Response to Justice and Home Affairs Committee report 'Technology rules? The advent of new technologies in the justice system'

1. The Government welcomes the opportunity to respond to the Committee's report on existing and future use of new technologies in the justice system, such as artificial intelligence (AI), live facial recognition and advanced data analytics. The report draws welcome attention to an increasingly important issue. We agree that advanced technologies offer many public protection and criminal justice benefits, but with this also come challenges and it is important that digital technologies are used in a responsible way. Whilst specific examples such as the emerging use of live facial recognition help illustrate some of the challenges, we think it is important to retain a long-term perspective.

2. Technologies such as fingerprints and DNA processing were once considered new and controversial by some but are now validated and very widely accepted. The adoption of DNA and fingerprinting required organisations responsible for delivering, supporting, and overseeing innovation to adapt to the changing nature of policing, crime and technology. The government will empower and support them to go further, taking opportunities to simplify and consolidate structures when there is likely to be a positive impact on consistency, accountability and transparency.

3. The digitisation of the economy and society is having an enormous impact on the criminal justice system and policing. For example, within ten years the level of data police may need to analyse as part of their investigations has grown immensely and without digital data capabilities it would be impossible for operational staff to meet the growing information burden of investigating complicated, networked criminals and terrorists and identify key evidence.

4. Of course, as the Minister of State for Crime, Policing and Probation stressed in his evidence, this challenge must be met within the norms of democratic accountability in a free society. Members of Parliament as the elected representatives of the public, set the legal framework providing the police with their powers and legal duties. It is then for the police to determine how best to use new technologies like artificial intelligence or predictive modelling to protect the public. The existing oversight bodies monitor how the police carry out their duties and ensure safeguards and standards are upheld. HMICFRS is responsible for inspecting and reporting on the efficiency and effectiveness of all police forces. This includes how forces use existing and emerging technologies to prevent and detect crime.

5. We do not underestimate the challenges addressed by the report, but the Government does not agree with the report's characterisation that new technologies will inevitably override societal values or hand over judgement on matters of necessity and proportionality to machines. The Government remains committed to the principle that people, not machines, take the key decisions such as whether to arrest, charge, prosecute or ultimately convict. The future capabilities of artificial intelligence in automated decision making will act to improve the justice system by augmenting rather than replacing existing processes.

6. It is also important to recognise that automation that supports decision making through advanced data analytics is very different from automated decision making. The use of fingerprints and DNA to help solve crimes through identifying and eliminating suspects is widely accepted. These technologies rely on a completely automated system to file and subsequently link profiles taken on arrest to those taken from crime scenes. Automation also ensures that the biometrics of people arrested but not subsequently convicted of a crime are

deleted. The circumstances of each case then guide how this information is used, with the police and later the courts left to interpret this connection, with the aid of expert witnesses where appropriate.

7. Given the pressure on policing to respond to crime we also think that more emphasis should be placed on the benefits of automation. South Wales Police estimate that they save around £230,000 a year from using retrospective facial recognition. One example, featured on the BBC's Crimewatch, allowed South Wales Police to use facial recognition to quickly identify a man caught on CCTV trying to abduct a woman late at night and arrest him before he could commit further offences. Previously, identification of suspects caught on CCTV would take around fourteen days, whereas now this is typically reduced to minutes.

8. In our written evidence we also highlighted the role that artificial intelligence has supporting officers faced with tackling the most serious crimes. The Child Abuse Image Database combined the powerful data processing capabilities with human expertise to help identify, link and categorise serious indecent images of children. Quicker identification and connection between abuse images helps identify where abuse is happening, and the scale of abuse being perpetrated against a victim. Better identification increases the chance to identify the victim and remove them from harm and hold the perpetrators to account. As well as fighting crime, artificial intelligence in this context has important operational welfare benefits in one of the hardest areas of law enforcement to work in. It protects officer welfare by reducing their exposer to harmful and upsetting content. The use of artificial intelligence to counter child sexual exploitation was developed in partnership with industry and academia, which meant a clear development cycle including an extensive testing and staff training stage.

9. Criminals will use any technology which helps their illegal activity. The police need to be able to adapt quickly and trial new technologies to keep pace. The public want the police to fight crime effectively and efficiently, and they want criminals held to account when they commit crimes. Opinion polls consistently demonstrate that police use of technologies such as live facial recognition, which are considered controversial by some, have strong public support.

10. The report is a welcome reminder of the many challenges and benefits which innovation may bring to the criminal justice system. With continued support and scrutiny from parliament the Government will continue to support the use of new technologies to fight crime, protect the public and bring justice to those undertaking illegal activities.

Response to recommendations

Legal and Institutional Frameworks

- **Recommendation 1 - We recommend that the Government rationalise the respective roles of Departments as they pertain to the use of new technologies in the application of the law. (Paragraph 42)**
- **Recommendation 2 - We recommend that the Government conduct a review to rationalise and consolidate governance structures of the use of technologies in the application of law. (Paragraph 43)**

12. As digital underpins ever more aspects of our economy, society and daily lives we believe a coordinated, cross-government strategy is critical and this is preferable to seeking to consolidate or rationalise roles. There is a cross government effort to address common challenges around ethics, data standards and procurement in the justice system and the wider economy.

13. The Central Digital and Data Office (CDDO) was launched in April 2021 to lead the Digital, Data and Technology (DDaT) function and put the conditions in place for digital transformation at scale across the public sector. The CDDO works closely with government departments, including the Home Office and Ministry of Justice to ensure a consistent approach to deploying digital technologies. The Department for Digital, Culture, Media and Sport (DCMS) holds oversight of policy and regulation for the governance of digital and technology more broadly, working across Government to ensure a coherent approach. The Centre for Data Ethics and Innovation (CDEI) promotes the responsible use of new technologies with organisations in law enforcement and the justice system benefitting from their expertise.

14. The report identifies several organisations with a responsibility for ensuring the ethical use of new technologies in policing. Provided overlap and duplication are minimised, the Government does not think that having some level of oversight responsibility, or interest in the ethical use of new technologies, shared across different organisations reduces the effectiveness of this oversight.

15. Both the policing landscape and the governance of digital technologies are complex areas, but Government remains confident that - taken together – the existing structures and organisations create a comprehensive network of checks and balances. Where the roles are no longer clearly defined the Government has acted, for example by appointing a joint Biometric and Surveillance Camera Commissioner in 2021. The Government will continue to monitor how the overall system of oversight is working and act as needed.

- **Recommendation 4 - We recommend that the Government bring forward primary legislation which embodies general principles, and which is supported by detailed regulations setting minimum standards. We consider that this approach would strike the right balance between concerns that an overly prescriptive law could stifle innovation and the need to ensure safe and ethical use of technologies. (Paragraph 65)**
- **Recommendation 5 - Along with 41 other countries, the Government has endorsed principles of Artificial Intelligence. In response to this report, the**

Government should outline proposals to establish these firmly in statute. (Paragraph 66)

- **Recommendation 8 - The Government should appoint a taskforce to produce guidance to ensure that lines of accountability, which may differ depending on circumstances, are consistent across England and Wales. The taskforce should act transparently and consult with all affected parties. (Paragraph 85)**

16. The Government agrees that the use of technologies in the criminal justice system must be safe and ethical. For policing specifically, there are already many safeguards. The data protection, equalities and human rights framework set by parliament has created a principles-based framework. Together with the foundational Peelian principles for policing, now enshrined in the Standards of Professional Behaviour (schedule 2 of the conduct regulations), the existing legal framework requires the safe and ethical deployment of new technologies. Therefore, the Government will focus on encouraging policing in particular, to provide innovative solutions which identify and promote best practice; supporting the APCC and NPCC to use their ground level experience to identify where change is needed.

17. The UK is a signatory to the OECD Principles. Internationally the Government works with like-minded countries to support the responsible use of AI. The Government's Plan for Digital Regulation notes the importance of exploring a range of outcomes-focused regulatory and non-regulatory tools to promote a pro-innovation approach. Later this year we will be setting out what this means for our approach to regulating AI through a forthcoming White Paper.

18. With respect to policing, the Government does not agree that further central guidance on accountability is needed, because it is the role of local Police and Crime Commissioners to hold their local forces to account as the elected representative of the local population. If it is a matter of conduct, or professional standards, then institutions such as the Independent Office for Police Conduct act to monitor and investigate any wrongdoing. HMICFRS inspects and reports on the efficiency and effectiveness of police forces in England and Wales, including how forces promote ethical behaviours and deal with corruption. At present HMICFRS are undertaking a report into digital forensics which will report back in Autumn 2022.

19. However, the Government will continue to work with the professional standards bodies in the justice system, to identify where they can consider the use and deployment of new technologies in ongoing monitoring, reporting and compliance duties.

- **Recommendation 6 – Guidance, both general and specific, is urgently needed. The Government should require that national guidance for the use of advanced technological tools in policing and criminal justice is drawn up and, as part of their response to this report, should outline concrete plans for this. (Paragraph 74)**
- **Recommendation 7 - There is a need for a 'one-stop shop' collating all relevant legislation, regulation and guidance and drawing together high-level principles with practical user guides. This collation should be updated by the College of Policing on an ongoing basis, and direct users to the guidance and regulation relevant to their circumstance and need. (Paragraph 75)**

20. The Government agrees that further guidance on new technologies for the police may help operational deployment and officer confidence when using powerful new capabilities.

However, this should be sector-led with the government's support, not centrally imposed. Indeed, the sector already acts responsively to develop tailored guidance. For example, since the committee's inquiry concluded, the College of Policing has issued guidance on the use live facial recognition. The guidance includes advice on how to forces should take account of data protection, equality, and human rights issues, and is based on learning from early pilots.

21. More widely, the Police Chief Scientific Adviser also provides support and guidance. The Government created this position in 2021 to support the scientific support and expertise available within policing at the strategic level. The Chief Scientific Advisor is already developing a digital platform to support police forces which will include information on the science and standards of different technologies and scientific capabilities. The Government is providing support to ensure that technical evaluation and analysis is part of the information captured. New technologies could be covered by this work once they start being used.

Oversight body

- **Recommendation – 3 As part of rationalisation the Government should establish a single national body to govern the use of new technologies for the application of the law. The New national body should be independent, established on a statutory basis and have its own budget. The body would have several functions and responsibilities, which we detail in Chapter 5. It should draw on as wide as possible range of expertise. (Paragraph 44)**
- **Recommendation 9 - Moratoria are important and powerful mechanisms. In its response to this report, the Government should set out the circumstances in which it would be willing to deploy them in the future. The new national body we recommend should be empowered to refuse certification for a new tool under those circumstances. (Paragraph 89)**
- **Recommendation 20 - Minimum scientific standards should be set centrally by the new national body we have recommended in paragraph 44. They should then be transposed into regulations through secondary legislation. (Paragraph 173)**
- **Recommendation 21 - The new national body recommended in Chapter 2 should systematically certify technological solutions following evaluation and prior to their deployment. No technological solution should be deployed until the central body has confirmed it meets the minimum standards. After a transition period, this requirement should retrospectively be applied to technological solutions already in use. (Paragraph 189)**
- **Recommendation 25 - The new national body recommended in paragraph 44 would have distinct responsibilities to set minimum standards for the use of new technologies in the application of the law; certify every new technological solution against these standards; and to carry out regular audits into their use. With the assurance brought by the certification process and the register of algorithms, police forces and other public bodies would remain free to procure the technological solutions of their choice, as long as the products have been certified. (Paragraph 219)**

22. The Government is not persuaded by the arguments put forward to create a new national body and certification system. While certification can work in some contexts, it can also create false confidence and be prohibitively costly.

23. We are similarly not persuaded by the suggestion a national body would play a role in enforcing moratoria. The technology areas which need the most restrictive regulations, and where the Minister is required to authorise use, are mature capabilities and those which can inflict lethal or less lethal force. Ministerial sign off and moratoriums are a resource heavy process which can create significant delays in the roll out of new equipment and should be preserved for where the risk is greatest and the material impact on individuals the highest.

24. The Minister of State for Crime, Policing and Probation outlined the benefits of a less codified approach in his oral evidence. Benefits include greater agility in the face of rapid change and local decision making. The Government is also against removing the power for local communities to have a say over how their neighbourhoods are policed and centralising control nationally. However, national regulators like the ICO ensure a strategic coherence across policing and the wider economy.

25. A further barrier to establishing a centrally overseen certification regime is a lack of common and internationally agreed standards to test and benchmark against. Indeed, the current volume of use across many of the advanced technologies referenced in the report is not yet sufficient for there to be technical standards, which are a practical requirement for effective regulation. Further pilots and innovation are needed before there is consensus on how a capability such as artificial intelligence applies in the justice system.

26. Polygraph tests have become embedded into probation practice as a means of managing certain high-risk offenders on licence, providing probation practitioners with risk-related information about the individual that they otherwise may not have known. A full evaluation of the impact of polygraph testing people with sexual convictions was undertaken prior to this being fully rolled out, and a pilot is currently underway of polygraph with domestic abuse offenders. The Offender Management Act 2007 sets out the limitations of how, and with whom, polygraph can be used, including prohibiting the use of polygraph testing outcomes in criminal proceedings.

27. The Government will continue to develop common definitions and standards and ensure they relate to the justice system. As announced in the National AI Strategy, the Government is currently undertaking a review of the AI Governance landscape. This will look at current regulation and legislation, regulator expertise and capacity and the institutional landscape including standards and assurance bodies, to ensure the regulatory regime facilitates innovation while protecting people and our fundamental values.

Transparency

- **Recommendation 10 - One of the principles in the new statute we recommend should be transparency. (Paragraph 94)**
- **Recommendation 11 - We urge the Government to consider what level of candour would be appropriate to require of police forces regarding their use of advanced technologies. (Paragraph 102)**

28. It is in the interests of the police and the wider justice system to be transparent, to maintain public trust and deliver services efficiently.

29. Since the first pilots of live facial recognition the police forces involved have published additional information on their website, with public facing resources aimed at technical and

non-technical readers, alongside operational documents including their impact assessments. This shows openness and transparency and may act as a template for how forces should approach transparency and accountability when other new technologies are used.

30. Some level of operational secrecy may be required in some contexts to protect capabilities and ensure criminals are not given information they can exploit to cause harm. In these instances, internal or non-public facing accountability is also needed. The Government will consider if transparency and information sharing between relevant organisations, as already used in the oversight of covert surveillance, would allow scrutiny by appropriately vetted experts. The benefit of internal transparency is that it is carried out by individuals with the expert knowledge needed to effectively challenge whether the use is fair and ethical. If transparency is set out in statute, then organisations may limit transparency efforts to whatever is stated in the legal reporting duty. Legal reporting duties overlook the value of sector led scrutiny, such as that provided in the oversight model for covert surveillance.

- **Recommendation 12 - Full participation in the Algorithmic Transparency Standard collection should become mandatory, and its scope extended to become inclusive of all advanced algorithms used in the application of the law that have direct or indirect implications for individuals. This would have the effect of turning the collection into a register. Engaging with this register will require additional and dedicated resourcing. The central body we have recommended should have the power to review and issue penalties if entries are not completed. (Paragraph 112)**
- **Recommendation 13 - The register should be user-friendly. Users should be able to find information about technological solutions being deployed, who is deploying them, where, on what occasions, and for what purposes. They should also be able to find detailed impact assessments and details of the certification issued by the central body we have recommended (see paragraph 189). (Paragraph 113)**

31. The first version of the Algorithmic Transparency Standard was published in November 2021. The Standard is accompanied by prioritisation guidance, but its use is encouraged for all algorithmic tools in the public sector. The CDEI and CDDO are currently piloting the algorithmic transparency standard with public sector bodies, including some police forces. The Government will continue to pilot and gather feedback on this to explore options for how to deploy the standard more broadly.

Human Technology Interactions

- **Recommendation 14 - The Home Office should, in conjunction with the Ministry of Justice and the College of Policing, undertake or commission appropriate research to determine how the use of predictive algorithms affects decision making, and under what circumstances meaningful human interaction is most likely. (Paragraph 130)**
- **Recommendation 15 - We endorse the principles provided by the Information Commissioner's Office regarding meaningful interaction with technologies. These principles should be applied through mandatory training for officers and officials using advanced technologies. As appropriate this should include both generic data analytics and specificities of the particular technology in question. As part of continuing professional development, training should also**

be made available to lawyers, members of the Judiciary, and other professionals involved in the justice system. Training will need to be tailored for the specific context and delivered by the relevant professional body with the support of the central body recommended in paragraph 44. (Paragraph 138)

32. The Government will continue to develop its research of existing technology capabilities and identify future trends or adoptions. However, a lack of agreed terms to describe what is being done and a lack of consensus about how to define concepts such as artificial intelligence presents additional research and collaboration challenges. The Government will therefore work with the justice system to establish common, scientifically robust, definitions around advanced technologies, ensuring they are more consistent in how they are described and categorised. This will allow better long term research and evaluation of the different circumstances in which predictive algorithms are and support future decision making.

33. Whilst any training or resources developed by the Information Commissioner's Office may be shared with professionals involved in the justice system and delivered by their relevant professional bodies, policing and the judiciary is wholly independent of Government. Training is exercised by the Judicial College and College of Policing. As such, it would not be constitutionally appropriate for any judicial training to be supported or overseen by a statutory body established by the Government.

- **Recommendation 16 - At a minimum, there should be one person within every team which uses advanced technologies with the expertise required to support colleagues in the use of advanced technological solutions. Enabling meaningful support and proper assessment will require substantial investment in continuing professional development and the development of leadership skills. (Paragraph 139)**
- **Recommendation 17 - Institutional processes to enable challenge to algorithmic outcomes should be reviewed and inspected. These inspections should also assess whether the users of the relevant tool(s) are appropriately trained. (Paragraph 146)**
- **Recommendation 18 - There should be a requirement upon producers of technological products to embed explainability within the tools themselves. The interface of tools should be designed to facilitate the experience of users: equipping them with the necessary information to interpret outputs, and an indication of the level of surety its outputs provide. The specifics of what should be explained will vary depending upon the context. The tool should reflect that variation and encourage users to consider and challenge results. (Paragraph 155)**

34. It is not appropriate for the government to dictate how technical support is embedded into the structure of an organisation deploying new technologies and there are circumstances where centralised technical support will be of greater value.

35. The Government will explore whether accountability and explainability can be better documented and how this information could be safely shared with the public. For policing specifically, if guidance on different use cases will help ensure consistency in the level of challenge staff undertake during a technology's deployment, then the sector is well placed to develop it. They may wish to draw on wider best practice in the public sector.

36. The Service Standard, available on GOV.UK is a 14 point guide that helps government teams and departments create and run public services. It requires government teams to make sure that services are accessible and usable for all. All departments are assessed by the CDDO against the Service Standard and new digital services are required to comply in order to be launched on gov.uk. Individual police forces and the wider justice system are not assessed by default but are encouraged to follow the best practice outlined in the Service Standard and Service Manual.

Evaluation and oversight

- **Recommendation 19 - Comprehensive impact assessments should be made mandatory for each occasion an advanced technological tool is implemented in a new context or for a new purpose. They should include considerations of bias; weaknesses of the specific technology and associated datasets; and discursive consideration of the wider societal and equality impacts (including explanations of public consultations). Impact assessments should be regularly updated and open to public scrutiny. (Paragraph 169)**

37. The Government agrees that impact assessments are an important part of the pre-deployment process. Organisations within the justice sector have a legal duty to undertake an equality impact assessment and data protection impact assessment prior to deployments.

38. There are existing resources on how to approach these exercises when looking at advanced data analytics and sensitive personal data. The existing instruments for AI impact assessment, such as the Data Ethics Framework or the Guide to Using AI in the Public Sector, contain sections on addressing and mitigating bias, and ensuring that algorithmic tools used in the public sector have a positive social impact. More generally, regulators produce additional resources and guidance on how to undertake an impact assessment and the questions that should be asked when exploring if the use is proportionate. The Government will work with the justice sector to ensure they are connected to the expert support available to them from regulators in this space.

- **Recommendation 20 - While police forces should remain free to procure the technological solutions of their choice among those certified by the new national body, they need extra support to become proficient customers of new technologies. Pre-deployment certification could, in itself, reassure them about the quality of the products they are procuring. Enhanced procurement guidelines are also needed. (Paragraph 206)**

39. The Government does not agree that pre-certification is required for police forces to be proficient customers of new technologies. Enhanced procurement guidelines for the public sector can be found in the recently published DDaT Playbook which enforces the importance of using the Technology Code of Practice and contains guidance on how to avoid vendor lock-in.

40. The Playbook is implemented on a 'comply or explain' basis for central government and arms-length bodies. The Playbook is not mandatory for use by police forces, but it is strongly encouraged that they apply its principles and policies as it represents best commercial practice in the public sector. The Playbook has been developed by commercial and digital experts across government and industry to capture and outline the most important considerations when procuring digital goods and services. The Government will continue to

support the police to establish any guidelines they feel are needed for better procurement practices and encourage forces to learn from what has been tested elsewhere, but it is not for the Government to set these guidelines.

- **Recommendation 23 - We urge the Government to continue work on the national data ethics governance body. This body will need the independence, resources, and statutory underpinning to enable it to scrutinise the deployment of new technologies and act as a central resource of best practice. (Paragraph 217)**

- **Recommendation 24 The Home Office should encourage and facilitate the development of local or regional specialist ethics committees. These committees should be granted independence, a statutory basis, and an independent budget. They should be transparent, and their membership should be diverse. They should scrutinise the use of new technologies by police forces throughout their lifecycle and in their deployment contexts, confirming that their proposed and actual uses are legitimate, necessary, and proportionate. These committees could be given a veto of the deployment of a particular technological solution during a mandatory trial period. (Paragraph 218)**

41. Involvement and engagement with the public on how technology is used is important to its successful use. Ethics groups are one form of better community engagement and one way this can be done.

42. The justice sector continues to develop how ethics groups can support innovative use of technologies. The Government will continue to support policing as it develops ways to get local feedback and allow the public to voice their concerns. The Government does not agree that there should be a mandate for ethics groups across all forces or that these should be on a statutory footing. While ethics groups may provide decision makers with useful advice, only Members of Parliament and the democratically elected Police Crime Commissioners are empowered to act on behalf of the public. It is for elected representatives to set the laws and the policy; and Chief Constables are rightly operationally independent.