House of Commons

Science and Technology Committee

Work of the Biometrics Commissioner and the Forensic Science Regulator: Government Response to the Committee's Nineteenth Report of Session 2017–19

Third Special Report of Session 2019–21

Ordered by the House of Commons to be printed 16 March 2021

HC 1319
Published on 19 March 2021
by authority of the House of Commons

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Greg Clark MP (*Conservative, Tunbridge Wells*) (Chair)

Aaron Bell MP (*Conservative, Newcastle-under-Lyme*)

Dawn Butler MP *(Labour, Brent Central)*

Chris Clarkson MP (*Conservative, Heywood and Middleton)*

Katherine Fletcher MP (*Conservative, South Ribble*)

Andrew Griffith MP (*Conservative, Arundel and South Downs*)

Mark Logan MP (*Conservative, Bolton North East*)

Rebecca Long-Bailey *(Labour, Salford and Eccles)*

Carol Monaghan MP (*Scottish National Party, Glasgow North West*)

Graham Stringer MP (*Labour, Blackley and Broughton*)

Zarah Sultana MP (*Labour, Coventry South*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO. No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/science and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are: Masrur Ahmed (Second Clerk), Dr Harry Beeson (Committee Specialist), Dr Christopher Brown (Committee Specialist), Dr James Chandler (Committee Specialist), Emma Dobrzynski (Committee Operations Officer), Sonia Draper (Committee Operations Manager), Danielle Nash (Clerk), Robert Paddock (POST fellow), and Emily Pritchard (Senior Media and Communications Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, House of Commons, London, SW1A 0AA. The telephone number for general inquiries is: 020 7219 2793; the Committee's e-mail address is: scitechcom@parliament.uk.

You can follow the Committee on Twitter using @CommonsSTC.

Third Special Report

On 18 July 2019 our predecessor Committee published its Nineteenth Report of Session 2017–19, *The work of the Biometrics Commissioner and the Forensic Science Regulator* [HC 1970]. On 9 March 2021 we received the Government's response to the Report, which is appended below.

Appendix: Government Response

Dear Committee Chair,

Biometrics Commissioner and Forensic Science Regulator Report

In the 2017 Parliamentary session, the Science and Technology Committee published its report on the work of the Biometrics Commissioner and Forensic Science Regulator. With apologies for the long delay, please find enclosed the Government response to the Committee's conclusions and recommendations, which also provides updates and information on our commitment to empower the police to use new technologies like biometrics, while maintaining public trust.

KIT MALTHOUSE

BARONESS WILLIAMS

Committee's Conclusions and Recommendations

The Government welcomes the House of Commons Science and Technology Select Committee's report. Much has happened since it was issued. For example, on forensics we are supporting Darren Jones' Bill to give the regulator statutory powers, and are investing in a standing national policing capability (the Forensic Capability Network and associated Transforming Forensics programme). On biometrics, we have had the Court of Appeal judgment on live facial recognition and the Government has committed to empower the police to use new technologies like biometrics while maintaining public trust, where the Committee's report has helped to highlight some of the key issues. The following sections provide responses to the Committee's conclusions and recommendations in detail, including updates on legal and policy developments, including the Court of Appeal judgment on the use of live facial recognition.

Forensics

It is wholly unacceptable that the forensics market has—once again—come perilously close to collapse in the year since we published our Report. We remain seriously concerned about the long-term viability of the market for forensic science services and the significant risk that this poses to the effective functioning of a criminal justice system. It is encouraging that the Home Office did, eventually, accept our recommendation to review the sustainability of the forensics market. However, the implementation plan for the joint review of forensics provision (2018), published in April 2019, does not appear to propose measures that would adequately address many of the market stability challenges in the forensic services market. (Paragraph 14)

1. We accept that market instability has for too long impacted negatively on the delivery of forensic science into policing and the criminal justice system. The Government is committed to maintaining and improving our world-class forensic services and supporting the forensic scientists who work in them. We have worked closely with the police and other stakeholders to stabilise the forensics market and will continue to strengthen capabilities through investment in the police-led Transforming Forensics programme.

2. The programme has established a nationally networked forensics capability called the Forensics Capability Network (FCN), which opened in April 2020. The FCN will enable police forces to maximise economies of scale, manage commercial risks, and deliver consistent quality into the justice system. We will also ensure that the Regulator has the powers required to improve quality standards by supporting legislation to put the role on a statutory footing.

3. The 2018 Joint Review and implementation plan committed us to secure sustainable funding and commercial models and to encourage investment, in order to stabilise the market, and ensure the needs of the CJS were met. The plan highlighted that a specialist team had been established (now part of the FCN) to manage and develop the market; manage commercial strategy; manage contracts; co-ordinate capability building and provide long-range demand forecasts so that all provision needs can be met efficiently and sustainably. This was an important and necessary first step towards ensuring market stability.

4. The long-term stability of provision is a priority and we have invested £28.6m in forensics capabilities in 2020/21, and are investing a further £25.6m in 2021/22. The specialist commercial team in the FCN serves all 43 territorial police forces. They are addressing the fragility of niche services and producing a workforce strategy for developing the overall skill base as a priority. The FCN is also leading implementation of a long-term marketplace plan, which is being developed with input from CJS partners and stakeholders.

5. The onset of covid-19 led to a sharp drop in submissions from police forces to forensic service providers in some disciplines, which left unchecked would have further destabilised the market. However, The NPCC, APCC and FCN worked effectively with providers to manage this risk until submissions return to normal levels.

6. It is also important to note that the UK's mixed model of private and public provision has allowed for a more flexible approach to delivering forensic services. For example, the ransomware attack on Eurofins Forensic Services in June 2019 had a negative impact on capacity, which policing and CJS partners worked hard to mitigate. At the height of the Eurofins incident, all forces were able to continue with the highest priority cases due to effective sharing and reallocation of resources. This would not have been possible with a single-supplier model.

The Government should work with the Forensic Science Regulator to develop her proposals for a National Forensic Science Capability. This should focus on those forensic disciplines where skills were threatened and/or already insufficient. The National Forensic Science Capability should also ensure that cyber security standards and protection are strictly applied and secure data back-up of information is routinely and securely stored. (Paragraph 15)

7. Our investment in the FCN will provide policing with the expertise and support needed to build and maintain nationally networked forensics capabilities in England and Wales, including helping forces manage the increasing complexity and demand for digital forensics.

8. We are working closely with the Ministry of Justice, Attorney General's Office and other key stakeholders across the CJS to deliver a forensic science reform programme to strengthen forensics provision and address key risks and issues. This is being overseen by the Criminal Justice Board (CJB) Forensics Sub-Group, of which the Regulator is a vital member.

9. The reform programme tackles four key areas: regulation of forensic provision, including putting the Regulator on a statutory footing and an assessment of the legal framework for the collection and retention of digital forensics; CJS capabilities, which will seek to improve the transparency of expert witness skills and qualifications and ensure that legal practitioners fully understand the science presented in courts; improved police capabilities through the NPCC Transforming Forensics Programme and Forensic Capability Network; and a research and development strand to identify current and future research needs, and coordinate research priorities across the CJS.

10. The CJB Forensics Sub-Group will evaluate the success of the reform programme according to four tests: that police, prosecution and defence in criminal proceedings are adequately, sustainably and proportionately served by high quality scientific analysis of the relevant evidence; that evidence is collected, handled and analysed in accordance with the Regulator's codes and standards; that evidence is clearly presented and explained by experts to the Court; and that policing and the CJS benefit from the most relevant advances in science and technology.

11. On the specific issue of cyber security, following the ransomware attack on Eurofins, the Regulator worked with the National Cyber Security Centre to develop requirements for cyber security which could be incorporated into her Code of Practice. A draft text was published as Regulatory Notice 02/2020 on 1 August 2020 and will be incorporated in the next issue of the Code. We will continue to monitor developments in tandem with the Regulator's office and colleagues in policing.

In the face of an unstable forensics market which has been on the brink of collapse, and the clear need to uphold quality standards across forensic services, the Regulator—now more than ever—needs statutory powers. The Government professes to "strongly support" the Forensic Science Regulator Bill yet it has not taken any active steps to facilitate its passage through Parliament. Nor are we reassured that it has contingency plans in place to ensure a similar Bill is afforded a legislative slot in the next Parliamentary session. This is unacceptable. The Government has failed to show leadership and pass what is ultimately an uncontroversial piece of legislation, but which is vital for the effective administration of justice. (Paragraph 21)

The Home Office should apply for a legislative slot for a Forensic Science Regulator Bill in the next Parliamentary Session and not rely on backbench Members to get the Bill through Parliament. Legislation is needed not only to put the Forensic Science Regulator on a statutory footing but also on the use of forensics in the civil and family courts. The Bill should include: i) Prohibition on the police using non-accredited laboratories; and

ii) All in-house police laboratories should be accredited within a year. (Paragraph 22)

12. We agree and accept that the Regulator needs statutory powers, hence we have given full support to the Darren Jones MP Private Members' Bill that is currently progressing through Parliament.

13. We do not agree that the Bill should include a prohibition on police use of non-accredited laboratories; and that all in-house police laboratories should be accredited within a year. The independence of the Regulator is key to ensuring accountability and oversight of the provision of forensic science services. We believe that creating such a statutory prohibition and obligation would detract from the independence of the Regulator. The legislation will give the Regulator the discretion and ability to act when they have a concern about the way in which forensic science activities are carried out.

14. The FCN's specialist quality management team is supporting forces' efforts to gain accreditation by validating new techniques and creating standard operating procedures. We expect this investment to drive significant improvement over the next 12 months.

Biometrics

The Government's 27-page biometrics strategy was not worth the five-year wait. Arguably it is not a 'strategy' at all: it lacks a coherent, forward looking vision and fails to address the legislative vacuum that the Home Office has allowed to emerge around new biometrics. Ultimately, it represents a missed opportunity for the Government to set out a principles-based approach for the use and oversight of second generation biometrics. Simply establishing an oversight board, with no legal powers, is not good enough given the highly intrusive nature of the technologies. Further, the development and use of biometric technologies must be transparent and involve as much public awareness and engagement as possible, to ensure that there is public trust in the technologies. Unfortunately, public engagement has been sorely missing from the Home Office's approach to date. Its ongoing 'consultation' on the governance of biometrics has no published terms of reference and there is no obvious way for interested parties to participate. This is not good enough. (Paragraph 27)

The UK Government should learn from the Scottish Government's approach to biometrics and commission an independent review of options for the use and retention of biometric data that is not currently covered by the Protection of Freedoms Act 2012. The results of the review should be published along with a Government Response, and a public consultation on the Government's proposed way forward should follow. This process should culminate in legislation being brought forward that seeks to govern current and future biometric technologies. (Paragraph 28)

There is growing evidence from respected, independent bodies that the 'regulatory lacuna' surrounding the use of automatic facial recognition has called the legal basis of the trials into question. The Government, however, seems to not realise or to concede that there is a problem. (Paragraph 36)

We reiterate our recommendation from our 2018 Report that automatic facial recognition should not be deployed until concerns over the technology's effectiveness and potential bias have been fully resolved. We call on the Government to issue a moratorium on the

current use of facial recognition technology and no further trials should take place until a legislative framework has been introduced and guidance on trial protocols, and an oversight and evaluation system, has been established. (Paragraph 37)

We recommend that the Home Office should issue guidance on Automatic Facial Recognition Trials when it introduces a legislative framework for these trials and that trials must be of a scientific standard. (Paragraph 38)

15. Biometrics, such as DNA, fingerprints and increasingly facial images, are critical tools for delivery of public safety and efficient public services. The Biometrics Strategy set out how the Home Office and its partners currently use biometrics, the approach to future developments, and the overarching framework for considering and deciding on new biometric technologies, but did not seek to outline all future uses of biometrics in this fast-evolving space.

16. The public expects the Government to support operational partners in making use of these technologies to tackle serious harm such as knife crime, child sexual exploitation, terrorism and other serious offences. The Government will therefore back the police by empowering them to use these technologies in a way that maintains public trust.

17. There is already a comprehensive legal framework for the management of biometrics, including facial recognition. This includes police common law powers to prevent and detect crime, the Data Protection Act 2018 (DPA), the Human Rights Act 1998, the Equality Act 2010, the Police and Criminal Evidence Act 1984 (PACE), the Protection of Freedoms Act 2012 (POFA), and police forces' own published policies. In terms of oversight and regulation, the Information Commissioner's Office (ICO) regulates compliance with the DPA, including police use and retention of biometrics and POFA created the Surveillance Camera Commissioner and Biometrics Commissioner roles, and the Forensic Information Databases Service strategy board, which oversees the police DNA and fingerprint databases. PACE also provides specific powers for police to collect DNA, fingerprints and custody images and sets out the data retention regime for DNA and fingerprints. There is also an agreed regime for the retention, review and deletion of custody images laid out in the College of Policing's Authorised Professional Practice (APP) on the Management of Police Information.

18. While it is a strong framework, as described in detail above, the Government recognises that it is complex for the police and public, and so could arguably inhibit the confident adoption of technologies that can help us improve public safety and keep up with the pace of technological change.

19. As part of that consideration the Government will continue to work with relevant partners, and in particular will watch with interest how the Scottish Government's legislation, which created a Biometrics Commissioner for Scotland, evolves. Whilst no Commissioner has yet been appointed, their ability to issue codes of practice on Police Scotland's use of biometrics is one that replicates many of the principles that already exist in data protection and human rights legislation across the UK.

20. The Government welcomed the Court of Appeal's recognition in its ruling in *Bridges vs South Wales Police* (SWP), believed to be the first legal case on facial recognition in the world, which confirmed that there is an existing legal framework made up of legislation

and published local police policies. This framework allows the police to exploit new technologies, including biometric identification and overt surveillance, for a policing purpose and where necessary and proportionate.

21. The Court of Appeal 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 it. It 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. In taking forward the ruling and recognising the complex environment, the Government is working with partners to produce national College of Policing guidance on the use of live facial recognition (LFR), consistent with the Bridges' judgment, and has taken steps to simplify the oversight landscape by appointing Fraser Sampson, on a full-time basis, to take on the existing functions of the part-time Biometrics Commissioner and Surveillance Camera Commissioner roles.

23. Looking more broadly, facial recognition technology has been widely adopted for business uses across the UK and has reached a level at which it can be effectively deployed for law-enforcement purposes for both live and retrospective matching. There is therefore a reasonable expectation in the public, particularly amongst victims and their families, that the police will use it for the prevention, detection and investigation of crime.

24. Police use of facial recognition retrospectively is well established. For example, SWP use it to identify facial images captured on CCTV of people suspected of committing a crime. This has produced around one hundred identifications a month, with half of those leading to a positive outcome (caution, charge, etc), ranging from murder suspects to deceased persons. Before using this technology, identification would take around fourteen days, whereas now the response to the officer is mostly within the same day but typically within minutes. This brings considerable financial savings, which SWP estimated at around £230,000 a year; but they have found the investigatory benefits to early identification to be much greater, particularly for property or contact crime.

25. For LFR the Government supports the trials conducted by SWP and the Metropolitan Police Service (MPS), and does not agree that there should be a moratorium or an outright ban. This support is reflected in polling which shows public support for LFR, particularly for its use against violent crime. Some people have, however, expressed concerns including on privacy, accuracy, and effectiveness.

26. Police officers have always been able to use their training and skills to spot a person who is wanted for a crime and then use their powers to stop them in the street. The difference with the use of LFR is the ability in real time to scan large crowds against a large watchlist, instantly eliminating the vast majority and highlighting a small number of people of potential interest for the police 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, which the Court of Appeal noted was an important safeguard.

27. The trials showed that if you are not on a watchlist the chances of the system producing a false alert are at most 1 in 1,000, with an even smaller chance of being approached by a police officer. Importantly, a human operator always takes the final decision on whether to

engage an individual when there has been an alert. SWP found the chances of someone on the watchlist passing the camera being identified were over 80% at a trial in 2019, before their technical upgrade. This is a level of performance that police officers could never achieve on their own, and the technology is improving quickly.

28. SWP's LFR trials resulted in over 60 arrests for offences including robbery, violence, theft and court warrants, before covid intervened. To give one specific example, it was used at a music event in Cardiff. Similar concerts in other parts of the UK 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 watch list, resulting in one person being arrested for going equipped to steal and there were no reports of any mobile phone thefts. Separately, the MPS' 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.

Since the Committee published its Report in 2018, progress has stalled on ensuring that the custody images of unconvicted individuals are weeded and deleted. It is unclear whether police forces are unaware of the requirement to review custody images every six years, or if they are simply 'struggling to comply'. What is clear, however, is that they have not been afforded any earmarked resources to assist with the manual review and weeding process. The Minister previously promised improvements to IT systems that would have facilitated automatic deletion. Such improvements now appear to have been delayed indefinitely. As such, the burden remains on individuals to know that they have the right to request deletion of their image. As we stated in 2018, this approach is unacceptable and we agree with the Biometrics Commissioner that its lawfulness requires further assessment. (Paragraph 44)

Police forces should give higher priority in the allocation of their resources to ensure a comprehensive manual deletion process of custody images in compliance with national guidance. In turn, the Government should strengthen the requirement for such a manual process to delete custody images and introduce clearer and stronger guidance on the process. In the long-term the Government should invest in automatic deletion software as previously promised. (Paragraph 45)

29. Custody images play an important role in the detection and prevention of crime and PACE provides police with specific powers to collect facial images in custody suites. The regime for the retention, review and deletion of custody images is set out in the Review of the Use and Retention of Custody Images 2017. Anyone detained but not ultimately convicted of the offence in relation to which custody images were taken can request the deletion of their custody image after the investigations or proceedings have concluded, with a presumption in favour.

30. To support implementation of this policy, the Home Office has been working with the police to produce guidance for all people going into custody setting out the right to request deletion of their custody images, which will issue shortly, and has stressed to the police the importance of compliance with the existing policy.