Home Office — Written evidence (NTL0055)

1. We welcome this inquiry and understand that the Committee is particularly interested in:

    a. the use, procurement and monitoring of advanced algorithms – *including Artificial Intelligence, Machine Learning and Data Analytics* - to assist law enforcement; and

    b. the use of new technology in the investigation of crimes with a digital element.

2. This submission accordingly sets out the Government's overall approach to supporting the development of relevant technologies in law enforcement organisations, with specific case studies providing further detail.

3. The public expects the Government to support operational partners in making best use of technology to tackle serious harm such as knife crime, rape and serious sexual assault, child sexual exploitation, terrorism, and other serious offences. We will therefore back and empower the police to use new technologies to deliver operational effect in a way that maintains public trust.

4. The way in which people lead their lives is becoming increasingly digital and this is changing society, criminality, and the communities policing serves. The Government will therefore also support innovation to confront ever more sophisticated criminality, protect people from harm and enable police to work effectively and efficiently in a rapidly changing world.

5. Advanced algorithms that have powerful data processing capabilities, either through their training or programming, are general purpose technologies and are being deployed across economies globally. In policing and the Criminal Justice System (CJS), advanced algorithms are already enabling efficiencies by automating some transactional processes and are showing their potential to augment human intelligence. This is demonstrated by the examples below, where decision making by people is being supported by machines with the ability to process large volumes of data, which could not be done in a manual way to the level of assurance required.

6. We agree with the Justice and Home Affairs Committee that the use of advanced algorithms in law enforcement poses both opportunities and challenges. We also agree with the Home Affairs Committee of the House of Commons that it is vital that we have processes and governance in place to ensure that new technology is used fairly and proportionately. However, we strongly disagree with the characterisation put forward by some that these technologies are being deployed without regard to proper evaluation or engagement, or that we are allowing sensitive decisions to

be delegated to machines in a way that is either contrary to the law or the core principles of the CJS. Moreover, we agree with the position set out in the Metropolitan Police Commissioner's speech to the Royal United Services Institute in February 2020, where she explained that this is about "using a tool that can augment intelligence rather than replace it" and, where algorithms can assist in identifying patterns and drawing critical insight from data, "almost all citizens would want us to use it".

7. The case studies below demonstrate the significant opportunities to use advanced algorithms to improve the speed and quality of investigations, evaluate crime types, identify crime, improve police welfare, and improve customer services. At present, to differing extents, law enforcement organisations in England and Wales use advanced algorithms to support a range of tasks via process automation, predictive modelling, social network analysis and data visualisation. However, organisations are at different stages of advancement and maturity and our analysis suggests that most data analytics used by police forces is currently used to enable organisational effectiveness and resource planning rather than directly to tackle crime.

8. We know that organisations with ambitions to use advanced algorithms in a transformative way must systematically address complex issues around data quality and security; data management; interoperability across systems; specialist skills and resourcing; public engagement; ethics and governance. These needs are reflected in the National Policing Digital Strategy. We are also supporting law enforcement organisations to address risks and issues raised in recent reports by independent bodies, which include the need for transparency, consistency and careful mitigation of the risk posed by any algorithms or automation. These core requirements are not new - policing is committed to being transparent, testing necessity and making judgements about proportionality - and our legal system is generally well able to deal with these issues. However, we recognise that advanced data processing necessitates the development of new skills in policing and those holding them to account, and that effective governance is vital to maintaining public trust.

9. Locally, it is for Chief Constables with Police and Crime Commissioners to lead engagement with the communities they serve and decide when and how to deploy new technologies. However, the policing landscape is structured to ensure that lessons are learned continually and that there is effective ongoing scrutiny and public accountability. We are therefore working with the National Police Chiefs' Council (NPCC), the Association of Police and Crime Commissioners, the College of Policing, Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services and police forces to enable a consistent approach to the evaluation of efficacy and ethics of advanced algorithms.

10. We supported the appointment of the Police Chief Scientific Advisor (CSA), who took up post in June 2021, because ensuring that all technological developments in policing are based on good evidence and the best understanding of science is crucial. Professor Paul Taylor chairs a police science and technology investment board, which demands rigorous quality

assurance of all proposals. He is also represented on the relevant NPCC committees and is developing national research and development guidance with the College of Policing. We will also support the adoption of AI procurement guidance produced by the Government Office for Artificial Intelligence and, more broadly, the principles of open science.

11. We also recognise the need for appropriate coordination of investment decisions across the policing landscape. Therefore, with oversight from the ministerially led Strategic Capabilities and Investment Board, we are supporting the development, mobilisation, and implementation of the 10-year National Policing Digital Strategy to ensure the right infrastructure is in place across policing to harness and exploit the benefits of data and analytical capabilities. Work underway includes:

    - Establishing an NPCC Data Board to promote a consistent approach to developing data literacy; assessing efficacy, ethics; and quality and standards.

    - Establishing a Central Data Office within the Police Digital Service (PDS), which aims to improve data management and sharing across policing. The Data Office will provide the essential infrastructure for the sector to ensure strategic direction, central coordination, and accountability on national expectations of locally held data.

    - Developing a National Data Ethics Governance model, building on the work West Midlands Police (WMP) have done to establish an Ethics Committee (described in more detail below) to advise on data science projects. The national model will also be developed in collaboration with the Centre for Data Ethics and Innovation and the Home Office.

12. The following **case studies** further demonstrate our role in enabling and supporting the development of consistently excellent law enforcement capabilities to address priorities.

National Data Analytics Solution

13. We are funding and developing the National Data Analytics Solution (NDAS) programme to meet the needs of policing. NDAS has developed algorithms on specific crime types that are applied to police-controlled data to produce insights and analysis which inform strategic and operational decision making. WMP host NDAS with an additional seven regional forces and the National Crime Agency currently participating. In one example, NDAS is piloting a use case on Modern Slavery with West Yorkshire Police (WYP). This uses natural language processing, behavioural and network analysis techniques to spot cases of modern slavery which might otherwise have gone undetected.

14. WMP Ethics Committee works with NDAS in an advisory capacity to ensure proper scrutiny and robust evaluation. In the development phase of the

Modern Slavery example, the Committee asked for evidence on mitigation of potential bias. NDAS put together a methodology to manually sample Modern Slavery events which were identified by the algorithm and investigated whether these were flagged based on individuals' characteristics. NDAS also demonstrated how protected characteristics would not be used as a primary or secondary rule in natural language processing before proceeding to operational evaluation as part of the WYP pilot.

Automatic facial recognition and image classification

15. The Committee will be familiar with automatic facial recognition (AFR) from evidence given in oral hearings. AFR is an example of a technology that is being widely adopted for business uses across the UK and, such is the rate of improvement, has reached levels of accuracy where it can be deployed to assist law enforcement. There is therefore a reasonable public expectation, particularly amongst victims and their families, that the police will use it in a carefully controlled way for the prevention, detection, and investigation of crime. This position is supported by polling.

16. AFR's use retrospectively is well established. For example, South Wales Police (SWP) use it to identify facial images captured on CCTV of people suspected of committing a crime. This produces around one hundred identifications a month, with half of those leading to a positive outcome e.g. a caution or a charge. Previously, identification on CCTV would take around fourteen days, whereas now the response is typically within minutes. In one example, which was featured on the BBC's Crimewatch programme, SWP used it to quickly identify a man caught by CCTV trying to abduct a woman on a street late at night. They were able to arrest him before he could commit further offences. This use of AFR also brings considerable financial savings, which SWP estimated at around £230,000 a year. However, they have found the investigatory benefits to early identification to be much greater, particularly for property and contact crime.

17. Police officers have always been able to spot a person who is wanted for a crime and then use their powers to stop them in the street. However, human reliability in matching faces can be impinged by various factors, including bias. It is therefore beneficial in certain circumstances to use carefully tested matching algorithms in live facial recognition (LFR) to assist police officers in identifying wanted people in crowded spaces. LFR helps because it can scan large crowds against a carefully constructed watchlist in real time, instantly eliminating the vast majority and highlighting a small number of people of potential interest for police officers to consider approaching. Where the system does not produce an alert for a possible match, the biometrics of those captured by the system are deleted near-instantaneously. Possible matches are also reviewed by trained officers before any intervention takes place.

18. SWP's LFR trials, which were evaluated by Cardiff University, have resulted in over 60 arrests for offences including robbery, violence, theft

and court warrants. Separately, the Metropolitan Police Service's trials resulted in eight arrests, including a double count of rape, false imprisonment, breach of a non-molestation order, assault on police and discharge of a firearm. In one example, LFR was used by SWP at a music event in Cardiff because similar concerts had resulted in more than 220 mobile phones being stolen from people attending. Thirty people who were thought to be part of an organised crime group who specialise in stealing phones at music events were placed on a watchlist, resulting in one person being arrested for going equipped to steal and there were no reports of any mobile phone thefts.

19. AFR is also a useful lens through which to assess the current legal framework which, to be effective, must protect people's rights and enable innovation as technology advances. Through the Department for Digital, Culture, Media and Sport's Data Reform consultation, we are currently seeking views on proposals to simplify oversight of police use of biometrics; make it easier to amend the rules on collection, retention and use of biometrics, as new technologies emerge; and develop a Code of Practice on police use of emerging technologies. Our view is that these changes would enhance what is an already comprehensive legal framework for the use of technology by law enforcement in England and Wales. This framework places important obligations on those responsible for its deployment, including the need to undertake Data Protection and Equality Impact Assessments. The framework also has provisions to regulate automated decision making where there are significant implications for the individuals affected.

20. The framework includes police common law powers to prevent and detect crime, the Data Protection Act 2018, Human Rights Act 1998, Equality Act 2010, the Police and Criminal Evidence Act 1984 (PACE), the Protection of Freedoms Act 2012 (POFA), and law enforcement bodies' own published policies.

21. As described above, we recognise the importance of our role in enabling and supporting a consistently excellent and transparent approach to the use of advanced algorithms. For example, the Court of Appeal's recognition in its ruling (August 2020) in *Bridges vs South Wales Police* confirmed that there is an existing legal framework for police to use LFR. However, they found that SWP needed to provide more clarity about the categories of people they were looking for, and the criteria for determining when they might use LFR. The Court also found that SWP did not comply with the Public Sector Equality Duty because they did not take reasonable steps to demonstrate the lack of bias in the facial matching algorithm, even though they have found no evidence of it.

22. We are therefore working with the NPCC to improve governance around the development of facial recognition capabilities and biometrics, as well as advanced algorithms more broadly. With respect to LFR, this approach has assisted the College of Policing in producing national guidance to enable a consistent approach.

23. Combining the best of AI technology and human expertise in a collaborative team-based approach can also help achieve results in the investigation of evidence in the investigation of crime. For example, the Child Abuse Image Database (CAID) Programme, working with industry on behalf of and with law enforcement partners, has developed and trialled an AI-assisted image classifier which helps to speed up the process of identifying new Indecent Images of Children (IIOC). This is a key tool in protecting officer welfare and speeding up investigations.

24. The CAID Programme has also deployed AFR to assist officers working with IIOC, helping them to identify victims and offenders. It searches the facial images on CAID to help spot previously unknown links between different cases, which might otherwise have gone undetected. The Programme consulted with industry and government experts before introducing this capability and carried out rigorous testing with operational users, who are supported with guidance. All potential matches are reviewed carefully by trained officers before any action is taken.

Digital forensics

25. The proliferation of digital devices into every part of society, the fact that the majority of crimes have a digital element, and the corresponding increase in data volumes mean that solving the data challenge in digital forensics is particularly urgent. The NPCC/APCC Digital Forensic Science Strategy addresses the core issues, and we are working with the police-led Transforming Forensics programme and policing in England and Wales's forensics co-ordinating body (the Forensic Capability Network (FCN)) to address the problems in a co-ordinated way.

26. The Government's recent End-to-end rape review report detailed the importance of effective systems, processes and training to effectively manage the gathering, analysis and disclosure of digital material in the investigation and prosecution of Rape and Serious Sexual Offences. In order to increase the confidence of victims in the criminal justice process, with fewer cases failing due to issues with digital evidence and disclosure, we are seeking to ensure a consistently proportionate approach. We need to enable officers and staff to carry out timely and high-quality investigations, whilst ensuring that digital evidence has forensic integrity and is presented clearly to support the CJS. It is within this context that we are approaching the technology challenge, in tandem with legislation.

27. The volume and complexity of the data held on mobile devices means that machine assistance is increasingly needed to assist police officers in extracting only the information that is strictly necessary and proportionate. Whilst there are technology providers who are confident that they can help solve specific problems, our strategy, working closely with stakeholders, the Crown Prosecution Service, NPCC, Transforming Forensics and the Police Digital Service has been to carefully define the problem from end- to-end and the outcomes required. We are also working to strengthen partnerships with industry in a co-ordinated way, so that we can be confident that the technology solutions adopted have all

been subject to consistent and rigorous testing, evaluation and validation.

28. In parallel, the Police Crime Sentencing and Courts Bill establishes a statutory basis for the extraction of information from digital devices. It also introduces clear safeguards to protect the privacy of victims, witnesses, and others. These powers can only be exercised where the police reasonably believe that the device contains relevant information, or is relevant to a reasonable line of enquiry, and be satisfied that the use of these powers is necessary and proportionate. These clauses and a supporting code of practice will complement the deployment of new technology by ensuring that the protection of victims' rights is placed at the centre of all investigations and that police do not take information from victims' digital devices as a matter of course.

29. More broadly, to ensure the transparency and consistency of digital evidence entering the CJS, we have given the Forensic Science Regulator statutory powers through the Forensic Science Regulator Act 2021. This will empower the Regulator to take enforcement action and drive up compliance with a comprehensive Code of Practice and internationally recognised standards. We have also provided funding to Transforming Forensics and the FCN to work directly with policing to support accreditation and uplift capacity where appropriate. This will ensure that only validated and accredited methods are used in the CJS.

30. We trust this submission is helpful to the Committee's inquiry.

11 November 2021