# Association of Police and Crime Commissioners (APCC), National Police Chiefs' Council (NPCC), and Police Digital Service (PDS) — Written evidence (NTL0049)

1. New technologies are central to policing's ability to tackle serious harms and deliver a seamless public service; balancing protection of the public with protection of civil liberties is important to PCCs and Chief Officers. This submission describes how the Association of Police and Crime Commissioners (APCC), the National Police Chiefs' Council (NPCC) and the Police Digital Service (PDS) collaborate to implement new technologies that are effective, proportionate, and fair.

### Our Joint Ambition for New Technologies

2. Our ambition for new technologies recognises: (1) the power of algorithms to achieve a 'step change' in policing efficiency; (2) the 'arms race' we face with criminals who benefit from new technologies; and (3) the need to maintain public confidence through standards, an ethical framework, and independent oversight.

3. Launched in January 2020, the APCC/NPCC Digital, Data and Technology strategy 2020-2030 sets out five digital ambitions for policing: provide a seamless citizen experience, address and prevent harm, enable officers and staff, embed a whole system approach, and empower the private sector. Coordinated by PDS, our progress against these ambitions includes standing up a national data office supported by a Chief Data Officer, delivering a centralised cyber assurance service that is modernising Forces' information security and cyber resilience, progressing 13 national technology programmes including harmonising cloud services, and implementing 69 National Standards in data, technology, skills, and commerce.

4. Individual use cases for new technologies are outlined in capability strategies. For example, the APCC/NPCC Digital Forensic Science Strategy makes clear the infrastructure, processing, and trust requirements that are needed for effective digital forensics within policing. The national Policing Science and Technology strategy, being developed by the Policing Chief Scientific Advisor, will identify the role of new technologies in delivering new capabilities aligned with our ambitions.

### The Operational Landscape

5. All Forces use advanced algorithms to some extent, with most applications focusing on organisational effectiveness and workforce planning (see the 2021 Home Office Data Analytics Landscape Review for a broad sector analysis). This includes demand management functions such as Lancashire Voice (see Box 1) and automation that reduces the need for manual intervention, such as using image recognition to categorise video footage. Because these tools address local needs, they vary in their form and focus; indeed, this variation underpins policing's extensive success in innovation.

## Box 1: Examples of New Technologies

**Demand management**. Working with Hewlett Packard Enterprise and Intelligent Voice, Lancashire Constabulary's 'Lancashire voice' tool uses voice-to-text technology and natural language processing to develop word models to understand, categorise and manage the Force's 999/101 calls (approx. 1.2m per year). As of 27 Sept, 2021, the system had categorised 730,000 calls, which would have taken Lancashire's team of 8 people 68 years if they continued reviewing unlogged calls manually. Read more.

**Preventing harm.** Governed by a principle of no 'misuse' of data while ensuring no 'missed use' of data, the Thames Valley Violence Reduction Unit uses a secure and accredited cloud computing environment to collate hundreds of live data feeds from across local partners, in policing, local authority, education, youth offending, health, and criminal justice. Using the power of cloud analytics and visualisation they have shifted policing's efforts toward early intervention and prevention. Read more.

**Tackling crime.** Home Office DDAT and Forces are collaborating on operational pilots that use automatic number plate recognition (ANPR) data to identify and proactively target high harm County Lines offenders. Developing new methods of identifying suspicious travel, this work complements existing analytical tools and policing techniques and has already proven highly successful. Read more.

**Automation.** Eastern region forces and the NPCC Lead for PNC are piloting a robotic process that checks PNC records on individuals in support of Vetting enquiries. The 'Bot' runs many procedural checks and passes key information to a vetting officer for assessment and decision, far quicker than achieved by the current manual search. This tool has real potential to introduce efficiency for all forces.

6. The use of algorithms for predictive analytics is less prevalent. A recent survey found roughly one third of Forces are exploring or implementing advanced algorithms. This slower adoption stems from due regard for ethics, the challenges of data infrastructure, limited but growing data science expertise, and budgetary constraints that limit Forces' abilities to experiment. Where implemented, those responsible act with a demonstrable understanding of how the technology is working, its risks, limitations, and their legal and ethical consequence.

7. To develop capability, propagate best practice, and remove duplication, policing is fast developing its national capabilities: PDS, the National Digital Exploitation Centre (NDEC), Tackling Organised Exploitation (TOEX), and the National Data Analytics Solution (NDAS). For example, in May 2021, NDAS transitioned its Modern Slavery proof-of-concept into an operational dashboard, allowing the adopting Force to identify new incidents, visualise networks, share intelligence effectively, and ultimately deliver a better policing response.

8. Several capabilities assess new technologies 'in the wild' with real users and data, so that policing can carefully and cumulatively understand its effects. The Home Office Accelerated Capability Environment allows industry and policing to work together in a controlled environment to develop new tools. The Home Office Digital, Data and Technology teams work closely with policing on advancing the analytics used on existing data; our collaboration on using ANPR to identify county-lines drug offending a case in point (see Box 1).

9. The Police Science, Technology, Analysis and Research (STAR) fund resources the innovation of new technology, though the fund's remit is wider. In FY20/21 it supported three projects (£0.97m) on new algorithm applications. One was a review of predictive analytic tools for knife crime detection, to identify best practice, challenges and lessons learned. STAR is fundamental to policing's ability to produce knowledge of the impact, fairness, and effectiveness of new technologies.

10. There is broad recognition of the need to upskill officers and staff in the use and management of new technologies. The College of Policing's specialist digital courses focus on data analytics in a tactical sense for intelligence and investigation gathering. The Strategic Command Course promotes a broader strategic, problem-solving approach to help achieve the best outcomes for individual forces. With this approach and the differing IT systems across the country, Forces can then source the right training according to their local needs.

11. Our specialist communities ensure continuous best practice via the Data Analytics Community of Practice, PDS's Knowledge hub, and community-led initiatives such as Police Rewired. Our communities are also active members of external networks and events, such as DataConnect21, Ordnance Survey Geospatial Hackathon, and the Government Statistical Service Methodology Symposium.

12. To anticipate and respond to future technology threats and opportunities, the College of Policing coordinates a cross-service horizon scanning network that identifies emerging issues, risks, challenges, and opportunities (see, e.g., Future Operating Environment 2040). The NCA's TRACER provides a complementary function for IP Act capabilities across law enforcement and UKIC. Their efforts are supported by the Government Office for Science's 'EmTech' database, an online library of data, analysis, reports, and resources on emerging technologies.

### Oversight and Accountability

13. Chief Constables are responsible for the operational deployment of new technologies to manage threat, harm, and risk. Together with the Police and Crime Commissioner (PCC), they ensure use is fair and lawful, balancing ethics, right to privacy, unbiased treatment and consent, with the absolute right to a fair trial. Thus, decisions are decentralised across 43 Forces and contingent on Chief–PCC relationships. This local discretion is essential to effective delivery. However, it is informed and supported by a system of independent scrutiny, national peer support, and evidence-based guidance, delivered *inter alia* by the following.

14. PCCs, who as representatives of local communities have the primary responsibility for holding Chief Constables to account for the provision of an efficient and effective police service. Their scrutiny and oversight are a critical element of the shared responsibility with Chief Officers for decisions about new technologies. PCCs are supported nationally by the APCC who work with the NPCC to share best practice and identify opportunities for joint working and resource pooling.

15. The strategic view of NPCC coordination committees, particularly the Crime and Operations Committee and the Information Management and Operational Requirements Committee (IMORCC), endorsed by Chief Constables' Council. IMORCC has introduced a new NPCC Data Office, led by a Chief Constable and managed by the new Chief Data Officer. It provides oversight of Data Quality, Data Protection and Freedom of Information, Records Management, information Sharing, Disclosure and Safeguarding, and Geographical Information portfolios.

16. Authorised Professional Practice (APP) issued by the College of Policing. In May 2021, the College published an APP on the extraction of material from digital devices. It provides guidance on ensuring police methods comply with legislation and balance people's rights to privacy and to a fair trial. Similarly, the College is at an advanced stage of developing APP that will set consistent standards on the police use of live facial recognition technology.

17. The new Policing Chief Scientific Advisor who provides independent scientific advice and challenge to ensure decision making and application of new technologies is supported by evidence and insights from academia and industry. For example, under the CSA's leadership, NPCC is appointing a Science Advisory Council (SAC) that will bring together diverse expertise to provide insight and strategic direction at the cutting edge of policing's use of new technologies.

18. Our obligations under the UK National Action Plan for Open Government 2019-2021, which we realise in part by pursuing five Open Science practices: open access, open data, open materials, pre-registration, and citizen science. For example, the College of Policing's What Works Network maintains a repository of research reports (see https://whatworks.college.police.uk/). The community of 'Police Rewired' (see https://www.policecoders.org/) make available their coding projects and utilise data (e.g. from https://data.police.uk) to drive forward innovations accessible to public input and scrutiny.

19. Our efforts to help private technology suppliers adopt open practices in ways that safeguard their Intellectual Property. An infrastructure that enables controlled access to real (not live) police data can accelerate innovation while providing an 'assessment gateway,' which can be assured as representing a fair, non-discriminatory test of the technology. The 'Impact Labs' of the Accelerated Capability Environment are early successful examples of this approach.

20. It is easy to view our system of oversight as unnecessarily complex. However, the federated structure enables local flexibility and accountability while providing redundancy and important checks-and-balances, which support rather than impede local decision making.

**Ethics, Proportionality and Fairness**

21. Chief Constables and PCCs receive detailed advice on ethics from local ethics committees. In the case of data analytics, these are often specialist committees organised by the Force's capability. For example, Thames Valley VRU integrates Public Health England's principles with learning from other data ethics reviews. Their committee works in public, is independently chaired, and includes academic experts in data ethics and medical ethics, as well as from Public Health England, senior officers, technical staff, community representation, and data scientists.

22. A particularly forward-leaning example of an ethics committee is the joint initiative by the West Midland's PCC and West Midlands Police. This committee embodies much best practice: it has independent members recruited openly on merit; it acts independent of operational policing; it combines independent security with collaborative working to find solutions and jointly evolve best practice; it engages with a project throughout its life, recognising that project often need to adapt to emerging concerns; and, it is transparent, among other things publishing all its deliberations for public scrutiny and awareness-raising.

23. To increase resilience on ethics, the NPCC Lead for Ethics and the National Police Ethics Group (NPEG) are, with NCA support, establishing a national Digital and Data Ethics Guidance Group (DDEGG). DDEGG will not replace Force processes but provide national support, particularly on complex cases. Its priorities are to:

(a) foster and enhance ethical policing in the digital and data arena by supporting the development of policy and practice;

(b) ensure the Code of Ethics is effectively adopted and central to all considerations and guidance provided;

(c) support NPEG as the principal conduit between NPCC and Chief Officers, across national, regional and local law enforcement, providing assurance, guidance, and recommendations to Chief Officers or their equivalent;

(d) promote, where operationally appropriate, an ethos of transparency and engagement with the public to maintain and promote trust and confidence.

24. The APCC and NPCC are committed to jointly delivering a national ethics framework that meets the highest standards. Supported by the Chief Scientific Advisor, we will (1) appoint externally recruited, independent members who will represent a diversity of views; (2) support the adoption of best practice tools, such as the CDEI framework for ethical decision making; (3) assure adoption of recommendations from learned bodies,

such as the Biometrics and Forensics Ethics Group, and best practices from Force committees; and (4) consider how best to stimulate wider ethical debate and scrutiny of emerging technologies, be that through an independent Institute and/or joint working with CDEI.

25. Algorithmic fairness refers to the extent a new technology makes predictions that do not systematically disadvantage a group or people. Bias occurs when the data used to build an algorithm over-/under-represents the characteristics of the population it seeks to model. We believe policing—from Chief Constables and PCCs, to ethics committees, to developers—recognise this and its importance for human rights. They take significant mitigation, undertaking careful assessments of data quality (data quality is often cited as the reason for not implementing predictive algorithms), peer review, bias audits, and impact assessments.

26. This consideration extends to wider coordination and investment decisions. The STAR board evaluates funding options using a rigorous peer-review process that considers ethics and fairness. The NPCC Data Board and the PDS Data Office drive the strategic direction on accountability and national expectations for locally held data. The Government Office for Artificial Intelligence's Guidelines for AI procurement inform contract implementation and management.

27. We recognise assessments of fairness must, wherever possible, be informed by experimentation. The Metropolitan Police Service's ten trials of face recognition technology is illustrative of best practice here, affording insights into the (absence of) bias in the technologies use across IC demographic class, but revealing difference performance profiles for men and women (see MetEvaluation.pdf). Currently, the level of resourcing available for experimentation limits policing's ability to understand fully the bias and impact of new technologies.

## Conclusions

28. We are committed to delivering our National Police Digital Strategy without unreasonably delay to the highest standards of scientific rigour in a fair and transparent way. This is best delivered by Force level partnerships that respond to local conditions with guidance and support from APCC, NPCC, PDS, as well as wider academia and industry.

29. The pace at which policing can assess the efficacy and ethics of new technologies is constrained by the resources available to Forces. More resource would unlock Force innovation and enable detailed experimentation and evaluation at pace, which will in turn better inform public debate.

30. Policing is often the 'frontline' that determines public perception by 'doing,' in the absence of wider consultation on legislation and policy. Government should seek to clarify public appetite for new technologies and legislate so that policing has a clearer basis on which to make policies and decisions about deployment.

31. As new technologies offer major ways to prevent crime, so Forces are increasingly having to consider their risk appetite and ambition. We must encourage adoption by establishing confidence in policing that actions, taken fairly and informed by evidence and public opinion, will be supported.

32. The first revision of the Strategy will occur in 2022, allowing policing to generate further common baselines but also consider what new technologies and associated investments should be made. It will also allow policing to further align itself with new Government strategies, such as the National AI strategy, and emerging new technology capabilities in the public and private sector.

*1 October 2021*

## ANNEX 1: Committee Question Cross-Reference

The following table identifies how we have sought to address the Committee's questions.

| Questions | Paragraph |
|---|---|
| 1. Do you know of technologies being used in the application of the law? Where? By whom? For what purpose? | 6, 7<br>Box 1 |
| 2. What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood? | 3, 4, 13, 14 |
| 3. Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers, and members of the public) understand how they work and how they should be used? | 7, 11, 12, 23, 27, 31 |
| 4. How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated? | 2, 29 |
| 5. With regards to the use of these technologies, what costs could arise? Do the benefits outweigh these costs? Are safeguards needed to ensure that technologies cannot be used to serve purposes incompatible with a democratic society? | 2, 15, 27 |
| 6. What mechanisms should be introduced to monitor the deployment of new technologies? How can their performance be evaluated prior to deployment and while in use? Who should be accountable for the use of new technologies, and what accountability arrangements should be in place? What governance and oversight mechanisms should be in place? | 3, 8, 9, 10, 15 - 26 |
| 7. How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks? | 30 |
| 8. How can transparency be ensured when it comes to the use of these technologies, including regarding how they are purchased, how their results are interpreted, and in what ways they are used? | 15 - 22 |
| 9. Are there relevant examples of good practices and lessons learnt from other fields or jurisdictions which should be considered? | - |
| 10. This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend? | 5. 28-31 |