fair trial and prevent miscarriages of justice. Fairness of criminal proceedings may require access to information about the quality and reliability of AI tools used in investigations, even if the technology itself is not submitted as evidence.

44. **Inadequate safeguards:** Russia provides an example of widespread use lacking regulation, oversight, or legal guardrails on police deployment of AI surveillance technology. Facial recognition technologies are deployed across Russia by law enforcement agencies. Starting in 2017, for instance, over 160,000 cameras were installed across Moscow, with more than 3,000 connected to facial recognition systems.[117] Though initially deployed to assist law enforcement in detecting suspected criminals and carrying out general policing work, these live facial recognition systems have been used against political protesters and dissidents to monitor their movement. A Reuters review of over 2,000 Russian court cases demonstrates that live facial recognition has been used to support the arrests of protesters.[118] Despite the major human rights and function creep concerns implicated by this research, Russia's model of surveillance is only expanding, with plans to develop a nationwide system of data collection from CCTV cameras across the country. As of 2024, the equivalent of $130 million USD has been designated for the expansion of live facial recognition.[119]

116 State of New Jersey v Francisco Arteaga, A-3078-21 (NJ Super Ct App Div, 2023) 37.
117 Cameron Manley, 'Russia's Boom In Facial Recognition Cameras To Crack Down On Dissent' Worldcrunch (25 October 2023).
118 Lena Masri, 'Facial recognition is helping Putin curb dissent with the aid of U.S. tech' *Reuters* (28 March 2023).
119 Masha Borak, 'Researchers spotlight Russia's opaque facial recognition surveillance system' *BiometricUpdate,* 21 June 2024.



Lesson 5: The public should be included at all stages

45. We found examples of the public being left in the dark about what AI is being designed, developed, piloted, or indeed used, in policing. Examples include a complete absence of information released into the public domain; a lack of effort to engage the public, academia, civil society, and impacted communities before, during and after use; and a lack of candour when direct questions are asked. This is a missed opportunity not just to inform the design, deployment or evaluation of technologies with wider perspectives, but also to inform society about the drivers for innovation and build trust about why a certain tool may be beneficial. The result can fuel distrust, misinformation, damaged relationships with communities, and overwhelmingly negative associations with a technology or private sector partners which then, no matter how much evidence of benefits may follow, become too difficult to overcome.

46. **Public Engagement in predictive policing:** The Vancouver Police Department has integrated public involvement during the design, development and deployment of its GeoDASH location-based predictive software, explained above. Firstly, external academics from a multitude of academic institutions in Canada and internationally were integrated into the design and development of the tool, which was described not as a bilateral process between Vancouver Police and the software company, Latitude Geographics, but rather as a "*three-way private-public undertaking*".[120] Secondly, the deployment of the tool was accompanied by quarterly meetings between Vancouver Police and community policing services, which are each operated, staffed and governed by members of the community.[121] These meetings allow communities raise issues of over-policing or put at-risk communities on the predictive policing unit's radar.[122] Finally, the technology has a rare public interface – anyone can access the GeoDASH interactive mapping tool to see recent local reports of crime in the Vancouver area.[123] The public tool is an attempt to be "*transparent*" and "*intended to enhance community awareness of policing activity in Vancouver*."[124]

47. **Too little too late:** Conversely, failing to engage appropriately with the public may have negative consequences for both AI developers and the public. As discussed above, in January 2020 the Canadian Broadcasting Corporation asked the RCMP whether they were utilising Clearview AI, to which a spokesperson from the RCMP national headquarters responded that the "*RCMP does not currently use facial recognition software.*"[125] However, a few months later, following FOIs and reports that Clearview AI's list of clients had been hacked, the RCMP publicly confirmed that they had been using Clearview AI,[126] announcing "*in the interest of transparency,* […] *we recently started to use and explore Clearview AI's facial recognition technology in a limited capacity*."[127] In addition to Canada's federal police force, the Toronto police admitted that certain officers had been using Clearview AI since October 2019, despite initially denying its use.[128] As discussed above, Clearview AI was subject to an investigation during which it entirely withdrew from the Canadian market and the software was ultimately found to be unlawful. It is impossible to know with certainty how the situation would have unfolded if Clearview AI and RCMP had been proactively transparent. However, it could even have led to a far more proactive collaboration with the Privacy Commissioner about what kind of facial recognition tools were lawful under Canadian privacy law,

120 Kate Robertson, Cynthia Khoo, and Yolanda Song, 'To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada' (The Citizen Lab and University of Toronto Faculty of Law, 2020), 42.
121 'Community Policing Centres' *Vancouver Police Department website.*
122 Kate Robertson, Cynthia Khoo, and Yolanda Song, 'To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada' (The Citizen Lab and University of Toronto Faculty of Law, 2020), 44.
123 'Vancouver Police Department GeoDASH Crime Map'.
124 Ibid.
125 Catharine Tunney, 'RCMP Denied Using Facial Recognition Technology – Then Said It Had Been Using It for Months' CBC News (4 March 2020).
126 Bryan Carney, 'FOI Documents Confirm RCMP Falsely Denied Using Facial Recognition Software' The Tyee (16 April 2020); 'Controversial Firm Clearview Gets Hacked' Biometric Technology Today, no 3 (March 2020) 12; Catharine Tunney, 'RCMP's use of facial recognition tech violated privacy laws, investigation finds' CBC News (10 June 2021).
127 Nicole Bogart, 'RCMP admits to using controversial Clearview AI facial recognition technology' *CTV News* (27 February 2020).
128 CBC News, 'Toronto police admit using secretive facial recognition technology Clearview AI' (13 February 2020).

saving any wasted taxpayer money which was spent on the unlawful software.

48. **Radical Public Participation:** Outside of a police-specific context, public participation in government policy-making has been subject to significant reforms in Taiwan.[129] Spearheaded by Digital Minister, Audrey Tang, since 2014, Taiwan has implemented innovative solutions for involving the public, going beyond traditional consultations and adopting citizen-led models. Through "Alignment Assemblies" and the digital platform Polis, it has prioritised radical transparency, public involvement, and consensus building, including "*invit[ing] everyday citizens to co-govern AI*".[130] By Tang's departure from government, the approval ratings had risen from 10% in 2014 to over 70% a decade later.[131] This example underscores the broader benefits of public engagement in policy-making, and serves as a reminder that the benefits of involving the public are tried and tested.

129 Audrey Tang, 'Democracy in the Age of AI' RSA Journal (25 June 2024).
130 Ibid.
131 Polly Curtis, 'How Taiwan bucked a global trend – and restored voters' trust in politics' The Guardian (22 July 2024).





Chapter

3

Chapter three: Learning from these lessons in England and Wales

Chapter three: Learning from these lessons in England and Wales

49. For each of the international lessons learnt in the previous Chapter, below we evaluate the lesson in the context of England and Wales and conclude what is needed in this jurisdiction. Our vision for the way forward, amalgamating our conclusions and setting out our recommendations, is set out in Chapter 4.

50. Our discussions and conclusions below are based on desktop research, discussions with stakeholders during one-to-one interviews as well as contributions made at a workshop hosted by JUSTICE in September 2025 and attended by a range of stakeholders from policing, academia, civil society, Parliament, regulators, oversight bodies, and industry.

Lesson 1: We need to ensure AI technology is fit for purpose

51. By "fit for purpose" we mean that AI technology used in policing must at a minimum be:

    (a) a valid method of solving a particular problem or producing a particular output;

    (b) the product of lawful and ethical data, design and development; and

    (c) capable of delivering reliable and accurate performance (i.e., "good enough" performance) in its specific context, with any bias or inaccuracy being tolerable for the intended use.[132]

52. This recognises that a tool can be adequate for one job, but not another. For example, a risk assessment tool may be validated for predicting the risk that a defendant may fail to appear, but will require separate validation for predicting recidivism risk, even if based on the same data.[133] Similarly, a facial recognition tool which is good enough for use on high quality photos may not be good enough to be used on poor quality CCTV footage, because it simply won't perform well enough. Furthermore, a tool may need to be more accurate and reliable based on what the output will be used for, and the consequences attached, for example an AI tool which suggests further lines of investigation, versus using the output as the singular reason someone is subject to police powers, for example stop and search. Finally, it also acknowledges that there may be the potential for high-performing tools to be not fit for purpose because that high performance comes at the cost of legal compliance, for example if a new voice recognition tool was shown to outperform all others, but only if it permanently retained all biometric voice data, which would breach data protection law as well as a disproportionate infringement to the right to privacy.

53. Determining whether an AI tool is fit for purpose therefore is not a simple technical calculation, but a matter of complex judgment, involving ethical, legal, technical, operational and strategic components. What counts as "good enough" depends on several factors. A critical factor is the current reality of the non-AI capabilities to perform a task – in many areas of AI innovation, the reality may be that, without AI, the information does not get reviewed or used at all. Another factor is the importance of that task to policing, especially in fulfilling its positive duties under Articles 2 and 3 of the ECHR. And, crucially, it also depends on how much risk is tolerable if the tool fails. That risk might involve wasting public funds, eroding public trust, infringing data protection or human rights or introducing unreliable information into policing and the wider criminal justice system.

132 See the Forensic Science Regulator's definition of "*fit for purpose*" in the context of method validation in digital forensics: "*Is good enough to do the job it is intended to do as defined by the specification developed from the end-user requirement*." Forensic Science Regulator, 'Method validation in digital forensics (accessible)' (Issue 2, 22 July 2024).

133 Partnership on AI, 'Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System' (August 2021) 14.

54. In England and Wales, there is no clear picture of how police are exercising this complex judgment over what is fit for purpose and we do not know the conclusions that forces are coming to in respect of key questions such as:

    (a) what level of accuracy is needed for the task?

    (b) what bias can be tolerated/mitigated and how?

    (c) what is suitable non-police training data when AI tools are bought off the shelf?

    (d) what police data sets should be used to test the tool?

    (e) how is performance benchmarked?

    (f) who has responsibility for such monitoring?

    (g) in what circumstances is unexplainable AI acceptable and where it is not?

    (h) what quality assurance processes should be in place?

    (i) what level of interference with rights, for example the privacy of individuals, is proportionate?

55. This is in large part due to the 43 territorial force-model of policing which operates in England and Wales. Although this model offers clear advantages, such as enabling individual forces or regional groups to innovate with AI to meet local needs, it currently lacks a reliable infrastructure to ensure consistent standards across the country. Instead, forces may be developing or using AI for similar tasks, but with radically different ideas of what "good enough" means.

56. The groundwork for improved consistency has been laid over the last few years, which has seen the NPCC creating an AI Portfolio, the creation of the Office of the Police Chief Scientific Advisor (**"OPCSA**") in 2021 which hosts a Police Science Council, sets national strategy, administers research funding – the Police STAR fund (Science, Technology, Analysis and Research) – which includes research in AI. In addition, in 2024 the NPCC appointed an AI lead and established the Science and Innovation Committee (SICC), to coordinate between NPCC, the Home Office and the Department for Science, Innovation and Technology ("**DSIT**"), work with the National Science and Innovation Board, as well as provide an audit and assurance role to the STAR fund.

57. Despite all this central work, there is no routine communication between police forces, nor any central knowledge bank which wider society – and other police forces – can consult, to better understand what other police forces are doing with AI, how they are applying the principles, how different forces are approaching the question of what is fit for purpose in particular use contexts, what answers they are arriving at, and how that is then being secured through in house development or procurement.

58. By contrast, standards for forensic science activities are now underpinned by a statutory code of practice, which sets obligatory technical and governance standards for various forensic science activities involved in criminal investigations or criminal proceedings.[134] However, most AI used by the police in England and Wales is not within the Forensic Science Regulator's remit. A lot of AI tools are not used during a criminal investigation, but rather in wider policing activities, such as intelligence gathering, safeguarding, community engagement and public safety. Meanwhile, AI tools which may be used in the course of an investigation are mostly excluded from the Forensic Science Regulator's remit and the code - facial recognition systems are excluded,[135] as are transcriptions from audio, by generative AI or any other method.[136] One exception seems to be digital forensics involving AI, which would have to meet the standards set out in the statutory code of practice, including method validation.

134 Forensic Science Regulator, 'Forensic science activities: statutory code of practice' (Home Office, 27 April 2023).
135 Ibid, section. 73.5.1(d).
136 ibid, section 87 FSA DIG 401.

59. Stakeholders we spoke to raised the following concerns about this current reality.

60. **Efficiency:** As the 2023 Policing Productivity Review recognised, it "*significantly hamper[s] better policing productivity*" when there is an "*unnecessary divergence of approach among forces to essentially common activities - along with a failure to adopt and share good practice where it is plainly evident and implementable*."[137] There is clearly an opportunity to rationalise resources and stop inefficiencies which are a result of 43 police forces wrestling with the same problems. Similarly, others raised the risk of missed opportunities by some forces, who may not have the same in-house technical expertise, or time and resources to convene external experts, as others. If knowledge were shared, they would benefit from the responsible innovations of other forces, rather than missing out.[138]

61. **Ineffective procurement:** Others also warned that when the policing sector is not collectively establishing what is fit for purpose from AI tools for particular contexts, that gap is easily filled by the private sector,[139] resulting in a missed opportunity for policing to be able to dictate their need as a customer. The risk lies in private developers making key design decisions tailored to what is most commercially viable for them, rather than specifications reflecting the requirements for the policing use context and incorporating police forces' legal duties (duties which are not delegable to the private sector, e.g. their public sector equality duty and their human rights duties).[140] For example, we are aware of commercial providers offering free trials and pre-setting technical thresholds for those trials, such as the level of confidence required for a transcription tool to produce a word for a portion of audio, as opposed to declaring audio "inaudible". This may be done without consideration of the legal context of its use in policing, and therefore without thought as to whether a higher level of confidence would be needed for some outputs than others – like PACE interviews.[141] A failure of policing to set standards for design and performance proactively will therefore mean the private sector will promote fitness for purpose on its own terms. For example, the private sector is not incentivised to be open with all the details of their products, due to incentives to protect commercially sensitive assets such as their training data sets. Nor are they incentivised to draw attention to the limitations of their tools, or to incorporate confidence scores to highlight the level of uncertainty in their outputs. As such, there was wide acknowledgement by many we spoke to of the risk of relying on the private companies who are selling nationwide to be the primary driver of national consistency on standards, rather than the police speaking with one voice on the standards expected.

62. **Risk of unfit technologies infringing rights:** Recent reports have identified that biometric technologies are being developed to perform a wider variety of functions beyond their current mainstream use of identification, including so called "emotion recognition". [142] The suggested function of these tools is that they will be able to recognise the emotions of an individual by analysing their facial expressions. This is known as "inferential" AI, purporting to be able to infer psychological information – i.e. someone's emotional state - from physiological traits.[143] Concerns about such tools are familiar to those surrounding polygraph use. Use of the polygraph by police persists outside of criminal

137 Home Office,' Policing Productivity Review' (November 2023)
138 The most recent NAO report published in November 2025 highlighted the "*lack of standardisation across the 43 forces and absence of collective decision-making has discouraged the adoption of new technologies, led to duplication of working practices and weakened forces' negotiating position with suppliers*". National Audit Office, *Police productivity* HC 1380 (3 November 2025).
139 Stakeholders highlighted the extent of commercial sponsorship of policing technology conferences and articles in policing publications being written regularly by commercial providers
140 See JUSTICE, 'Beyond the Blame Game: a responsible and rights-centred approach to government contracting' (2024)
141 Interviews conducted under the Police and Criminal Evidence act 1984.
142 Sam Stockwell, Megan Hughes, Carolyn Ashurst and Nóra Ní Loideáin, 'The Future of Biometric Technology for Policing and Law Enforcement' (Centre for Emerging Technology and Security, Alan Turing Institute, March 2024).
143 Kyriakos N Kotsoglou and Marion Oswald, 'Falling Behind the Pace: Lie Detectors, Policing and Lack of Foresight' (Northumbria University, 2023).

proceedings (in which it is inadmissible) despite the widely contested scientific validity of what it claims to do – to infer psychological deceptiveness from physiological information. Of particular concern are the non-statutory uses of polygraphs which occur opaquely, under police general common law powers, with recent academic research based on FOIs highlighting the lack of information, standards or policies guiding such use.[144] Such tools directly interfere with the right to privacy and bodily autonomy of the individual[145] by processing their biometric information, yet it is difficult to see how the use of such tools is not arbitrary, unnecessary and disproportionate given the lack of basic scientific consensus on validity, and the opacity of use outside any explicit legal framework. The risk of such rights-infringing technology going unidentified is compounded when its use occurs in silos, with no obligatory transparency requirements nor any technical standards.

63. **Trustworthiness:** Home Office[146], CeTAS[147] and CENTRIC[148] recent public attitudes reports on police use of AI all identify a consistent message from the public: they do not oppose police use of AI, but they are not willing to write a blank cheque. They want to know the technology is accurate and fair just as much as they want to know about any privacy intrusion;[149] they want to know the technology used is held to the same standards all over the country;[150] and they want to know the police are accountable for the AI tools they choose to use.[151] Notably, in CENTRIC's recent consultation of 10,114 members of the UK public, "*75.5% of the public wanted a mandatory accountability process, **before the police deploy AI**; while less than 20% of the public currently see AI accountability in policing as sufficiently established.*"[152]

64. As we explained above, there have been attempts already to improve consistency, one of the outputs being the identification of key principles. Principles in Government policy[153] and international treaties[154] have been explicitly adopted in the policing context to form the NPCC's AI Covenant in 2023,[155] and its Police Industry Charter to which the private sector can commit.[156] This year, there has been further work to build on those principles and distil them into facilitative guidance to help police forces to apply them in different contexts, namely in the NPCC's 2025 "*AI Playbook*",[157] incorporating the Probable Futures "*AI checklist*" created by researchers,[158] and College of Policing's Guidance on building AI-enabled tools and systems.[159]

65. However, thereafter forces are on their own, with there being no central resource of assistance to help those who want to innovate responsibly but need additional expertise. Nor is there assistance or knowledge sharing of what "good" looks like, despite the significant legal and ethical judgments made in such processes.

66. Some forces have introduced specialise data and technology ethics committees to help them innovate responsibly, a model

144 Ibid.
145 *Convention for the Protection of Human Rights and Fundamental Freedoms* (European Convention on Human Rights, as amended) art 8.
146 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025).
147 Rosamund Powell, Marion Oswald and Ardi Janjeva, 'UK Public Attitudes to National Security Data Processing: Assessing Human and Machine Intrusion' (CeTAS: Centre for Emerging Technology and Security, Alan Turing Institute, April 2025).
148 CENTRIC "Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime" Research, 'Citizen Consultation on the Police Use of Artificial Intelligence (AI) in the UK: Acceptance, Trust and Accountability' (October 2025).
149 Key finding 11, Rosamund Powell, Marion Oswald and Ardi Janjeva, 'UK Public Attitudes to National Security Data Processing: Assessing Human and Machine Intrusion' (Centre for Emerging Technology and Security, Alan Turing Institute, April 2025).
150 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025).
151 All – accountability was a central finding of CENTRIC and Home Office reports, and independent oversight highlighted as a key determinant of trust in CeTAS.
152 Our emphasis. CENTRIC "Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime" Research, 'Citizen Consultation on the Police Use of Artificial Intelligence (AI) in the UK: Acceptance, Trust and Accountability' (October 2025), 24.
153 Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation: Amended Government Response' (February 2024).
154 OECD, 'Recommendation of the Council on Artificial Intelligence' (2019) upon which UK government largely based its principles.
155 NPCC, 'Covenant for Using AI in Policing' (September 2023)
156 BlueLight Commercial, NPCC, APCC, the Home Office and the OPCSA, 'The Police Industry Charter' (March 2024)
157 NPCC AI Portfolio, 'Artificial Intelligence (AI) Playbook for Policing' (April 2025).
158 Marion Oswald, Muffy Calder, Claire Paterson-Young and Jennifer Dunkwu, 'PROBabLE Futures and NPCC Responsible AI Checklist for Policing', (May 2025).
159 College of Policing, 'Building AI-enabled tools and systems' (Guidance, 17 June 2025).

spearheaded by the West Midlands Police and its Police and Crime Commissioner. Discussed later in this paper for their value as an oversight body as well as a method of community participation, these data and technology ethics committees have contributed positively to the validity and responsibility of policing AI and supported operational policing, helping to develop understanding within the police of key ethical, scientific, legal and operational issues for planning and implementation.[160] However, specialist data and technology ethics committees are by no means common place, leading to wide variance in the processes forces are using to decide what AI to use in what contexts, and the level of engagement with independent experts and local communities in helping them answer those questions.

67. As of this year each police force has guidance and checklists to help the think about the key questions involved, but even this common guidance risks forces separately finding their own, potentially contradictory, definition of "fit for purpose" while others are missing out, because they simply do not have capacity or capabilities to reach the answers on their own from scratch.

160 Marion Oswald, Claire Paterson-Young, Pauline McBride, Michael Maher, Muffy Calder, Gitanjali Gill, Elizabeth Tiarks and William Noble, 'Ethical review to support Responsible Artificial Intelligence (AI) in policing: A preliminary study of West Midlands Police's specialist data ethics review committee' (Northumbria University Research Portal, 11 September 2024).



68. We therefore conclude that policing needs a central function to:

(a) Take responsibility for developing standards and benchmarks for what is "fit for purpose" for specific tools in specific use cases.

(b) Support local innovators on the ethics and legal implications of new technologies and whether they are good enough for particular contexts.

(c) Make it easier for police forces to incorporate these standards into local innovation, by providing centralised testing.

(d) Embed these standards into procurement to help communicate what is expected in terms of technical standards, responsibility and liability for those standards, and for ongoing monitoring and evaluation, to the private sector.

(e) Make clearly established standards for tools mandatory, thereby preventing the adoption of unfit for purpose and rights-infringing technologies, protecting the public and providing a legitimate basis for their trust.

69. Whilst we have concluded that the current system requires more central coherence, we stress that the aim should not be to quell local innovation, but to support it. Common minimum standards, and central resources for advice, review of assessments and checklists, and testing of tools against standardised data sets**,** will ensure forces who want to innovate can do so with confidence. It will still leave plenty of room for local adaptations, but those local differences can be depended on to be useful and purposeful, rather than preventable differences in quality or legality. And critically, we believe creating such an infrastructure will support trustworthiness. It will demonstrate that taxpayers' money is being spent efficiently on innovating with AI, and that any AI used by the police in a community is held to the same standard as that used anywhere else in England and Wales.

Lesson 2: We need to ensure AI technology is used competently, ethically and lawfully

70. Even if a tool is fit for purpose, it still needs to be used in a deployment environment which supports the competent, ethical and lawful use. This means:

(a) ensuring the humans using and overseeing AI tools can act competently and ethically; and

(b) ensuring lawful action through legal clarity.

Ensuring humans use AI competently and ethically

71. Our examples in Chapter 2 evidence the importance of human operators of AI understanding the limitations of tools, and the fallacy of expecting adequate human oversight if those people cannot interpret the output or alternatively verify it.

72. We further identified the following issues in consultation with stakeholders:

73. **Training, digital literacy and communicating limitations:** We heard concerns that there was no mandatory training for those operating AI systems, nor accreditation systems (with the exception of anyone using AI as part of digital forensics activities).[161] The Justice and Home Affairs Committee in 2022 recommended "*mandatory training for officers and officials using advanced technologies*" to include "*both generic data analytics and specificities of the particular technology in question.*"[162] Consultees were particularly concerned with the communication of any identified limitations of an AI tool, in a procurement or a development process, not making it through to the "*front line*". Stakeholders we spoke to also stressed that even the language used can be powerful: when referring to predictive AI which learns from past data, this could be referred to as "lead suggesters" rather than

161 For which the UK Accreditation Service tests the competence of staff, alongside the equipment, facilities and methods of a particular forensics environment, including digital forensics, for compliance with ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories'*. Forensic Science Regulator, *Code of Practice* (Version 2, May 2025), section 82.2.1; see also UKAS website.

162 The Committee were "unconvinced" by the argument that training could only be effective after tools had been "settled down," developed and consistently deployed. House of Lords Justice and Home Affairs Committee, 'Technology Rules? The advent of new technologies in the justice system', 1st Report of Session 2021–22, HL Paper 180 (2022), 53–54.

"AI" or "predictive technology" which may inspire over trust and make automation bias more likely.

74. **Responsibility distribution:** At the same time, many stakeholders stressed to us that systems which expect police officers to be computer scientists will fail. Those using a tool and providing a "*human oversight*" role are only one part of an overall quality assurance system, and they alone are unlikely to be able to spot issues which are baked into the way in which the AI tool has been designed or developed. For example, an officer overseeing individual recommendations of a risk prediction tool cannot identify systemic bias in the data, nor be expected to be a safeguard alone against discriminatory outputs. Instead, responsibility needs to be spread, with mandatory quality assurance systems upstream and ongoing monitoring and evaluation downstream. One developer explained to us: "*if you're not careful, your human over the loop quite easily becomes your human scapegoat for poorly designed systems.*"[163]

75. **Siloed understanding of what works:** as explained in the above section, there is no clear picture of how police are tackling the challenge of creating safe and fair deployment environments for particular AI tools used in particular circumstances. Nor is there a mechanism through which forces can share learning of what works.

76. **Counter-incentives for quality control of "efficiency AI":** in respect of AI tools used to reduce the amount of time spent on administrative tasks (such as redaction, summarisation, drafting and transcription tools) many highlighted a fundamental contradiction: that adequate human oversight of the outputs of such tools may detract from the time saved and therefore undermine the exact purpose of their use. While the quality of human oversight can be an acceptable trade off in lower risk environments, documents which will have any significant impact on a criminal investigation, the deployment of officers, or indeed any decision-making which will impact the rights of individuals, may require a higher quality of oversight.

77. Appropriate training and cultures which empower police to scrutinise AI outputs clearly have a role to play in the successful adoption of AI. In particular, digital literacy is a baseline competency, and ongoing research and development into training strategies, and sharing what works, is necessary. But training cannot alone support the successful deployment of AI unless other safeguards are also baked in upstream. For example, training users to be critical and adopt a sceptical approach will be of limited impact if a police officer cannot understand the predictions made by a tool or how they have been produced, because that information is proprietary. And when limitations and uncertainties are known, research into creating successful user interfaces is crucial, so those uncertainties are effectively communicated at the right time within a decision-making process.[164]

78. Therefore, quality human oversight is essential, as well as being dependent on other elements of a well-functioning quality assurance system. Learning through local innovations what quality assurance systems are effective and proportionate, for what tools, used in what circumstances, is a strength of the current policing model, but only when that learning can be shared, and contribute towards common standards, rather than lead to inconsistencies, missed opportunities and repeated mistakes.

79. Alongside technical standards, we therefore think that there should be a central function which proactively coordinates such learning, and distils it into quality assurance standards, specific to the tool and its use. This mirrors the approach of the Forensic

163 Interview with developer, 29 October 2025

164 For example, in the field of cognitive engineering, taking a human-centred approach to design and evaluation of user interfaces. See Sam Hepenstal, 'Towards Socio-Technical Evaluation for Artificial Intelligence in Policing' in Helmut Degen and Stavroula Ntoa (eds), *Artificial Intelligence in HCI* (Lecture Notes in Computer Science vol 15819, Springer 2025); Sam Hepenstal, Leishi Zhang, Neesha Kodagoda and B L William Wong, 'Developing Conversational Agents for Use in Criminal Investigations' (2021) 11(3–4) ACM Transactions on Interactive Intelligent Systems 1–35; Sam Hepenstal, Leishi Zhang and B L William Wong, 'The Impact of System Transparency on Analytical Reasoning' in 'Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems' (ACM 2023).

Science Regulator, whose code of practice sets standards for quality management systems, i.e. the processes and environments surrounding tools, including accreditation where appropriate for those operating the tool, as well as technical standards for the tools themselves. This will give assurance to those forces wanting to adopt systems with confidence, without having to start from scratch in thinking about how to create safe deployment environments, and provide reassurance to the public that similar quality management applies to similar AI tools, wherever they happen to live.

Ensuring legal clarity

80. A further significant barrier to ensuring AI is used lawfully is the challenge of actually understanding what use of AI is "lawful", and what is not. This challenge stems from our current legal framework, which does not feature specific legislative instruments or legal frameworks for the use of AI in policing. This contrasts most starkly with the approach of the European Union, which has passed an AI-specific overarching legal framework.

81. This is not to say AI is used in a legal vacuum. There are legal frameworks which will often be relevant to police AI use: data protection law,[165] the Human Rights Act 1998, the Equality Act 2010, all of which protect the rights of individuals against state intrusion, subject in some circumstances to such intrusion being in accordance with the law, in pursuit of a legitimate aim, and a necessary and proportionate means of achieving that aim. There are also specific laws which impose legal limits and requirements on how the police exercise their powers, including for example the Police and Criminal Evidence Act 1984 and its statutory codes of practice, the Regulation of Investigatory Powers Act 2000, and the Police (Conduct) Regulations 2020.

82. As discussed briefly in the previous Chapter, this patchwork of laws has been examined by the courts in *R (Bridges) v Chief Constable of South Wales Police.*[166] It was found to be *capable* of supporting legal deployment, but not alone. The court found that without further detail through police policies, it was inadequate. We consider the current legal patchwork approach, for this reason and others, poses a threat to the rule of law, as follows.

83. **Foreseeability and arbitrariness**: Much policing use of AI will engage the human rights of individuals, whether it is processing their private data, conducting surveillance of their behaviour in public places, using AI outputs to inform the exercise of police powers (decisions which affect people's safety, liberty, or their equal treatment by the state), or indeed using AI to analyse or produce evidence for use in criminal proceedings, impacting their right to a fair trial and the fair administration of justice. Where interference with individuals' rights is permitted this must be "*in accordance with the law*".[167] This requirement cannot be understood separately from the concept of arbitrariness, foundational to the rule of law. Protection from arbitrariness not only prohibits the exercise of state power without legal basis, but it also means that when there is a legal basis, it cannot be so broad or abstract as to make how it will be exercised in practice unknowable. Rather, the law must "*indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise*".[168] These requirements are a safeguard against arbitrariness, since they enable individuals to identify unlawful interferences with their rights. In *Bridges*, the Court of Appeal found that the legal frameworks governing the use of live facial recognition technology were not sufficiently clear on their own, and required additional policy documents from police forces to provide clarity on the manner of the discretion of the power; specifically,

165 Including the the UK GDPR, Privacy and Electronic Communications Regulations, the Data Protection Act 2018, as updated by the Data (Use and Access) Act 2025.
166 EWCA Civ 1058
167 It must also pursue a legitimate aim and be necessary and proportionate to that aim.
168 *S and Marper v United Kingdom* (2009) 48 EHRR 50, [95].

who can be placed on the watchlist for live facial recognition, and the criteria for determining where it would be deployed.[169] Doing so through policy documents is not, on the face of it, a problem with regards to the legal test. However, the Ada Lovelace Institute suggests such post-*Bridges* polices have not adequately met the test of "foreseeability", resulting in a risk of arbitrariness persisting.[170] It further concludes that the current "*fragmented patchwork of voluntary guidance, principles, standards and other frameworks*" is "*inadequate in practice, creating legal uncertainty, putting fundamental rights at risk and undermining public trust*."[171]

84. **Equality before the law:** *Bridges* confirmed that human rights compliance in the deployment of live facial recognition – and by implication other rights-interfering AI systems – requires specificity as to who it would be used on and where and when it would be used. It also confirmed in line with established case law that a police force policy document is an adequate mechanism for giving that additional detail. However, the court was not tasked with deciding whether, in the future, a landscape of force-led policies applying different watchlist and deployment criteria, was lawful or indeed desirable – its remit was only to adjudicate on the legality of the use by South Wales Police. However, we think such a future landscape *is highly* undesirable. While facial recognition adoption has so far been spearheaded by two forces – South Wales Police and the Metropolitan Police – announcements this year have signalled a far wider rollout funded by the Home Office.[172] Post-*Bridges* guidance from the College of Policing provides some consistency,[173] but the critical detail – of who can be on a watchlist and where and when deployments can occur – is left to local forces. Without an effort to ensure national consistency, we are concerned this will lead to inequalities between force areas. Equality before the law is a principle which entitles everyone to the equal protection of the law, and is reflected in the prohibition of discrimination in the enjoyment of rights.[174] Equality before the law does not demand detailed and inflexible proscribed use of every AI tool, but it cannot allow for completely inconsistent interpretations by different police forces. However, this is a risk which appears to be hardwired into the current legal framework.

85. Furthermore, our discussion of various AI use cases elucidated additional questions of legal clarity in several additional areas, underlining the fact that legal clarity is not a problem exclusive to live facial recognition, or indeed biometrics.

    (a) **Predictive technologies:** there is a legal requirement for "*reasonable*" suspicion in exercising police powers such as stop and search, arrest, search, seizure,[175] which interfere with right to liberty,[176] the right to privacy and bodily autonomy,[177] and the right to peaceful enjoyment of property.[178] However, what is "*reasonable*" in the context of algorithmic prediction is unclear. Can predictions based on past group data ever be "*reasonable*", since generalisations and suspicions are usually prohibited[179] and reasonable suspicion normally requires some sort of individualised suspicion? We note AI systems used by police to predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics, are banned in EU AI Act. We consider the role of group-level data in making decisions about

169 *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [91].
170 Nuala Polo, Jacob Ohrvik-Stott, 'An Eye on the Future' *Ada Lovelace Institute* (May 2025)
171 Ada Lovelace Institute, 'Mass facial recognition roll-out exists in 'legal grey area' due to inadequate governance' (Press release, 29 May 2025).
172 Home Office, 'Live Facial Recognition technology to catch high-harm offenders' (News release, 13 August 2025).
173 College of Policing, 'Live Facial Recognition' March 22, 2022.
174 Article 14 ECHR which ensures individuals can enjoy the protection of rights without discrimination based on grounds like personal characteristics, social or political associations, or other status.
175 The Police and Criminal Evidence Act 1984, Parts I-III.
176 Article 5 ECHR.
177 Article 8 ECHR.
178 Article 1 Protocol 1 ECHR.
179 See PACE Code A on Stop and search, para 2.2B which prohibits "*Generalisations or stereotypical images that certain groups or categories of people are more likely to be involved in criminal activity*" as well as basing suspicion on protected characteristics in the Equality Act 2010.

individuals is a complex and important issue which must be clarified legally.

(b) **Surveillance technologies:** potential use of surveillance technologies other than live facial recognition have received very little scrutiny, including social media surveillance, often referred to as an "OSINT" activity.[180] We are aware of AI in development by police which aims to use online traces including social media posts and interactions to identify someone and/or predict their movements and behaviours. However, legal academics we consulted highlighted a lack of clarity in whether such surveillance needed a directed surveillance authority under Regulation of Investigatory Powers Act 2000,[181] both in terms of how covert this surveillance is and when it counts as being outside of a pre-planned investigation or operation. Again, this seems to us to be an area in which legal clarity is required.

(c) **Transcriptions:** there is currently no clarity on whether AI can be used to transcribe interviews into the forms used in criminal proceedings, known as Records of Taped/Video Interview ("**ROTI**" / "**ROVI**"). There are surprisingly no rules on transcription currently, but there is space for them in PACE Code C (treatment during police suspect interview) and Codes E and F (audio and video recordings).[182] This is an area of important clarification, given the potential impact on the fair administration of justice and defendant's absolute right to a fair trial. We think clarity is required in terms of whether AI transcription is allowed, and if so what record-keeping processes should accompany it, whether it has to be declared, what defence access there should be to master recordings, and whether all versions (for example an initial transcription which includes an error which is then corrected) form part of the unused material.

86. We are not satisfied that legal clarity will be achieved by a piecemeal, force-by-force-issued policy document approach. Nor are we persuaded that waiting for such areas to be litigated is a desirable approach. It relies on access to litigation which can be prohibitively expensive, and is in any event a poor mechanism to achieve legal clarity in a fast-moving area of police technology adoption – litigation can span years, and will inevitably focus on the facts of one case. Instead, a proactive approach would engage with police and wider society – including academics, civil society, regulators, interested groups, and the general public – to identify legal ambiguity, and lead democratic processes which resolve such ambiguity and provide clarity. We also acknowledge, here and in the next Chapter, the need for rulemaking to keep pace with technology. Primary legislation is slow and will not always be the best instrument to make clarifications. But updates to secondary legislation or statutory codes of practice – or indeed non-binding guidance materials – are quicker *because* they are not subject to anywhere near the same level of scrutiny. In meeting the need of legal clarity, the balance must be struck between flexibility and speed to ensure legal clarity keeps pace with technological advancements, and the need for the law to be a result of a democratic process.

87. We also acknowledge, here and in the next Chapter, the need for rulemaking to keep pace with technology. Primary legislation is slow and will not always be the best instrument to make clarifications. But updates to secondary legislation or statutory codes of practice – or indeed non-binding guidance materials – are quicker because they are not subject to anywhere near the same level of scrutiny. In meeting the need of legal clarity, the balance must be struck between flexibility and speed to ensure legal clarity keeps pace with technological advancements, and the need for the law to be a result of a democratic process.

88. Primary legislation should be used for comprehensive new legal frameworks in which powers or principles need to be newly created or would benefit from being comprehensively clarified or codified.

180 Open Source Intelligence.
181 Section 28.
182 See Kate Haworth, *Written evidence to the House of Lords Public Services Committee Police Transcription Inquiry* (POL0004, August 2025).

Otherwise we consider that legal clarity can be delivered through updates to codes of practice. However, the recommendations relating to ongoing public participation (below) are indispensable if delegated legislation is used and therefore new rules have not benefit from full Parliamentary debate and scrutiny.

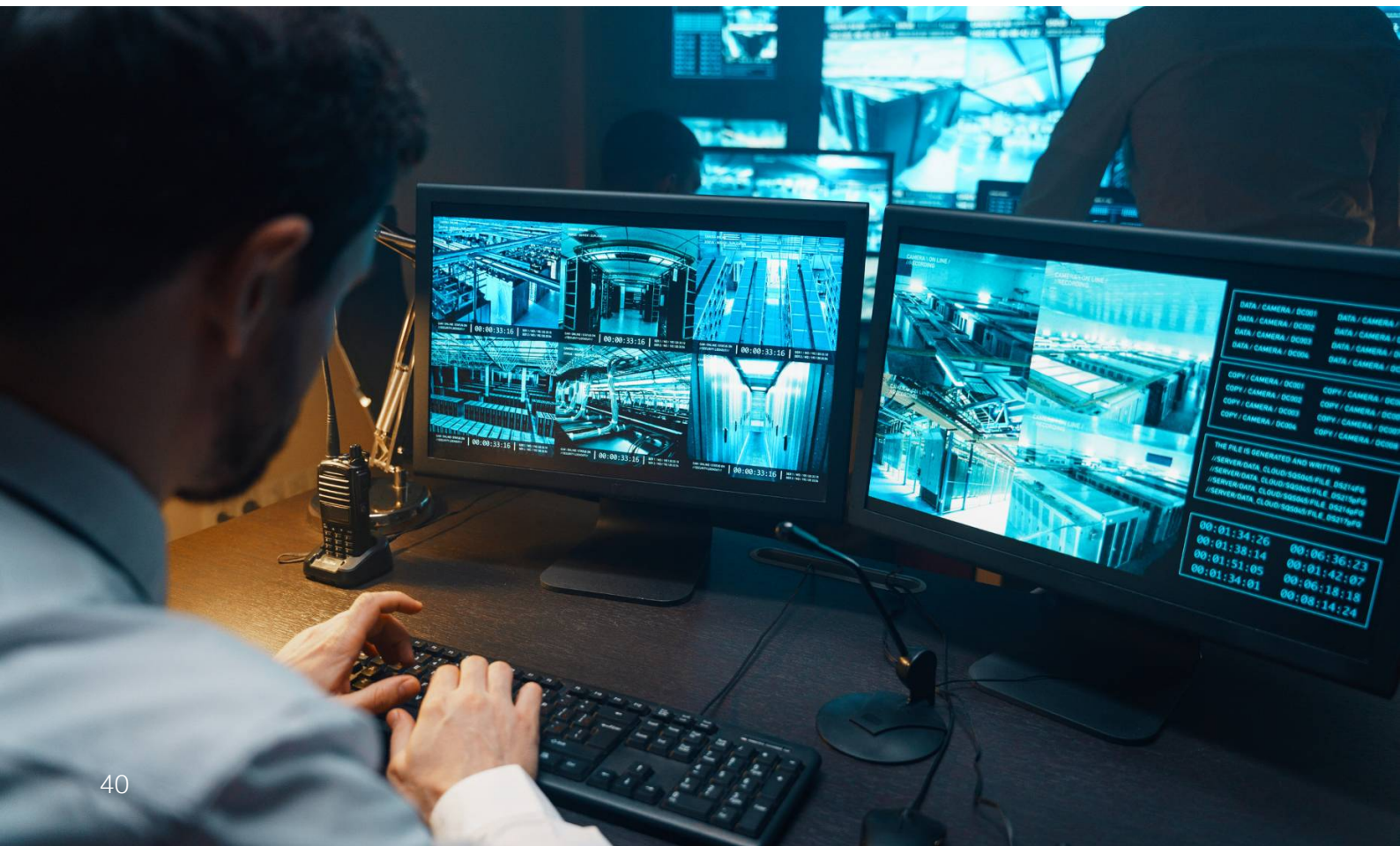
Lesson 3: We need to understand how AI technology is impacting people and systems around it

89. Testing and evaluation pre-deployment will form part of considering whether a tool is "*fit for purpose*". Understanding how AI actually performs once deployed is a separate and essential task. It involves assessing whether the tool achieves its intended impact, identifying any unintended consequences, and examining its broader effects beyond the immediate deployment environment. Stakeholders we consulted described this as taking AI "*out of the lab*" and "*into the wild*" and highlighted the importance of robust scrutiny to ensure quality outcomes, diverse perspectives, and the accountability of policing AI to the public.

90. Key issues highlighted included:

91. **Commercial design limiting what can be evaluated:** to test whether a tool is having the impact intended, this will often require performance metrics and data to be identified during design and development, so that their collection can be embedded into the design of the model. Consultees expressed concern about the design of tools being primarily established by the commercial provider of technologies to demonstrate beneficial impacts and further market the tool, rather than the design of tools being informed by policing need, legal requirements or what the public want to see. An English police officer we spoke with noted that cost-benefit analyses for AI and data services from private third parties were mostly "*opaque*." Impact was demonstrated through case studies rather than comprehensive evaluations, and police forces were not undertaking comprehensive cost benefit analyses themselves due to limited capacity and expertise.[183]

183 Anonymous officer, discussion with author, August 2025.



92. **Productivity incentives as a barrier:** productivity is a clear driver for adoption of AI in policing, however some noted this could produce a "fear of failure" in face of huge central drive for efficiency. We are concerned that this efficiency-driven culture risks disincentivising full evaluation of any trade-offs in that efficiency, including any unintended consequences which may undermine any benefit.

93. **Absence of support for impact evaluations:** While there is guidance which stresses the importance of ongoing monitoring and evaluations,[184] there are no services which can support individual forces with getting their evaluations right. Nor are there clear governance and data standards for evaluation purposes - for example what data should be retained, in what format and accessible to whom. As with substantive technical standards above, this is left to each force to determine, with significant risk of inconsistency.

94. **Routes in for independent research:** There are established partnerships between universities and police forces, which enable collaborative work between police forces and academia, for example through the Forensic Capability Network.[185] The OPCSA has also recently announced nine Policing Academic Centres of Excellence (**"P-ACEs"**) to drive collaboration between policing and academia. However, civil society and academic researchers told us it is often very difficult to conduct research outside these collaborations, and for new researchers and civil society organisations to get a "way in".

    (a) The initial barrier is, as we have explained above, that there is no central repository to find out what, where and how AI tools are being used in the first place. Such a central resource should include information about the tool as well as monitoring information, to assist independent research and audits.

    (b) For more sensitive data, there are different research access arrangements applicable across the country, and a lack of a standardised processes for independent researchers to submit proposals, have them reviewed (including independent review e.g. from ethics committee), obtain data access and publish findings.

    (c) It would also be beneficial if researchers were granted access to tools themselves, rather than only the monitoring data. There are well-documented issues with researcher access to major foundation models, upon which generative AI tools used in policing may be built, with ongoing calls for safe controlled access for good-faith researchers.[186]

95. **Multidisciplinary effort needed for difficult evaluations**: we identified that some questions of impact posed by AI require a variety of perspectives and disciplines, and which therefore would benefit from wide expertise. For example, live facial recognition technology is often accompanied by concerns about a "*chilling effect*" on freedom of expression, freedom of assembly and freedom of manifestation of belief, all protected human rights.[187] How any such chilling effect can be measured however is unclear, and would benefit from multidisciplinary research efforts to develop a methodology and help support some attempt to capture the impact, rather than it simply being missed.

96. **Siloed learning**: Again, we identified concerns about 43 different police forces conducting evaluations on different aspects, and learning from their experience but not consolidating that learning anywhere. We identified this as a missed opportunity to share known impacts of AI tools, failings and successes. This includes failures and successes during academic collaborations too. For example, we are aware that getting data sharing agreements in place is very time consuming for academic and policing

184 Marion Oswald, Muffy Calder, Claire Paterson-Young and Jennifer Dunkwu, 'PROBabLE Futures and NPCC Responsible AI Checklist for Policing', (May 2025); College of Policing, 'Building AI-enabled tools and systems' (17 June 2025).
185 Forensic Capability Network, 'Research and Innovation'.
186 Kevin Klyman, Shayne Longpre, Sayash Kapoor, Rishi Bommasani, Percy Liang and Peter Henderson, 'Safeguarding Third-Party AI Research' (Stanford Institute for Human-Centered Artificial Intelligence, Policy Brief, February 2025).
187 Articles 9, 10 and 11 of the ECHR.

partnerships – sharing templates of such documents for others to use was suggested as an easy win which could save significant time and promote confident data sharing.

97. **Disaggregated regulation**: other actors conducting a form of impact evaluation are regulators, since some have the power to conduct audits or conduct inspections of different aspects of policing against their particular areas of concern, including Police and Crime Commissioners, national police oversight bodies (His Majesty's Inspectorate of Constabularies, Fire and Rescue Services ("**HMICFRS**"); The Independent Office of Police Conduct ("**IOPC**")) and cross sector regulators (the Information Commissioner's Office ("**ICO**"). As AI adoption increases, there will be a need to ensure oversight bodies, including regulators have the adequate powers, remit and capacity to perform the evaluations required as part of their oversight function. (See further in Lesson 4 below).

98. **Beyond immediate impacts:** work on understanding the impact of police use of AI on other criminal justice actors and processes downstream is nascent. The impact of several, chained AI processes is part of a multi-year research project, PROBabLE Futures, funded by UKRI. Meanwhile, we understand that the NPCC and the CPS have developed joint operating procedures this year, which require police to notify CPS when they are using AI tools. This needs to be the start of ongoing evaluation and collaboration between actors across the criminal justice system, to consider how the police use of AI may impact criminal proceedings, including their timeliness, transparency and fairness. For example, the use of AI may necessitate changes to disclosure and access to experts.

99. **The public want transparency about system impact:** The public's support for the police's use of AI is conditional on evaluation. They want to see auditing of data for bias, they want continuous performance monitoring, and they want to see evidence of positive impact of AI efficiency by seeing resources saved applied elsewhere, such as greater community engagement and frontline policing.[188]

100. To understand impact, therefore, it is clear there are two levels of evaluation which need to be secured:

    (a) We need police to evaluate impact of the AI they deploy. This cannot be optional, but is rather an essential part of responsible AI use. Procurement or outsourcing arrangements with the private sector cannot be a barrier to this, but rather contracts need to be used to ensure clarity in terms of i) access to data, ii) retention of system information in auditable formats, e.g. error logs, and iii) who has responsibility for ongoing evaluation and monitoring.

    (b) However, we cannot rely on police to ask all the questions which need to be asked and conduct all the evaluations which need to be conducted. They should check their homework, but it is not up to them alone to mark it. This would waste the research insight and capacity of academia and civil society, it would undermine public trust, and it would lack a wider consideration of system-impact which is essential.

101. To secure this wider level of independent evaluation, we need to promote openness to academic research of police AI on a local and national level. Meanwhile, we need a central ongoing programme of performance evaluation in operational environments for the most commonly used AI tools[189].

Lesson 4: We need proportionate and effective safeguards

102. Several research reports into public attitudes to AI in policing have highlighted that accountability is essential for public trust:

    (a) CENTRIC's consultation of c.10,000 people found monitoring by an independent oversight body is expected whenever police deploy AI, not just in contexts of low public acceptance or

188 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025), 7-8.

189 Unlike the one-off approach taken so far, with only one such evaluations having taken place by the National Physicial Laboratory. See Tony Mansfield, 'Facial Recognition Technology in Law Enforcement Equitability Study' (*National Physicial Laboratory*, 2023).

low trust towards AI use by police. They further found that close monitoring, and knowing the police will be held to account, are the most effective measures to promote public trust.[190]

(b) The public participating in the Home Office's deliberative workshops delivered a strong message on accountability: the public should be made aware of how oversight works, who is involved, and what happens when something goes wrong; they want human oversight, continuous monitoring, high levels of data security, limited political involvement, and national consistency in accountability rather than each police force having their own approach. They also want consequences for failure, transparency when failures occur, and clear consequences for misuse.[191]

103. Our examples in Chapter 2 demonstrate that there is a wide variety of safeguards, the key variables being:

(a) **Advance or retrospective:** advance safeguards are positioned before harm occurs, to proactively prevent it, for example design features, or governance standards like accreditation, or pre-approval. They can also, or in the alternative, be positioned post-deployment, to secure accountability and oversight, such as complaints processes and inspections.

(b) **Internal or external:** The degree of external involvement can vary, with some safeguards being a matter of self-management, such as internal quality assurance systems, and while others involve an independent body or regulator.

104. Stakeholders stressed to us that what is the right level of oversight, and most appropriate safeguards, will necessarily depend on the level of risk posed to individuals' rights and freedoms, the administration of justice and the safety of the public, which in turn depends on the nature of the AI tool and how it is being used. This therefore demands a risk-based approach, which secures proportionate safeguarding mechanisms to the risk, thereby reducing administrative burden where it is unnecessary, while identifying where regulatory or oversight resources should be concentrated and prioritised. For example, the EU AI Act adopts such a risk-based approach, placing higher burdens on high-risk AI. The most burdensome oversight mechanism – requiring individual judicial approval for individual deployment decisions – is reserved for AI which the Act deems poses the highest risk to human rights while still being permissible – 'real-time' remote biometric identification system in publicly accessible spaces.[192]

105. Applying a risk-based approach to safeguards is easier said than done, however, hampered by the difficulty in assessing the current landscape and the extent to which safeguards are already in place *and are working effectively*. This is due in part to what others have identified as an "*unnecessarily complex*", "*crowded and confusing*" governance landscape for technologies in policing.[193]

106. This landscape already consists of a web of safeguards, from legal and governance standards to external oversight mechanisms like inspections, reports and applications for permission to a regulator. All these mechanisms relate to different types of risk, from different perspectives, and with different challenges to their effectiveness. For example:

(a) Professional conduct has its own regulations, internal complaint and disciplinary procedures, and oversight from the IOPC which has some statutory powers to demand information but is not an enforcement body of police conduct. An independent review published in 2023 identified clear resourcing issues: rising referrals, falling numbers of

190 CENTRIC "Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime" Research, 'Citizen Consultation on the Police Use of Artificial Intelligence (AI) in the UK: Acceptance, Trust and Accountability' (October 2025).

191 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025), 8.

192 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, art 5(3).

193 House of Lords Justice and Home Affairs Committee, 'Technology Rules? The advent of new technologies in the justice system', 1st Report of Session 2021–22, HL Paper 180 (2022), 21.

investigations, and considerable financial pressure.[194] Despite this, current draft legislation is proposing to stretch its oversight to include more public officials exercising police-like powers.[195]The management of personal data comes under data protection law, which imposes internal pre-deployment processes including data protection impact assessments (mandated in primary legislation, unlike equality or human rights assessments). Data protection is regulated by the ICO, which provides proactive guidance as well as having a suite of statutory enforcement powers including inspections and penalties, and even the power to prosecute data offences. Its effectiveness as a regulator is contentious, particularly in relation to its policy not to use fines against the public sector except in the most severe cases, preferring public reprimands.[196]

(b) The protection of equality and human rights is secured by proactive duties in equality and human rights law, including the Public Sector Equality Duty, internal processes including equality impact assessments (human rights impact assessments are less commonplace) and the oversight of the Equality and Human Rights Commission ("**EHRC**"). JUSTICE reported several concerns with the regulatory effectiveness of the EHRC in its 2023 report *The State We're In: Addressing Threats and Challenges to the Rule of Law.*[197] These include its drastically reduced funding since being established, from £70.3 million in 2007 to £17.1 million for the year 2023–24; its limited use of its enforcement powers; and civil society groups calling into question its independence in terms of appointments and funding arrangements.[198]

194 Dr Gillian Fairfield, *Independent review of the Independent Office for Police Conduct* (December 2023) Ss

195 Clauses 9 and 83 of the Public Authorities (Fraud, Error and Recovery) Bill 2025 will increase the remit of the IOPC to fraud investigators from the Public Sector Fraud Authority and the Department for Work and Pensions.

196 See feedback disagreeing with the approach and calling for tougher enforcement in response to the ICO's recent consultation: ICO, 'Summary of responses to our consultation on the revised approach to public sector regulation' (November 2025); see further Open Rights Group, ICO Alternative Report 2023-24 (2024).

197 JUSTICE, The State We're In: Addressing Threats & Challenges to the Rule of Law (September 2023)

198 See for example, former Chair of the EHRC David Isaac's comments, H. Siddique, 'EHRC undermined by pressure to support No 10 agenda, says ex-chair', (The Guardian, 2021), the comments of two former legal director, Richards, 'Former EHRC legal directors call for it to lose independent status amid trans rights row', (The National, 2022) and concerns raised by various civil society organisations as set out in JUSTICE, *The State We're In: Addressing Threats and Challenges to the Rule of Law* (2023), paras 6.61-6.73.

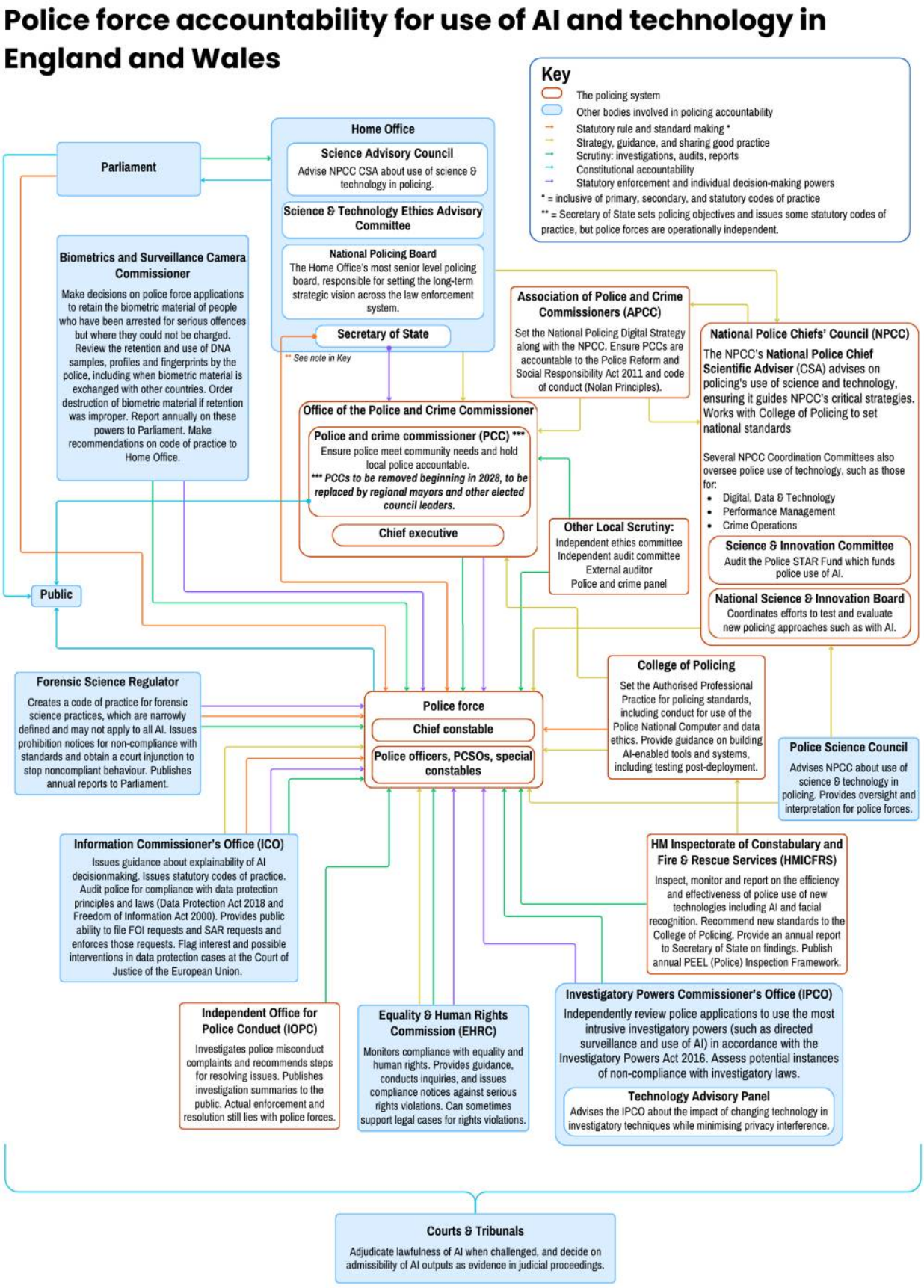


Figure 1: Diagram of governance and accountability arrangements for police use of technology.[199]

199 This diagram is an updated amalgamation of two previous police accountability diagrams, which we credit and by which we were assisted: the diagram in National Audit Office, *Police productivity* (3 November 2025), 14; and that of the Association of Police and Crime Commissioners (APCC), National Police Chiefs' Council (NPCC), and Police Digital Service (PDS) in their Supplementary written evidence (NTL0057) to the House of Lords Justice and Home Affairs Committee, then reproduced in House of Lords Justice and Home Affairs Committee, 'Technology Rules? The advent of new technologies in the justice system', 1st Report of Session 2021–22, HL Paper 180 (2022), 22.

107. This piecemeal approach has arisen over time, not by design, and we consider it inevitable that there will be inconsistencies and gaps, where the existing safeguards will need to be rethought, consolidated, better funded, or expanded. For example, data protection impact assessments are mandatory when there is a high risk to rights and freedoms of individuals, but only for systems in scope of data protection law, i.e. where the risk to rights and freedoms stems from the processing of personal data. There is no commensurate requirement to conduct an assessment of the impact on human rights for AI tools which do not process personal data, even if they pose an equal or higher risk to rights and freedoms, such as generative AI tools used to summarise court statements.

108. A proportionate and effective approach to safeguarding therefore needs leadership to identify gaps proactively, promote regulatory coherence, and respond to emerging technology and evidence. This needs to be included in any new central function for police and AI.

109. After which, gaps should be acted upon. Following our above conclusion – that standards for AI in policing should be mandatory when set by a new central function – there should therefore be consequences if standards are breached. This will ensure the trust of the public, who have been clear that they want to see police accountability, as well as mitigating the damage of unfair and harmful AI tools continuing to be used on the public. We note the standard-setting role of the Forensic Science Regulator is also combined with an enforcement role – he can conduct investigations, issue compliance notices, prohibit activities pending compliance, and apply to court for an injunction.[200] We foresee a future role for the central body therefore not just to set standards, but also to ensure that those standards are effectively overseen and enforced. If gaps are identified, and no other regulator is empowered to enforce them, the central body will need to be given powers to provide that oversight itself – including conducting investigations, audits, issuing compliance notices, and applying for court injunctions.

110. Some additional consideration will also need to be given to the adequacy of existing routes of redress and contestability if harm does occur. Complaint mechanisms, including courts, alone cannot safeguard against unlawful and rights-infringing AI. But as a backstop when other regulatory measures have failed they are an essential mechanism to uphold the rule of law, by providing access to justice, enabling challenge of arbitrary exercise of state power, and access to an effective remedy. However, we are concerned with the adequacy of redress and contestability safeguards in two ways.

111. **Access to challenge (outside of criminal proceedings)**: there are several barriers to people challenging the lawfulness of the police's use of AI.

    (a) Throughout this report we have highlighted the lack of basic information made available to individuals about what AI is used by police and when. This lack of transparency is a fundamental barrier to the contestability of AI in policing – individuals cannot challenge what they do not know. We note that recent data protection law amendments which seek to facilitate the use of automated decision-making in wider data processing, only secure a right to be informed if a decision is solely automated; there is no corresponding right to be informed if AI or other automation has been involved in a decision, even if its influence has been substantial.[201] Therefore there needs to be consideration of a wider right for individuals to be informed when AI has *assisted* in decision-making in their case, from victims whose mobile phones may be analysed by AI, to individuals who have been arrested following identification, when a facial recognition tool has been part of that identification even if combined with witness identification.

200 Sections 5-6 of the Forensic Science Regulator Act 2021
201 Section 80 of the Data (Use and Access) Act 2025

(b) Multiple routes of redress, through police complaint mechanisms, regulators and the courts and tribunals, will likely be confusing for individuals who want to seek redress but do not know where to go. There is a risk that this disproportionately impacts those who are disadvantaged, vulnerable or marginalised, and this confusion leads to them giving up rather than purposing meritorious complaints and claims. JUSTICE strongly advocates in all its work for justice systems to be user-focused, designed around the individual users who need them rather than the professionals and systems which create them. Consideration needs to be given therefore to how individuals can be supported to navigate complaint mechanisms.

(c) Judicial review exists as a last resort to challenge the lawfulness of police AI use, however it is important to recognise the inaccessibility of that action for most. Civil legal aid for judicial review is extremely narrow, and the availability and sustainability of legal aid services have been in decline over the last decade.[202] The reality is that judicial review is simply not an affordable option for most people and therefore it cannot currently be considered a reliable and accessible safeguard to protect an individual's rights. The Ministry of Justice should therefore consider how improvements to legal aid, costs-capping, and other mechanisms can improve the accessibility of judicial review for those who need it as a last resort.

112. **Fair administration of criminal justice:** In the context of a criminal prosecutions, the individual's access to a fair trial is an absolute right and an essential safeguard. This is secured in human rights law,[203] and general principles of common law including the right to have notice of the case against you;[204] to be heard and have the opportunity to respond to the case against you;[205] to have a hearing free from bias;[206] and access to courts.[207] In the US case *New Jersey v Arteaga,* discussed above in Chapter 2, the court considered the defendant needed to be able to test the reliability of the facial recognition technology in order to have a fair trial and mount his defence.[208] The law in England and Wales applies a common law presumption of reliability of computer evidence. This presumption is currently under review following the Post Office-Horizon scandal, which saw unreliable computer evidence go unchallenged, leading to multiple miscarriages of justice.[209] While this review is welcome, it alone is insufficient, as it only considers the evidential law in place and not other factors which may affect a defendant's ability to challenge the reliability of computer evidence in the case. These include access to expert evidence; the adequacy of the current disclosure regime (particularly when AI looks set to be embraced in disclosure itself as an efficiency measure[210]); the accessibility of information held by private third parties;[211] and the role of standards to streamline admissibility decisions. A holistic review of the rules and practices of criminal proceedings – beyond the presumption of reliability for computer-evidence – is required to consider whether they provide adequate access to challenge of AI evidence, and therefore adequate safeguards against miscarriage of justice.

202 Since the introduction of the Legal Aid, Sentencing and Punishment of Offenders Act 2012. See the Westminster Commission on Legal Aid, *Inquiry into the Sustainability and recovery of the legal aid sector*; (October 2021). See also the Law Society's interactive "legal aid deserts" maps in England and Wales.
203 Article 6 ECHR
204 R v Secretary of State for the Home Department ex p Doody [1993] UKHL 8, [1994] 1 AC 531.
205 Ridge v Baldwin [1963] UKHL 2, [1964] AC 40.
206 Dimes v Proprietors of Grand Junction Canal (1852) 3 HL Cas 759, (1852) 10 ER 301.
207 R v Secretary of State for the Home Department ex p Leech (No 2) [1993] EWCA Civ 12, [1994] QB 198.
208 State of New Jersey v Francisco Arteaga, A-3078-21 (NJ Super Ct App Div, 2023), 33.
209 Ministry of Justice, 'Use of evidence generated by software in criminal proceedings: Call for Evidence' (January 2025)
210 See recommendations of 'Disclosure in the Digital Age: the Independent Review of Disclosure and Fraud Offences by Jonathan Fisher KC' (March 2025).
211 The Post Office did not disclose the Horizon error logs in the prosecution of Tracy Falstead, citing they were not in their possession and it would cost them £20,000 to retrieve them from Fujitsu, which they refused to pay and asserted would fall on the defence. As a result, they were not obtained, leading to a serious miscarriages of justice. The error logs were only finally disclosed in the High Court proceedings before Mr. Justice Fraser in 2018. See Paul Marshall, 'Failed Justice –how commercial interests displaced the interests of justice in the Post Office Case', Queen's University Belfast, Institute of Professional Legal Studies, 2022.

Lesson 5: The public should be included at all stages

113. Above we have discussed access to information about AI tools for researchers, including those from academia and civil society. These are only two sub-groups of the wider "public" to be considered when contemplating public participation in AI tools. A wider understanding of the public includes:

    (a) the general public;

    (b) the affected public, for example victims, witnesses, defendants, their families;

    (c) community groups;

    (d) civil society groups;

    (e) academics and researchers; and

    (f) journalists and media.

114. The principle of "*policing by consent*" imposes an expectation of public participation. It recognises the tradition and philosophy which underpin policing in the UK, which derive legitimate use of police power "*not from fear but almost exclusively from public co-operation with the police, induced by them designedly by behaviour which secures and maintains for them the approval, respect and affection of the public*".[212]

115. When asked, members of the public have made their expectations of transparency and participation clear: they want clear communication from the police about AI and what it is being used for, who is providing oversight and how it works, and police should consider a diverse range of perspectives when developing AI, to guard against bias.[213] There is recent evidence that the public are enthusiastic about having more of a voice in how data and AI are used in law enforcement, and they see that voice as essential for democratic legitimacy.[214]

116. Furthermore, there is some evidence that those who fear police use of AI do so because it risks dehumanising policing, fearing that "*the police start seeing [individuals] as data rather than people*."[215] This chimes with what we know from social and psychological research into procedural justice: being treated with dignity by the police matters, and is critical to perceptions of legitimacy, and the likelihood of people to accept authority.[216] Public perceptions of dignity, and any perceived dehumanisation of policing by AI use, therefore requires vigilance, to understand the public acceptability of change, and the ongoing impact of such change on perceptions of fairness, legitimacy, and trust.

117. Unfortunately, we found the public are currently in the dark and lack power when it comes to the design, development and deployment of AI by the police in England and Wales.

118. **Optional transparency standards:** There is a high-level principle in the NPCC's AI Covenant that police use of AI should be "Maximum Transparency by Default". However, there is little further detail on what this means and we are concerned that this high ethical standard is nowhere near being reached in practice. The government's cross-sector transparency standard for AI – the Algorithmic Transparency Recording Standard ("**ATRS"**) - is only a requirement for central government departments; for wider public bodies it remains optional.[217] The ATRS was a result of significant

212 Per explanation of historian Charles Reith in 1956, quoted in Home Office, 'Definition of policing by consent' (FOI release, 2012).

213 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025), 8.

214 Key Finding 8, Rosamund Powell, Marion Oswald and Ardi Janjeva, 'UK Public Attitudes to National Security Data Processing: Assessing Human and Machine Intrusion' (Centre for Emerging Technology and Security, Alan Turing Institute, April 2025).

215 CENTRIC "Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime" Research, 'Citizen Consultation on the Police Use of Artificial Intelligence (AI) in the UK: Acceptance, Trust and Accountability' (October 2025), 11.

216 Tom Tyler has shown in the context of criminal justice that an individual's satisfaction with their experience of the police or court is not merely determined by the outcome of their case, but is more directly linked to their perceptions of how fair the process itself was. He demonstrates this insight as consistent across age, gender, education level, income, ideological beliefs, or ethnicity. Furthermore, court users' perceptions of fairness are shown to impact the legitimacy attributed to the institutions involved, and the likelihood of people to accept outcomes that are unfavourable to them. Tom Tyler 'Introduction' in Tom Tyler (ed.) *Procedural justice: Volume I. Procedural justice and the dynamics of authority* Vol. 1 (Ashgate, 2005), xi-xxiii.

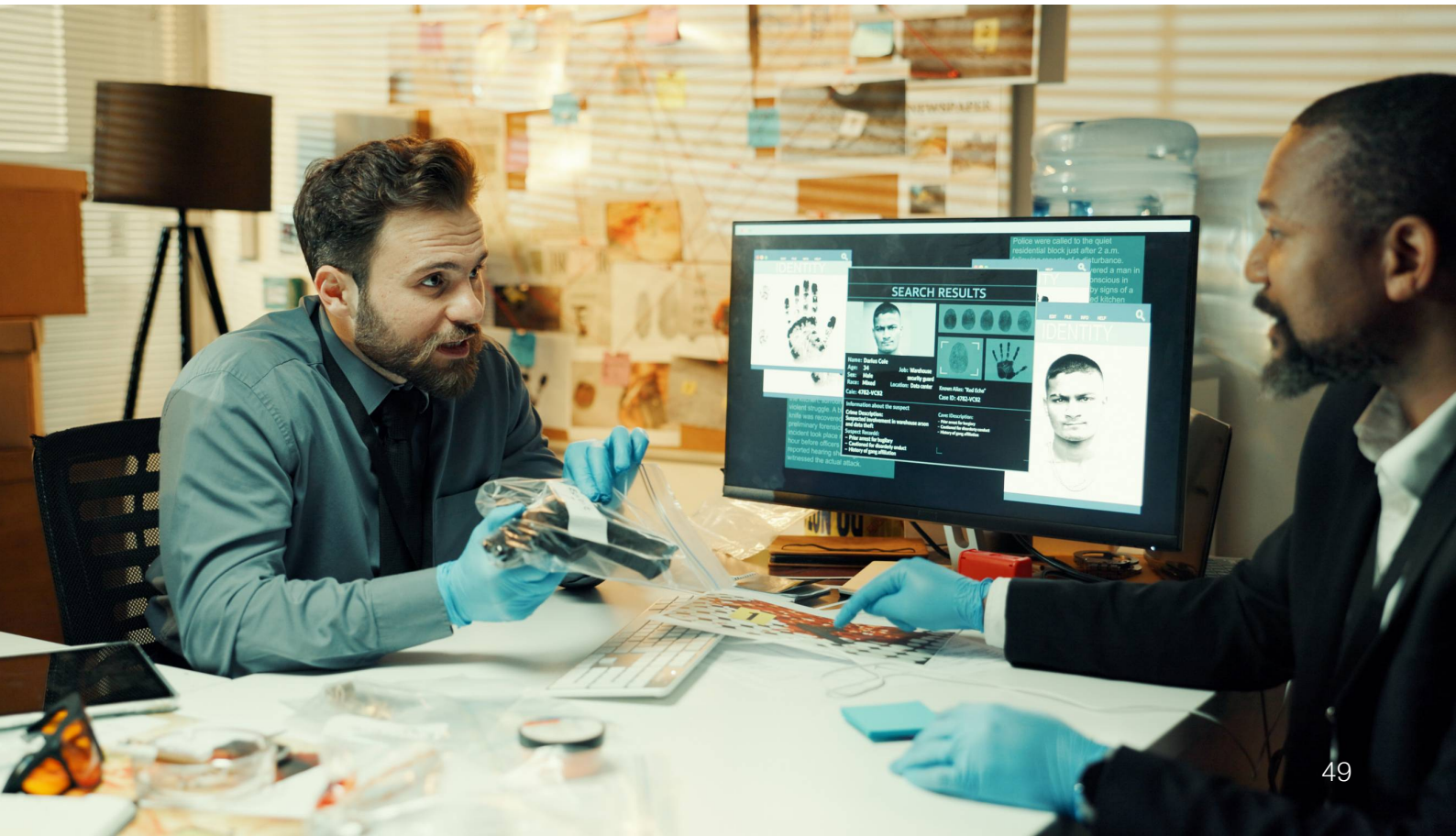
217 See Government Digital Service, 'Algorithmic Transparency Recording Standard Hub' (2023) and the 'Algorithmic Transparency Recording Standards (ATRS) Mandatory Scope and Exemptions Policy' (December 2024). It is mandated by Government policy only; there is no statutory requirement. Civil society groups including JUSTICE and the Public Law Project have argued a statutory footing would be preferable. See our joint briefing to peers during the Data protection and Digital Information Bill, (March 2024)

stakeholder consultation and has been designed to be suited for providing access to different levels of information for different public needs, i.e. different "sub-groups" as listed above. Tier 1 gives a basic level of information which gives a short and manageable summary of the tool and what it does. It also provides a contact email, for members of the public to ask questions. Tier 2 then gives more information for those with expertise or more capacity to scrutinise the detail (on the owner and responsibility of the tool, a description of the tool, its use, maintenance and system architecture, oversight mechanisms, information on data, and risk mitigation and impact assessment).

119. However, the police have almost never used the ATRS, despite its use being required in the College of Policing's Authorised Professional Practice on Data Driven Technologies.[218] Of the 100 entries currently on the register, only two are from police forces, and neither are currently in use (a retired algorithmic tool used by West Midlands Police to analyse the success or failure of rape and serious sexual offences investigations, and a risk prediction tool for domestic abuse still in development by Hampshire and Thames Valley Police.)

120. Absent any standardisation, we have observed extremely different levels of candour and transparency. We recognise the considerable information provided on some police forces' websites which are using live facial recognition technology[219] no doubt a consequence of the *Bridges* litigation and the importance placed in the Court of Appeal judgment on the foreseeability of use to the public. Beyond live facial recognition, however, there is little information in the public sphere. Absent any mandatory transparency mechanisms, we are concerned to see the ongoing need for civil society organisations to use FOI requests to access basic information about what AI tools are being used, by which police forces, and provided by which private sector partners. It was through such means that Bedfordshire Police's pilot project "Nectar" with US software firm, Palantir, was disclosed earlier this year, rather than through proactive transparency measures.[220]

218 College of Policing, 'Data-driven technologies APP'.
219 For example the policy documents, tables of deployment records, explanations and impact assessments available on the websites of South Wales Police, the Metropolitan Police.
220 Cahal Milmo, Mark Wilding 'Police use controversial AI tool that looks at people's sex lives and beliefs' (*The i Paper,* 16 June 2025)



121. **Sporadic engagement:** Any public participation beyond information provision, which substantively engages the public for their views, is again patchy. The above example of Bedfordshire Police's development of "Nectar" with US firm Palantir is in our view a missed opportunity for constructive engagement and co-creation of AI tools with affected groups who they are meant to benefit, such as groups representing victims' interests. The latter would be particularly appropriate given Palantir's statements to the press, following the FOI disclosure, that the tools had been used to identify children at risk of abuse and were being used to enact Clare's Law – the system giving women the right to know if their partner has an abusive past.[221] Instead of early involvement, key VAWG stakeholders were faced with responding to Nectar for the first time based on limited information disclosed in the FOI response. The Victims' Commissioner Baroness Newlove and the End Violence Against Women coalition[222] responses were primarily ones of concern, about sensitive victim data processing, the focus on victims' data rather than that of the suspect, and the dangers of re-victimisation.[223] We cannot see the benefit of such opaque approaches to the development of tools, but we do consider the missed opportunity – to understand with an affected community what design aspects and governance they would want to see – can only serve to damage relationships and undermine trust.

122. By contrast, we know that there is evidence of successful engagement at a local level. The West Midlands specialist data and technology ethics committee-model has included diverse voices, including the public, academia, the third sector, alongside policing and industry, and those voices were evaluated as having made positive contributions to the validity and responsibility of the AI produced. This success was conditional, however, on membership including genuine representation from the community that the police serves, transparent engagement with those members, time taken to allow them to understand the technical and legal aspects of the work, and the operational context is explained by operational police officers, and time taken to understand how AI outputs will be used, so as to enable potential benefits, risks/harms and proportionality to be assessed in the same conversation.[224] We are also aware of several public engagement efforts which have surrounded the expansion of live facial recognition, including community meetings in Croydon ahead of the first permanent live facial recognition camera having been installed. We would encourage evaluation of such exercises, similar to the evaluation of the ethics committee conducted by West Midlands, and publication of that evaluation, to better understand what works.

123. **No AI-specific legal framework and a democratic deficit:** the fact that there has been no move to legislate for AI thus far in England and Wales in one AI-specific legal framework, as the EU has, has meant one key participatory mechanism at a national level has not been available: Parliamentary debates of laws, through which the public participate through our representative democracy. Above we analyse issues of legal clarity and equality before the law which arise from using the patchwork of existing laws, however, this approach also risks creating a democratic deficit, in which the public have had no say in tools which can drastically change the way in which communities are policed. On the other hand, primary legislation cannot alone provide all the answers: it clearly benefits from longer and more detailed consideration from democratically elected Parliamentarians, but it can be a long and inflexible process, which is unlikely to meet the needs of a fast-changing technological environment. We therefore recognise

221 Ibid
222 EVAW is a UK coalition of 163 specialist women's support services, researchers, activists, victim-survivors and NGOs working to end violence against women and girls in all its forms.
223 Liberty Investigates, 'Rape victims could have health data and sexual history trawled by police AI tool' (23 July 2025)
224 Marion Oswald, Claire Paterson-Young, Pauline McBride, Michael Maher, Muffy Calder, Gitanjali Gill, Elizabeth Tiarks and William Noble, 'Ethical review to support Responsible Artificial Intelligence (AI) in policing: A preliminary study of West Midlands Police's specialist data ethics review committee' (11 September 2024)

50

the usefulness of codes of practice and delegated legislation in providing legal clarity around the use of new technologies given their relative ease of updating. However, we are also conscious that their use may exacerbate this democratic deficit unless compensatory measures are put in place, which provide alternative mechanisms to facilitate public participation.

124. **Perceptions of inevitability:** One striking finding from recent public deliberative dialogues on the use of AI in policing was that there was a perceived "inevitability" of its implementation without much public involvement.[225] One participant was quoted as follows:

"I feel uncomfortable because this is already being done and I had no idea. I feel like we haven't had a chance to consent to it." – London participant.[226]

125. We consider such attitudes to be consistent with a lack of empowerment, the public identifying essentially that, whatever their views on AI in policing, its implementation is inevitable. This chimes with the sporadic evidence we found of engagement with the public.

126. We conclude that much more needs to be done to hardwire public participation into AI design, development and deployment, at both a national and local level. This should include:

(a) Mandatory public inventories of AI tools being used by police forces and tiered information accessible to different groups of the public. While the ATRS may benefit from ongoing review and improvement, we do consider it is the best recording standard available and it should be mandatory for police forces.

(b) Opportunities to engage at a local level, such as specialist data and technology ethics committees, through which communities can be given the time and opportunity to understand what is being proposed, for whose benefit, the trade offs, any funding consequences, and details of projected risks and opportunities. We consider this includes co-design of key outcomes against which any tool is evaluated, so that what "good" looks like for that community forms part of the evaluation process. In turn, these local engagement mechanisms need to be evaluated themselves for impact, and lessons of what works shared with other forces.

(c) There needs to be a centralised public participation function which feeds into research priorities, the development of standards, and codes of practice providing legal clarity. Models such as citizens' panels or assemblies could be considered as ongoing central functions within policing, rather than depending on ad hoc Home Office consultations

127. In addition to, and not instead of, the above improvements, we note that primary legislation will likely be required for some of our recommendations, which are set out in the next Chapter. Primary legislation would provide a valuable opportunity for society which it has not had so far: a democratic process through which we debate what role we want AI to play in policing. Given the evidence of the public feeling in the dark and lacking power, that is an opportunity which the Government should embrace.

225 National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'Artificial Intelligence in Policing: A Public Dialogue' (Sciencewise, April 2025), 4.

226 Quoted in National Police Capabilities Unit (NPCU) and Home Office Policy and Innovation Lab (CoLab), 'A public dialogue on Artificial Intelligence in Policing: Summary Report' (May 2025), 7.



Chapter Four: The way forward – responsible AI in policing that the public can trust

Chapter 4

Chapter Four: The way forward – responsible AI in policing that the public can trust

128. We need to ensure police and the public can benefit from new insights, capabilities and efficiencies AI technology can offer, while maintaining – even building – trust, protecting human rights and upholding the rule of law.

129. This will not happen by accident. And we have found our current infrastructure wanting in various ways. Without change, we risk missing opportunities; developing siloed understandings of what works and does not; a market led by commercial products rather than policing need; inconsistent quality and governance standards across the country; unclear legal frameworks; and a public in the dark and lacking power who become disenchanted, even oppositional, to the police's use of emerging technology, undermining their trust and confidence in policing more broadly.

130. Our central recommendation is for **a new independent central body**. This body will support the responsible use of AI by all 43 police forces by providing the following central functions:

    (a) **establish standards;**

    (b) **secure effective oversight;**

    (c) **support responsible innovators and efficient procurement;**

    (d) **improve legal clarity;**

    (e) **facilitate ongoing research; and**

    (f) **enable the participation of wider society**

131. The Home Office has committed to the establishment of a new "*National Centre of Policing*", envisioned to "*harness new technology and forensics, making sure policing is better equipped to meet the changing nature of crime*".[227] Pending any further information, we think this sounds like a good fit for these centralised functions for AI. Alternatively, the new independent central body for police AI could sit separately.

132. Either way, the work to deliver these functions can begin now. There are several current actors in policing who can make a start on the above, for example beginning to collaborate on standards with police forces. These include the NPCC, College of Policing and the OPCSA, with the support of the Home Office.

133. However, rather than the functions being subsumed into these existing bodies, we go further in insisting on a new independent central body. We do so because we think a single body with a single focus on AI in policing is what the task requires. We also recommend a new body because there needs to be clarity in who is responsible for setting technical and governance standards, which we recommend should be mandatory in due course. This will require the independent central body to be given statutory powers by a primary legislative act to issue codes of practice (see recommendation 6) and to conduct audits or enforce the standards if needed (recommendation 9).

134. Creating the new independent central body in a primary legislative act would provide a valuable opportunity for society which it has not had so far: a democratic process through which we debate what role we want AI to play in policing. Alongside creating the body and giving it statutory powers, it would also provide an opportunity to debate the key principles guiding AI in policing, which are currently in guidance only - such as safety, fairness, transparency and accountability – and what these mean in the context of policing. Given the evidence of the public feeling in the dark and lacking power, we strongly urge the Government to grasp the opportunity for democratic engagement that such a primary legislative instrument would present.

227 Home Office and The Rt Hon Yvette Cooper MP, 'Home Secretary announces major policing reforms' (GOV.UK, 19 November 2024).

135. However, this would not be the only opportunity for the public to participate in the discussion around AI – the technology moves too fast for a "*one and done*" approach to public engagement. This is why our recommendations below include a permanent ongoing public participation mechanism as part of the independent body (see recommendation 25).

136. The body would also review for legal uncertainty, and recommend solutions to the Government. Primary legislation may be necessary when there is significant risk of uncertainty or inconsistency - we conclude biometric technologies present such a risk (recommendation 17(c)).

137. Any new body would not itself be beyond accountability to the public to deliver. It would have the overriding purpose we highlight above: **to support the responsible innovation and use of AI by all 43 police forces, so police and the public can benefit from new insights, capabilities and efficiencies AI technology can offer, while maintaining – even building - trust, protecting human rights and upholding the rule of law.** It would therefore need to be accountable to meeting this overriding purpose in practice, serving the operational line of policing and delivering for the public.

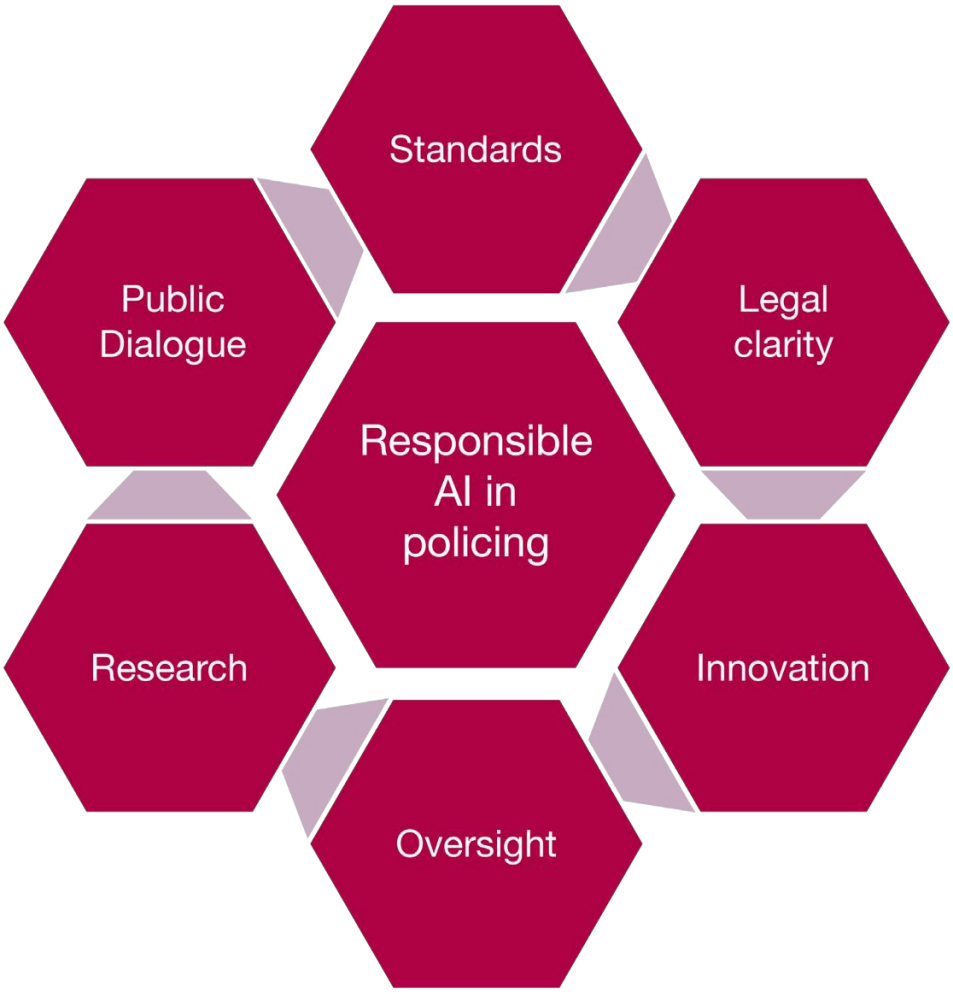


Figure 2: Central functions for an independent central body which supports the responsible innovation and use of AI in policing.

Our recommendations

1. **A new independent central body should be created to support the responsible innovation and use of AI by all 43 police forces**, so police and the public can benefit from new insights, capabilities and efficiencies AI technology can offer, while maintaining – even building - trust, protecting human rights and upholding the rule of law. For independent status, the Home Office could create and fund it as a new arm's length body. **In due course, the body will need to be given some of the functions and powers below through primary legislation.**

Establish Standards

2. **The new independent central body should develop technical and governance standards for particular tools in particular use contexts.** The Home Office, NPCC, OPCSA and the College of Policing should start work to develop these standards in the meantime.

3. **Technical standards should establish what is "fit for purpose".** These could include:

   (a) data standards and tool design standards, such as when data transparency is required, when confidence scores should be included in the user interface, other design features of user interfaces to guard against cognitive offloading, explainability and auditability design features, or data retention standards.

   (b) Performance standards and benchmarks, which address what is an indicator of success for a tool, how it is measured, and what is "good enough" for specific use contexts. These benchmarks will be applicable both pre-deployment for testing and assurance, and post-deployment for ongoing monitoring.

4. **Governance standards and safeguards should be proportionate to risk**, including pre-deployment and post-deployment standards.

   (a) Internal quality management systems and transparency standards:

      (i) pre-deployment standards would include at a minimum mandatory completion of checklists or assessments, publication of those assessments, local testing requirements prior to use and training requirements for operatives. Where needed they would also include central accreditation of operators; in some cases a requirement for police to have access to and review training data and validation testing from private suppliers.

      (ii) post-deployment standards would include ongoing monitoring and evaluation processes and documentation; requirements to publish evaluations; require keeping certain documents and logs; and require notification requirements to individuals and communities of use, as well as notification of justice system actors who will also be impacted, such as the CPS.

   (b) External oversight standards and safeguards:

      (i) pre-deployment standards could require third-party verification for higher risk use cases or requirements for pre-approval processes, or accreditation to international standards,

      (ii) post-deployment standards could impose reporting duties for non-compliance; require complaint mechanisms; or impose oversight through audits and inspections.

5. **Standards should be developed collaboratively** with police forces, private sector providers, academics, civil society, existing regulators (including the Forensic Science Regulator, the Biometrics and Surveillance Camera Commissioner, the Information Commissioner's Office and the Equality and Human Rights Commission) existing independent specialist advisory groups, such as the Science and Technology Ethics Advisory Committee,[228] and the public (see below).

228 STEAC is an advisory non-departmental public body, sponsored by the Home Office: Home Office, 'Science and Technology Ethics Advisory Committee: About us' (GOV.UK).

6. **The new independent central body should have the power to draft standards into statutory codes of practice**, which will be for the Secretary of State to lay before Parliament.[229] This power will need to be created in a primary legislative act.

Secure effective oversight

7. **Standards in statutory codes of practice would be mandatory.** Non-compliance would not automatically be a breach of civil or criminal law but will be admissible in any civil or criminal proceedings, and taken into account in any regulatory investigations. Any court or regulator would be able to take non-compliance into consideration to determine any matter in question.[230] For example, this could be taken into account if any criminal court were considering the admissibility of any AI output into evidence.[231]

8. **The independent central body should help ensure regulatory coherence**. Standards must identify and incorporate existing standards where possible, or be jointly developed with existing regulators where there is crossover with their regulatory remits. For example, when the use context is considered a "forensic science activity" and there are overlaps with the Forensic Science Regulator; or when stipulating data retention standards which overlap with the Information Commissioner's remit. This regulatory coherence role should also include engaging with regulators collaboratively where there are potential conflicts of regulatory approach.[232]

9. **The new independent central body must keep under review gaps in oversight and enforcement of the standards**. **Any gaps identified should be filled with new legislative powers for the independent central body itself to provide oversight of AI tools, and where proportionate, enforce standards to ensure unlawful and harmful technology is not used.** We anticipate the most likely powers which will be required are new investigatory powers, audit powers, powers to demand compliance with the standards, and prohibit use of an AI model pending compliance, or apply for an injunction to stop use.[233]

10. **Separately, the Ministry of Justice should review the adequacy of current legal processes to challenge unlawful AI use**:

    (a) It should consider how improvements to legal aid, costs-capping, and other mechanisms can improve the accessibility of judicial review for those who need it as a last resort.

    (b) It should conduct a holistic review of the rules, facilities and practices in criminal proceedings – beyond the current review into the presumption of reliability for computer-evidence – to consider whether they provide adequate access to challenge of AI evidence and therefore enable a fair trial and adequately safeguards against miscarriage of justice.

Support responsible innovators and efficient procurement

11. **A new independent central body should house an AI innovation hub.** We recommend the Home Office, the NPCC, the OPCSA, the College of Policing and the Police Digital Service should collaborate to design such a hub in the meantime.

12. The innovation hub should have the following functions:

    (a) **To support police forces by providing access to ethical, legal and technical expertise**, to provide guidance on responsible innovation and standards, review checklists and assessments for innovations, and advise on implementation and ongoing monitoring and evaluation.

229 Modelled either on the Forensic Science Regulator's statutory Code of Practice powers in the Forensic Science Regulator Act 2021, or those of the College of Policing in s.39A of the Police Act 1996.
230 Giving the codes of practice the same status as the Forensic Science Regulator's codes of practice (s.4 FSRA 2021), the PACE codes of practice, RIPA codes of practice, Terrorism Act codes of practice, and Information Commissioner's Codes of practice.
231 Under their discretion under s. 78 of PACE 1984.
232 For example when a new AI tool incorporates proactive personal data collection and retention for the purposes of the public sector equality duty, but there are concerns about the impact on privacy and the extent of data retention under data protection law. This would engage both the regulatory remits of the EHRC and the ICO.
233 As Forensic Science Regulator can, see ss.6-9 FSRA 2021.

(b) **Facilitate knowledge sharing** by establishing an inventory of AI with accompanying assurance information (assessments, checklists, testing, evaluations) for police to access.

(c) **Provide a central front door for private sector innovators**, to identify key areas of need, and provide them with advice and guidance on standards. We recommend consideration of the NHS innovation Service which provides such a service for healthcare innovations.[234]

(d) **Embed the above standards into ready-made procurement frameworks** for police forces, which can then be customised to local need.[235]

(e) **Central testing capacity** to test and provide pre-approval for new innovations against standards and benchmarks.[236]

Legal clarity

13. **The new independent central body should have a duty to conduct an ongoing review of legal clarity, identifying areas of legal uncertainty in the ongoing emerging use of AI technologies in policing, and recommending solutions.** This is different to technical standards: they would clarify the lawful *use* of AI tools in exercising police powers i.e. what is and is not reasonable, necessary and proportionate deployment of AI by the police in certain contexts.

14. **This must be done collaboratively**, with the experts in the AI innovation hub, police forces, private sector providers, academics, civil society, regulators, independent advisory groups, and the public (see below).

15. **The body would then recommend solutions to the Secretary of State, which could be incorporated into legal frameworks** through a number of routes.

234 NHS Innovation, 'Homepage' (NHS Innovation).
235 Blue Light Commercial ("**BLC**") has created one AI-related procurement framework already for live facial recognition: BlueLight Commercial, 'Live Facial Recognition'. Created by Home Office in 2020 and a contracting authority under the Procurement Act BLC is a non-profit membership organisation and all 43 police forces are members.
236 See similar recommendation from the Police Foundation for "*a central test and assurance centre for AI technologies, working with a network of regional test centres*": Rick Muir and Felicity O'Connell, 'Policing and Artificial Intelligence' (The Police Foundation, February 2025).



16. **Some solutions could be implemented through updates to codes of practice**, for example:

    (a) To provide clarity on whether an algorithmic prediction which is based on past group data can ever satisfy the reasonable grounds test for most police powers in PACE, which normally require some sort of individualised "reasonable" suspicion.

    (b) the need for a directed surveillance authority under RIPA 2000 for use of AI to analyse online traces to identify someone and/or predict their movements and behaviours.

    (c) Rules on AI transcriptions of Records of Taped/Video Interview (ROTI/ROVI), in PACE Code C (treatment during police suspect interview) and/or Codes E and F (audio and video recordings), for example clarity on whether they can be used, and if so, defence access to master recordings, and what artefacts form part of the unused material in any future proceedings.

    (d) clarity on when retrospective facial recognition can be used in PACE Code D, including rules on data retention and defence access, and what forms part of the unused material in any future proceedings.

17. **Primary legislation should be used for comprehensive new legal frameworks** in which powers or principles need to be newly created or would benefit from being comprehensively clarified or codified.

    (a) **Putting the principles of AI in policing on a statutory footing, while creating the new independent central body and giving it statutory powers, would provide society with an important opportunity to have a national conversation through our representative democracy**. This would be in addition to, and not instead of – a permanent public participation mechanism (recommendation 24).

    (b) Such a legislative framework could include **a future power to create codes of practice** relating to the use of specified technologies in policing, to ensure they protect individuals' rights and freedoms, and respect the rule of law.

    (c) We also recommend **a comprehensive framework for biometric data and technologies**, which goes beyond their use by police and includes all public and private use, for identification and classification.[237]

18. **The recommendations relating to public participation (below) are indispensable if delegated legislation is used and therefore new rules have not benefit from full Parliamentary debate and scrutiny**. In meeting the need of legal clarity, the balance must be struck between flexibility and speed to ensure legal clarity keeps pace with technological advancements, and the need for the law to be a result of a democratic process.

Facilitate ongoing research

19. **The new independent central body should develop centralised research capacity and undertake a programme of ongoing research of AI tools** (rather than one off evaluations such as the one public evaluation of a facial recognition tool conducted by the National Physical Laboratory).

20. **The new independent central body and the OPSCA should have a duty to promote openness to academic research on a local and national level.** They must work with researchers in industry, academia, and civil society, to develop this, including:

    (a) Encouraging proactive publication of performance data and monitoring information (e.g. equality impact evaluations, deployment data, audits, numbers of complaints received or successful appeals);

    (b) Encourage formal partnerships with academic institutions, including defined access protocols, co-design of research, joint research governance.

    (c) Developing a central bank of resources, including templates such as data sharing agreements.

237 See further Matthew Ryder KC, The Ryder Review: Independent legal review of the governance of biometric data in England and Wales (Ada Lovelace Institute June 2022); Nuala Polo, Jacob Ohrvik-Stott, 'An Eye on the Future' *Ada Lovelace Institute* (May 2025); Sam Stockwell, Megan Hughes, Carolyn Ashurst and Nóra Ní Loideáin, 'The Future of Biometric Technology for Policing and Law Enforcement' (Centre for Emerging Technology and Security, Alan Turing Institute, March 2024).

(d) For those applying from outside formal partnerships, develop standardised processes for independent researchers to submit proposals, have them reviewed (including independent review e.g. from ethics committees), obtain data access and publish findings.

21. **The new independent central body must ensure research then informs standard-setting.** For example, if research finds a new tool produces non-statistically significant disparities between people of different demographics if used at a certain threshold, that that finding would inform a technical standard to use the tool at that threshold setting.

22. In addition, the OPSCA should collaborate with the new independent central body, in:

    (a) **taking a systems-approach to setting research strategy on AI,** including research on police AI use and trust in communities; de-skilling and cognitive offloading impacts of AI use and effects on policing over time; and the impact of different AI tools on the fairness of the criminal justice system; and

    (b) **including the public in setting research strategy**, to co-design what they want to know and measure, for example through input into OPSCA's Areas of Research Interest.[238] For example, learning from health settings in which "Priority Setting Partnerships" have successfully involved the public in the development of research priority topics.[239]

Enable participation of wider society

23. **The Home Office should make the Algorithmic Transparency Recording Standard mandatory for police**.

24. **The new independent central body should facilitate knowledge sharing between police forces to highlight best practice and evaluation of local participation and accountability models,** see for example the evaluation of the West Midlands Data Ethics Review Committee model.

25. **The new independent central body, and in the meantime the Home Office or the NPCC, should establish a new permanent public participation mechanism through which to engage with different groups of the public on an ongoing basis.** This could be a citizen's panel or assembly, or another structure – we recommend an initial scoping and feasibility study to identify the best mechanism. The public participation mechanism would inform the independent central body and its work in AI in policing, including but not limited to:

    (a) Technical standards and benchmarks, to co-design standards on what good looks like with the public.

    (b) Governance standards, particularly to understand what information the public want to know about AI and how it is being used to inform transparency standards; to understand what concerns they want to be tightly regulated through oversight mechanisms, to inform the ongoing review of governance and oversight and the need for the central body to adopt enforcement powers itself.

    (c) Research priorities, to understand what research questions the public are asking. If they can be answered through new research, ensure that it influences research strategy (as above) and if they are questions on which there is already evidence, to identify the need for more knowledge mobilisation and accessibility of current research, for example research summaries or primers.

    (d) Areas where there is public support for AI innovation, where public attitudes are sceptical, and why.

238 Science & Technology in Policing, 'Policing Areas of Research Interest'.
239 See James Lind Alliance, 'Home' (JLA).

Acknowledgements

JUSTICE is extremely grateful to our expert advisory group, who have steered this report from initial conception to completion:

Lord John Thomas of Cwmgiedd (House of Lords, JUSTICE Council)

Sophia Adams Bhatti (Independent consultant, co-author of JUSTICE's *AI in our justice system*)

Professor Jacqueline Hodgson (University of Warwick, JUSTICE Council)

Professor Marion Oswald MBE (Northumbria University)

Dan Squires KC (Matrix Chambers)

Dr Jeni Tennison OBE (Connected by Data).

Thanks also go to all those who shared their time and expertise with us, through individual consultation or by attending our workshop on the project, including:

Professor Arshad Jhumka (University of Leeds)

Professor Tom Sorell (University of Warwick)

Tom Guest (Crown Prosecution Service)

Professor Carole McCartney (University of Leicester)

Dr Daragh Murray (Queen Mary University of London)

Detective Sergeant David Thomason KPM (Cheshire Constabulary)

The Information Commissioner's Office

End Violence Against Women Coalition

Lord Tim Clement-Jones CBE (House of Lords, Co-Chair of the All Party Parliamentary Group on Artificial Intelligence)

Fabian Chessell (DATA Alliance)

Donna Murray-Turner (Another Night of Sisterhood)

Caroline Selman (Public Law Project)

Jasleen Chaggar (Big Brother Watch)

Urja Lakhani (Association of Police and Crime Commissioners)

Dylan Alldridge (Strategic Lead for AI at Office for the Police Chief Scientific Adviser)

Ryan Woodburn (Deloitte)

Lewis Lincoln-Gordon (West Mercia Police, NPCC AI Portfolio Coordinator)

Gaia Marcus (Ada Lovelace Institute)

We are also indebted to the University of Cambridge Pro Bono Project, whose researchers helped us identify international examples. Thanks to Dr Arushi Garg, Andrew Charroux, Nikita Bhakare, Stephen Watson, Andolan Sarkar, Hannes Bastians, Javid Rahimli, Krishna Agarwal, Prakriti Bandhan, Sanat Narayan, Sarah Abell, and Suvradip Maitra.

We are also grateful for the pro bono research assistance of DLA Piper, who helped us identify AI use cases in England and Wales and hosted our workshop.

As ever, we are grateful to our JUSTICE staff members who have helped produce this report: Ellen Lefley, Senior Lawyer who led this project with oversight from Legal Director, Stephanie Needleman, and all those who assisted with research, drafting and workshop facilitation - Emma Snell, Leyya Kitmitto, Caroline Arnold, Carl Dennis, Lilly Maxfield and Bronwyn Tonelli; and the communications and events team for their assistance in producing the report - Jessica Kaplan, Ben Davis and Honor Johnston.

Finally, thank you to Dechert LLP for producing the digital version of the report and formatting it; thank you to Sidley Austin LLP for printing the report; and thank you to Macfarlanes LLP for hosting our launch event on 2nd December 2025.

The views and recommendations expressed in this report are those of JUSTICE and do not reflect the views of everyone we consulted or worked with to produce this report, nor the organisations or institutions to which they belong.





JUSTICE Registered Charity in England & Wales No 1058580. In Scotland,
JUSTICE is known as ‘JUSTICE Scotland’ Charity No SC043518.

A company limited by guarantee and registered in England No 3216897.
Registered office address as above.