



House of Commons
Science and Technology
Committee

**Biometrics strategy and
forensic services**

Fifth Report of Session 2017–19

*Report, together with formal minutes relating
to the report*

*Ordered by the House of Commons
to be printed 23 May 2018*

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

[Norman Lamb MP](#) (*Liberal Democrat, North Norfolk*) (Chair)

[Vicky Ford MP](#) (*Conservative, Chelmsford*)

[Bill Grant MP](#) (*Conservative, Ayr, Carrick and Cumnock*)

[Darren Jones MP](#) (*Labour, Bristol North West*)

[Liz Kendall MP](#) (*Labour, Leicester West*)

[Stephen Metcalfe MP](#) (*Conservative, South Basildon and East Thurrock*)

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

[Damien Moore MP](#) (*Conservative, Southport*)

[Neil O'Brien MP](#) (*Conservative, Harborough*)

[Graham Stringer MP](#) (*Labour, Blackley and Broughton*)

[Martin Whitfield MP](#) (*Labour, East Lothian*)

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 relevant [inquiry page](#) of the Committee's website.

Committee staff

The current staff of the Committee are: Simon Fiander (Clerk); Yohanna Sallberg (Second Clerk); Dr Harry Beeson (Committee Specialist); Seb Motala (Committee Specialist); Martin Smith (Committee Specialist); Sonia Draper (Senior Committee Assistant); Julie Storey (Committee Assistant); and Sean Kinsey (Media 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.

Contents

Summary	3
1 Background	5
Our inquiry	6
2 Forensics	7
Procurement, and market sustainability	7
Standards and accreditation	9
The Radox case	11
Civil courts	12
Statutory powers	13
Forensics strategy and oversight	14
3 Biometrics	16
The Biometrics Strategy	16
Deletion of facial images from police databases	17
Facial recognition and ‘watch lists’	20
Oversight structures	21
Conclusions and recommendations	24
Formal minutes	27
Witnesses	28
Published written evidence	28
List of Reports from the Committee during the current Parliament	29

Summary

In March 2016, the Government published its Forensic Science Strategy—more than two years after the date originally promised by the Government. It came without a ‘Biometric Strategy’ that had been originally planned to complement it. It is now more than four years since the Government originally promised to produce a strategy on biometrics. The Minister has now told us that the Biometrics Strategy will be published in June this year. This report flags up issues that the Biometrics Strategy should take on board. We also take the opportunity to review the situation in forensics services, 18 months after our predecessor Committee’s report on the Forensics Strategy.

On forensics, there have been concerns about the sustainability of the market, with the collapse of private sector providers in recent months. The overarching focus in the police’s forensics procurement appears to be on low price. Problems of fragmentation of forensics testing remain, where testing is split between different providers. The Government should review the sustainability of the forensics market as part of a wider review of its Forensics Strategy, including the underlying causes of market unsustainability and fragmentation.

Accreditation of forensics providers remains vitally important in maintaining the confidence of the courts and the public in the evidence used in the criminal justice system, but not all providers are meeting the Regulator’s accreditation deadlines. The Radox case last year has demonstrated the importance of all forensic providers becoming fully accredited and of the need for rigorous auditing of standards compliance. The case also pointed to a more fundamental disconnect of standards and regulatory systems between the criminal courts (which are covered by the Regulator’s remit) and civil courts (which are not). The Forensics Regulator should work with the UK Accreditation Service to strengthen auditing. The Government should give the current private members’ Forensic Science Regulator Bill, which it has drafted, time in its legislative programme in order for it to make progress, and rapidly implement it following Royal Assent.

We welcome the Government’s commitment to make the Regulator a ‘prescribed person’ under the whistle-blowing legislation, which should happen as soon as her position is put on a statutory footing.

The Ministry of Justice should work with the Home Office and the Forensics Regulator to examine the scope for the Regulator’s remit to be extended to the civil courts forensics system, or for a similar regulator to be established with a similar remit, to bring a comprehensive and enforceable standards system to that sector also.

The Forensics Strategy requires re-evaluation. The Government should revise, re-issue and consult on a new version, and in doing so address the forensics requirements of the civil courts, as well as the criminal justice system.

On Biometrics, the Government’s rationale for the more than four years’ delay in producing a Strategy is less than convincing. It must now produce the Strategy in June, without any further delay.

The courts ruled in the 2012 ‘RMC’ case that it is unlawful to hold custody images without making a distinction between those who are convicted and those who are not.

In response, the Home Office has introduced a system for unconvicted individuals to be able to request the deletion of their images, but not an automatic deletion system, reflecting current weaknesses in IT systems and a concern about the potential cost of a comprehensive manual deletion process. The Government's approach is unacceptable because unconvicted individuals may not know that they can apply for their images to be deleted, and because those whose image has been taken should not have less protection than those whose DNA or fingerprints have been taken.

The Government must ensure that its planned IT upgrade is delivered without delay to introduce a fully automatic image deletion system for those who are not convicted. If there is any delay in introducing such a system, the Government should move to introduce a manually-processed comprehensive deletion system as a matter of urgency. The forthcoming Biometrics Strategy must address which of these possible routes will be followed. The Strategy should also set out the Home Office's assessment of the lawfulness of its deletion-on-application response to the 'RMC' case, and the legal advice underpinning that assessment.

Facial image recognition provides a powerful evolving technology which could significantly help policing. There are concerns, however, over its current use, including its reliability and its potential for discriminatory bias. We welcome the Government's assurances that the technology is only being used at the moment for targeting those on 'watch lists' rather than as a blanket approach. The technology should not be generally deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved. Ministers and Parliament, rather than the police, should take the final decision on any wider deployment. The Biometrics Strategy should include an undertaking that the House will be given an opportunity to debate and vote on the issue.

There are important ethical issues involved in the collection, use and retention of facial images in particular because they can easily be taken and stored without the subject's knowledge and because various image databases already include 90% of the adult population between them. We welcome the Minister's decision to set up a facial images 'oversight Board'. The forthcoming Biometrics Strategy should consider how image databases should be managed and regulated, potentially by a dedicated 'Regulator' or by the Biometrics Commissioner with an extended remit.

Our brief inquiry has identified an urgent and significant need for action on the governance and oversight of both forensics and biometrics. This is vitally important because these disciplines, and the way their techniques and data are used, are at the heart of our courts system and underpin essential confidence in the administration of justice.

1 Background

1. In March 2016, the Government published its Forensic Science Strategy.¹ Our predecessor Committee had significant concerns about it. The Strategy was published more than two years after the date originally promised and had no “coherent vision for forensic services [or] a route-map to deliver it”. The Committee concluded that:

The [Forensics Strategy] document leaves too many issues under-developed to constitute a coherent description of the Government’s policy and direction in this important area. The Government should now aim, on the back of the hopefully imminent publication of its long-awaited Biometrics Strategy and the conclusion of the police’s currently underway forensics ‘scoping work’, to present a revised ‘draft Forensic Strategy’ for a full public consultation.²

The previous Committee highlighted the risks to the sustainability of the forensics market and an inconsistency in the forensics procurement approaches rehearsed in the Strategy.

2. In February 2017, two staff at a private-sector toxicology forensics lab—Radox Testing Services in Manchester—were arrested for manipulating test results. The then Home Office minister, Brandon Lewis MP, told the Committee that the Forensic Science Regulator, Dr Gillian Tully, was undertaking a review to identify the lessons of the case.³ Subsequently, in November 2017, the Regulator wrote to us (and gave us a private briefing) to provide further information on the case and its implications.⁴ She explained that a large number of criminal cases would be affected, along with civil court cases, by the malpractice and that systems for regulating the quality of forensics work would have to be reassessed. In April 2017, a digital forensics supplier, Forensic Telecommunications Services, ceased trading.

3. The 2016 publication of the Forensics Strategy came without a ‘Biometric Strategy’ that was originally planned to complement it. It is now more than four years since the Government originally promised to produce a strategy addressing biometrics. In February 2017, the Home Office published its Custody Images Review,⁵ following a 2012 ruling by the High Court that convicted and unconvicted individuals should be treated differently in terms of the retention of their custody images. Meanwhile, there has continued to be controversy about the police’s use of facial recognition technology to identify wanted individuals at the Notting Hill Carnival and other events.

1 Home Office, [Forensic Science Strategy: A national approach to forensic science delivery in the criminal justice system](#), Cm 9217 (March 2016)

2 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, p3

3 [Letter from Brandon Lewis MP](#), Minister for Policing and the Fire Service, Home Office, on Radox Testing Services (March 2017)

4 [Letter from Dr Gillian Tully](#) on Radox Testing Services (November 2017)

5 Home Office, [Review of the use and retention of custody images](#) (February 2017)

Our inquiry

4. Against that background we decided to take evidence from the Forensics Regulator on the lessons of the Radox case and on developments since the Forensics Strategy was published in 2016, and from Baroness Williams of Trafford, the current Home Office minister for countering extremism, about the still outstanding publication of a Biometrics Strategy and how the management of facial images is being taken forward.

5. The Minister has now told us that the Biometrics Strategy will be published in June this year.⁶ We aim in this brief report to flag up issues that the Biometrics Strategy should take on board (Chapter 3). We also take the opportunity to review the situation in forensics services, 18 months after our predecessor Committee's report and in the light of recent difficulties at some testing facilities (Chapter 2). **The main result of our inquiry is that there is a need not just for the long-delayed Biometrics Strategy, but also a reassessment and revision of the 2016 Forensics Strategy. Our brief inquiry has identified an urgent and significant need for action on the governance and oversight of both forensics and biometrics. This is vitally important because these disciplines, and the way their techniques and data are used, are at the heart of our courts system and underpin essential confidence in the administration of justice.**

2 Forensics

6. Our predecessor Committee’s examination of the 2016 Forensics Strategy found that it was vague about how the police’s locally-negotiated procurement of forensic services would deliver the proposed ‘more consistent national approach’ on procurement, against a background of shrinking workloads for most types of forensics work (the main exception being digital forensics). The Committee also highlighted the challenge faced by some police forces in securing accreditation for their forensic laboratories, and urged the Government to give the Regulator statutory powers to be able to enforce quality standards at all forensics providers.⁷ We revisit these issues in this Chapter.

Procurement, and market sustainability

7. Our predecessor Committee reported in 2011 a then “widespread view that the forensics market was fragile”. The Committee was concerned about the police increasingly undertaking forensic science work, which could distort the market “by the police customer increasingly becoming the competitor”.⁸ In a 2013 follow up report, concerns were raised about “the willingness and capacity of private forensic providers to operate and invest in that market”.⁹ On the other hand, the Committee also highlighted the risk of forensics work that was previously done by the police being contracted from private sector providers in a way that resulted in tests related to criminal cases being split between different providers. In 2013, Dr Tully (then working at a private forensics company, but subsequently to become the Forensic Sciences Regulator) warned about such “dangers of fragmentation in procurement”.¹⁰ The Government’s response was that: “The [national procurement framework for forensics] does not, in itself, lead to fragmentation, as sole suppliers can be (and are) used on any one case. Cases do not need to be split or fragmented between suppliers. In fact, it would be very unusual for individual cases (especially major cases) to be split across suppliers.”¹¹

8. In the Committee’s subsequent 2016 inquiry, on the Forensics Strategy, Dr Tully, by then the Forensic Science Regulator, commented that: “Looking at the [Forensics] Strategy, it does not seem, from my reading of it, that it provides stability or certainty for forensic science providers going forward.”¹² The Strategy had emphasised the potential advantages of new local ‘partnership’ approaches to procurement, but our predecessor Committee had highlighted uncertainty about how this would be carried through into the ‘national approach’ also advocated by the Strategy.¹³ Since then, the capacity of private sector providers has been reduced. In 2017, a textile fibre laboratory, Contact Traces, closed; as did a digital forensics supplier, Forensic Telecommunications Services. Dr Tully told us that the Forensic Archive took possession of some of the latter company’s test-result material on a temporary basis.¹⁴ It was reported in January 2018, that another firm—

7 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, para 63

8 Science and Technology Committee, [The Forensic Science Service](#), Seventh Report, Session 2010–12, HC 855

9 Science and Technology Committee, [Forensic science](#), Second Report, Session 2013–14, HC 610

10 Science and Technology Committee, [Forensic science](#), Second Report, Session 2013–14, HC 610

11 Home Office, [Government response to the Second Report from the Science and Technology Committee: Forensic science](#), Cm 8750 (November 2013)

12 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, para 22

13 [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, paras 19–23

14 Q11

Key Forensic Services—almost collapsed before being bought, and the police had to pay to keep it operational for a three-month period while outstanding contracted work was completed.¹⁵

9. The Regulator, in her latest Annual Report in January 2018, highlighted that with forensics providers exiting the market there were risks for the security of exhibits and data, as well as a loss of forensic skills, and that “the level of resilience is very low”.¹⁶ Dr Tully highlighted work underway within policing and the Home Office to establish contingency plans for supplier exits from the forensics market, but warned against competitive procurement processes which drove prices down to the extent that supplier exits are more likely in the first place. She concluded that avoiding such outcomes would be “a more effective and efficient use of resources than the costly planning and execution of contingency plans following company failures”.¹⁷ Value for money was important but, she emphasised, “achieving the lowest cost does not always equate to the best value for money” and “greater focus on value than on cost is urgently required”.¹⁸

10. When Dr Gillian Tully gave evidence to us in February 2018, she reiterated those concerns about the sustainability of the forensics market:

Over the last couple of years, we have seen some of the risks that were raised at the time [of the Forensics Strategy] crystallise. We have seen two smaller companies and, now, one large company offering forensic services to the police in the UK go out of business.¹⁹

I think that something different has to happen if we are to ensure continuity of supply and, in particular, enough expertise remains in the field. A number of people have been made redundant once or twice. You cannot keep making people redundant time and again and expect that they will stay and retain their expertise in the [Criminal Justice System].²⁰

It seems that the way in which some of the contracts are procured tends to push towards lowest pricing; it is not the case in all the contracts, but it is in some of them.²¹

When you look at the picture across the board, I do not think that enough has been done to make sure that there is stability in the marketplace.²²

Dr Tully explained to us how despite the capacity of the market reducing, forensics providers were seeking to win a workload that was also falling in many disciplines, and the police’s procurement practices continued to engender fragmentation of tests, with providers asked to undertake narrowly defined test procedures without being asked to consider the results in the wider context of the relevant criminal case. Dr Tully, in her evidence to us in February, believed that the problem of fragmentation had worsened.²³

15 [Press reports](#)

16 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

17 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

18 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

19 Q1

20 Q2

21 Q4

22 Q5

23 Q10

11. The continued unsustainability of the market was a factor in Dr Tully’s call for a wider review of the Strategy (paragraph 30):

If it is a mixed economy between the private and the public sector, some sort of strategy needs to be in place to ensure that there is continuity of supply and that there is appropriate payment for what is difficult and complex work. [...] We need to take stock now. We have suddenly ended up in a situation that could have jeopardised thousands of cases, had emergency funding not been provided. It could still result in our losing a great deal of the skill that we have available. We have a very complex situation, in which the vast majority of analytical and interpretive skills sit in the commercial sector and the majority of fingerprint comparison skills sit in policing. [...] There needs to be a policy that says, “What services do we need? How are we going to ensure that they are sufficiently recompensed to be able to meet the required standards?” We need to make sure that the commissioning processes across whatever sectors the services sit in take account of the national status of sustainability, and not just the impact of one contract at a time.²⁴

12. Concerns about the sustainability of the forensics market—a problem identified many years ago—have continued, with the collapse of private sector providers in recent months. The overarching focus in the police’s forensics procurement appears to be on low price, and problems of fragmentation of forensics testing remain. The Radox case has highlighted how an unsustainable market has also affected standards in the forensics providers supporting the civil courts (paragraph 22). *The Government should review the sustainability of the forensics market as part of a wider review of its Forensics Strategy. That should include planning for dealing with providers exiting the market, but also an assessment of the underlying causes of market unsustainability. It should consider afresh whether the fragmentation of forensics testing is a result of the unsustainability of the forensics market or a contributing factor to it, and whether the procurement approaches examined by our predecessor Committee need to change.*

Standards and accreditation

13. Our predecessor Committee noted in 2011 that while all forensic service laboratories providing services for the police were required to be accredited to the ISO 17025 standard,²⁵ police in-house forensic services were not subject to the same requirement. The Committee had concerns about the potential transfer of the Forensic Science Service’s work to police laboratories,²⁶ and secured an assurance from the Government that when the Forensic Science Service was wound up in 2012 its work was transferred only to accredited private forensic providers.²⁷

14. In 2014, the Regulator made it a formal accreditation requirement to include adherence to the Regulator’s ‘Codes of Practice and Conduct for Forensic Science Providers and

24 Qq 49, 50

25 international standard ISO 17025—General requirements for the competence of testing and calibration laboratories—intended to ensure organisational competence, individual competence, validity of methods and impartiality within a forensics laboratory.

26 Science and Technology Committee, [The Forensic Science Service](#), Seventh Report, Session 2010–12, HC 855

27 HM Government, *The Forensic Science Service: Government response to Seventh Report*, Cm 8215 (October 2001), para 14

Practitioners in the Criminal Justice System’ (the ‘Codes’). In March 2016 the Regulator announced that the scientific standards set out in the Codes would form part of the assessment for all accredited organisations in the criminal justice system from October 2016 onwards,²⁸ and set out deadlines for accreditation for all forensic providers, including police in-house facilities—digital forensics (October 2017), fingerprint comparison (October 2018) and crime scene examination (October 2020). The aim, as the Government put it, was “to provide parity in the forensic market-place, which would involve police forces being required “to implement the same quality standards as those demanded from commercial providers”.²⁹ Our predecessor Committee concluded in 2016 that “the Government must be clear that, while some police forces may face particular challenges in securing accreditation, there must be no failure to meet the Regulator’s deadlines.”³⁰

15. When Dr Tully gave evidence to us earlier this year, she differentiated between three groups of forensics providers in the criminal justice system in terms of their progress in meeting the required standards—large commercial providers, police services and small providers. Large commercial providers, she told us, were “extremely compliant with the standards and have been for many years”.³¹ The police in-house service was “running very substantially behind where it needs to be”. Only 17 out of 46 police forensics providers had “any sort of accreditation by the time the [October 2017] deadline passed” for digital forensics³²—an “impressive” increase from only one police force 18 months before, but “with around 46 legal entities within law enforcement requiring accreditation, there is a long way to go”.³³ On fingerprint comparison, the Regulator told us that she now expected that only 13 police providers will meet the October 2018 deadline for accreditation.³⁴ Later accreditation deadlines appeared also in doubt: “If policing can do something radically different, there is a chance that we will be able to avert missing the 2020 [accreditation] deadlines around crime scene, collision investigation and fire investigation.”³⁵ The third group—‘one- and two-person providers’—were “the most non-compliant of all”.³⁶

16. The uneven progress on accreditation has impinged on the sustainability of the forensics market. The four large accredited providers, Dr Tully told us, “have a very fair complaint that [...] not enough due diligence was done to say whether [smaller] providers would be compliant in time for the deadlines, so they missed out on those contracts to cheaper providers that were not investing in the quality standards”.³⁷ The large commercial accredited providers have calculated that accreditation involves an overhead of about 15% to 20%, and Dr Tully acknowledged that for small providers the costs would be proportionately higher, but “it is very difficult to see how I could fairly set a different standard for those people, because they are still providing evidence to the criminal justice system”.³⁸ Dr Tully explained that under the criminal procedure rules, all organisations now have a duty to disclose any non-compliance with standards in any statements they

28 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

29 Science and Technology Committee, [Forensic Science Strategy: Government Response to the Committee’s Fourth Report](#), Second Special Report of Session 2016–17, HC 845

30 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, para 55

31 Q18; Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018), p10

32 Q18

33 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

34 Q18; Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018), p29

35 Q20

36 Q24

37 Q24 (See also Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018))

38 Q26; Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018), p26

make to the courts, and that she had asked all non-compliant organisations to tell the courts “what mitigation they have in place that will enable the court to decide whether their evidence is sufficiently reliable to be used as expert evidence”.³⁹

The Radox case

17. The Radox case has had significant adverse consequences for the integrity of the criminal cases that utilised the laboratory’s toxicology test results. Dr Tully told us in November 2017 that 10,000 criminal cases could be affected and that retesting of toxicology samples was likely to take 2–3 years to complete.⁴⁰ Some tests will not be able to be redone however because, for example, the products of cannabis in a blood sample degrade quickly and might now be below the legal limit rather than above it. Dr Tully concluded that “there will be criminal justice implications from that, but it is impossible to say whether there was originally a miscarriage of justice”.⁴¹ If cases are referred to the Criminal Cases Review Commission, the degradation of sample could “certainly cast doubt” on the results, although other factors would also be relevant depending on the specific case.⁴²

18. There are also consequences for the accreditation system and for the auditing of providers’ compliance with standards. The Regulator noted in January 2018 that:

Although [Radox] held accreditation to the appropriate quality standard, the malpractice was not discovered by the usual quality checks. This raised a number of questions including: (a) whether or not potential malpractice is more widespread than at [Radox], particularly given the movement of staff between forensic service providers; and (b) whether or not the quality standards need to be strengthened.⁴³

Dr Tully explained that Radox did not have the additional accreditation to the ‘Codes’ (paragraph 14), which include a requirement for the ‘separation of responsibilities’, which appears to have been a factor in the Radox case.⁴⁴

19. The Regulator’s recent Annual Report noted that during the year to October 2017, the United Kingdom Accreditation Service (UKAS) had carried out 23 Codes accreditation visits—on both police and private facilities—which identified over 700 ‘non-conformities’. Many of these addressed issues around ‘business continuity’ and ‘test methods and validation’.⁴⁵ Dr Tully acknowledged that the weaknesses identified in the UKAS inspection visits could allow improper conduct to go undetected,⁴⁶ and she told us that “as we have seen with organisations going out of business, having a proper business continuity plan is absolutely critical”.⁴⁷

20. As a result of the Radox case, the Regulator asked all major forensic science suppliers to the criminal justice system to review their practices, and these audits found “no data

39 Qq21, 23

40 [Letter from Dr Gillian Tully](#) on Radox Testing Services (November 2017)

41 Q14

42 Q17

43 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

44 Q36

45 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018); Q26

46 Qq32, 33

47 Q27

manipulation”.⁴⁸ UKAS was also reviewing the accreditation of toxicology providers and considering whether any changes to the assessment process might help find deliberately concealed manipulation of data.⁴⁹ UKAS planned “to have a bit more variety” in its inspections, Dr Tully told us, “so that people cannot predict how they are going to be audited. It will do more vertical audit, right down to raw data.”⁵⁰ She cautioned, however, that “the inevitable cost of adding additional safeguards should be balanced against risk”.⁵¹

21. In the meantime, the Regulator has sought to strengthen her investigation and whistle-blowing procedures. Dr Tully told us that she was developing an anonymous reporting facility through the Regulator’s website. But she also wanted to be added to the list of ‘prescribed persons’ under the whistleblowing legislation⁵² and to be exempt from data disclosure requirements under the EU General Data Protection Regulation that would make it difficult to undertake investigations of individuals. She had raised these issues with the Government.⁵³ We wrote to the Home Office, urging action,⁵⁴ and the Minister gave us assurances on these matters, including that the Regulator could be made a whistle-blowing ‘prescribed person’ once put on a statutory footing.⁵⁵

Civil courts

22. One of the lessons from the Radox case was that a failure to meet the forensics standards required in the criminal justice system were not as readily identified in the civil courts system. Dr Tully explained that the oversight system deployed for criminal forensics is missing in the civil courts system. Staff involved in the malpractice at the Radox laboratory had previously worked at another business, Trimega (which subsequently folded), and Trimega’s failings in a family court case had not been communicated to any oversight body.⁵⁶ Dr Tully explained that:

In the criminal justice system, for people who are compliant with the Codes of Practice and Conduct, there is a very clear requirement to escalate what has gone on. There are very clear escalation requirements, and organisations must report to me when things have gone wrong. In this [Trimega] case, [...] it was not escalated in that [family courts] jurisdiction. One can think of it then as infecting, almost, the criminal justice system. There was no central record anywhere of that judicial criticism.⁵⁷

23. Accreditation of forensics providers remains vitally important in maintaining the confidence of the courts and the public in the evidence used in the justice system. The Radox case has demonstrated the importance of all forensic providers becoming fully accredited (including to the Regulator’s ‘Codes’) in accordance with the deadlines set

48 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

49 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

50 Q38

51 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018)

52 Q38 (Although there is already provision for reporting concerns to the Regulator, there may be no statutory protection under the Employment Rights Act 1996, as amended by the Public Interest Disclosure Act 1998. The Regulator is not a ‘prescribed person’ under the provisions of s43F of the 1996 Act (see the Public Interest Disclosure [Prescribed Persons] Order 2014) and there is no guarantee that the provisions of s43G would apply).

53 Qq58–59; [Letter from the Forensic Science Regulator](#), 16 March 2018 (also [BSF001](#))

54 [Letter to Baroness Williams](#), 27 March 2018

55 [Letter from Baroness Williams](#), 17 April 2018 (also [BSF003](#))

56 Q34

57 Q34

by the Regulator. That case also highlighted how standards and accreditation cannot be fully effective unless there is rigorous auditing of compliance. The Radox case, and its links to the earlier Trimega case, also point to a more fundamental disconnect of the forensics standards and regulatory systems between the criminal justice system (which is covered by the Regulator’s remit) and the civil courts system (which is not).

24. *The Regulator should work with UKAS to strengthen the auditing of standards compliance, to include validation of test results as well as governance structures and processes; the effectiveness of which would be bolstered by the Regulator being given statutory enforcement powers, which we discuss below. The Ministry of Justice should work with the Home Office and the Forensics Regulator to examine the scope for the Regulator’s remit to be extended to the civil courts forensics system, or for a similar regulator to be established with a similar remit, to bring a comprehensive and enforceable standards system to that sector also.*

25. We welcome the Government’s commitment to make the Regulator a ‘prescribed person’ under the whistle-blowing legislation. *That should happen as soon as her position is put on a statutory footing.*

Statutory powers

26. The effectiveness of standards, and of the accreditation of those forensics facilities adhering to them, will depend in part on how well they can be enforced. Our predecessor Committee concluded in its 2011 report on the then Forensic Science Service that “it is time for the Forensic Science Regulator to have statutory powers to enforce compliance with the quality standards and Codes of Conduct that [the then Regulator] has developed”, and recommended that the Government “bring forward proposals to provide the [Regulator] with statutory powers immediately”.⁵⁸ The Committee’s 2013 follow-up report reiterated that recommendation; specifically that the Government “decide on a statutory role by March 2014”.⁵⁹ In its response, later in 2013, the Government announced a consultation “on proposals to put the role of the Regulator, and the scope of regulation, on a statutory footing, and to make adherence to the quality standards set by the Regulator mandatory for all providers.”⁶⁰ It was not until July 2015, however, that the Government published an analysis of the response to the consultation, without giving any Government opinion, stating simply that “the way forward will be published alongside the [Forensic Science] Strategy”. When the Forensics Strategy was published in March 2016, it contained a commitment to granting the Regulator statutory powers by the end of the 2015 Parliament. Dr Tully told the Committee in 2016 that “it will not be possible to ensure full compliance with the standards without statutory powers”.⁶¹

27. The Forensics Regulator repeated the point in her latest Annual Report in January 2018, stating that “without statutory powers to enforce compliance, the Regulator cannot guarantee that all science being used in the [criminal justice system] is being carried out to the required quality standards”.⁶² The Regulator wrote to us in January 2018, at

58 Science and Technology Committee, [The Forensic Science Service](#), Seventh Report, Session 2010–12, HC 855

59 Science and Technology Committee, [Forensic science](#), Second Report, Session 2013–14, HC 610

60 Home Office, [Government response to the Second Report from the Science and Technology Committee: Forensic science](#), Cm 8750 (November 2013)

61 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, para 60

62 Forensic Science Regulator, [Annual Report Nov 2016 – Nov 2017](#) (January 2018), p12

our request, with details of the specific statutory powers she wanted.⁶³ She subsequently told us that “we can reach 80% to 90% compliance with the standards without statutory powers, but I do not think that we will ever get full compliance”.⁶⁴ In March 2018, Chris Green MP presented his Forensic Science Regulator Bill—a private members’ bill—with the Government’s support.

28. The Forensics Regulator needs statutory powers to allow her to ensure that providers seek accreditation and that standards are delivered. Governments have stated a desire over several years to introduce statutory powers, with varying degrees of enthusiasm, and the Government has now lent support to a Private Members’ Bill. The Government, having supported the drafting of the current Forensic Science Regulator Bill, should now give it time in its legislative programme in order for it to make progress. It should then ensure rapid implementation following Royal Assent.

Forensics strategy and oversight

29. In our predecessor Committee’s report in 2016, it complained that the Forensics Strategy lacked a “coherent vision for forensic services” and concluded that a revised document was needed (paragraph 1).⁶⁵ In our current brief 2018 inquiry, Dr Tully agreed that the 2016 Strategy had not delivered,⁶⁶ and concluded that:

When the [Forensics] Strategy was published a couple of years ago, it talked about national approaches and so on. A programme has been set up within policing—Transforming Police Forensics—but it is only now at the ‘business case’ stage. There has been uncertainty for another couple of years, and I would say that there is still uncertainty among providers about what that will mean for them.⁶⁷

Home Office witnesses explained that such work, to take forward the developments in both biometrics and forensics, was still underway, two years after the Forensics Strategy was published:

Work on developing the capacity and capability in the police to deal with biometrics and forensics—particularly in forensics—is being taken forward through the Transforming Forensics Programme, which has done some initial work, and the more recent proposals that have been put together by the police are being looked at, at the moment. Exactly how they will then provide improved forensic services themselves and work with the market will depend on the outcomes of that programme. [...] The latest proposals from the police for the Transforming Forensics Programme have just been submitted and are being reviewed at the moment. Decisions should be taken shortly, which will then decide on which elements are to be taken forward.⁶⁸

63 [Letter from the Forensic Science Regulator](#), 10 January 2018

64 Q53

65 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, para 82

66 Q51

67 Q5

68 Qq97, 100 [Christophe Prince, Director for Data & Identity, Home Office]

30. Against a background of accreditation delays (paragraph 15), the Radox case (paragraph 17) and the failure of some forensics companies (paragraph 8), Dr Tully believed that there was now a need for a Strategy review:

I really feel that now is the time for there to be a review of forensic science policy that asks, “What do we want to guarantee for forensic science in this country for the criminal justice system? For whom do we want to guarantee access to the services? For what services do we want to ensure that we have continuity of supply, and how are we going to make that happen?”⁶⁹

The Regulator told us that “a large majority of the forensic science that is delivered in England and Wales is delivered to a good quality. [...] There are a lot of very good forensic scientists doing very good work out there, but a lot of them are frustrated that they do not work in an optimal system that enables them to do the best work that they could do.”⁷⁰

31. The concern expressed by our predecessor Committee in 2016 that the Forensics Strategy failed to fully address the linkages between biometrics and forensics policies also continues to be an issue. The Forensic Strategy document noted “an already ongoing review by police forces of the case for a ‘Joint Forensic & Biometric Service’ to achieve economies of scale, increased capability and resilience.” The Home Office told our predecessor Committee in 2016 that “Chiefs and [Police and Crime Commissioners] will want to consider the case for a [Joint Forensic and Biometric Service] in the round. One likely potential benefit will be an improved ability to innovate, to send signals to suppliers about priorities for innovation, and an enhanced ability both to trial new approaches and ensure these are rolled out widely over a service supporting a large area of law enforcement.”⁷¹ In our current inquiry, the Minister emphasised that although there were distinct applications of forensics (in criminal justice) and biometrics (for example in immigration), a Directorate for Data & Identity had been set up in the Home Office to help align common forensics and biometrics interests.⁷²

32. One of the lessons from the Radox case (paragraph 17) is that the Forensics Strategy may also have been sub-optimal in not addressing the forensics requirements of the civil courts.

33. The Forensics Strategy requires re-evaluation. The weaknesses identified by our predecessor Committee in 2016 remain, and have since been exacerbated by accreditation delays, the Radox case and some forensics companies failing. The work underway under the ‘Transforming Police Forensics’ programme, intended to help shape future forensics services, is still underway two years after the Forensics Strategy was published. *The Government should revise, re-issue and consult on a new Forensics Strategy; one that addresses the forensics requirements of both the civil and criminal justice systems.*

69 Q49

70 Q71

71 Science and Technology Committee, [Forensic Science Strategy](#), Fourth Report of Session 2016–17, HC 501, para 69

72 Q91

3 Biometrics

The Biometrics Strategy

34. When the Home Office published its Forensic Science Strategy in March 2016, it came without the complementary ‘Biometric Strategy’ that was originally planned. In 2013, the Government had committed to producing a ‘Biometric and Forensic Strategy’ by the end of that year.⁷³ Subsequently, in March 2015, the Home Office undertook to publish it by the end of that year;⁷⁴ later opting for two strategies—a ‘Forensic Strategy’ and a ‘Biometric Strategy’—to be produced by the end of 2015. It said:

The Government’s Biometric Strategy and associated policy framework will support an aligned approach on the use and retention of biometrics and how its implementation is governed. Whilst forensics and biometrics both involve the use of science and technology, they are different. The Government is developing two separate but aligned Forensic and Biometric strategies and remains committed to publishing both strategies by the end of 2015.⁷⁵

The Government told our predecessor Committee in November 2016 that a Biometrics Strategy was “in the final stages of completion and will be published shortly”.⁷⁶

35. Last year, with the Biometrics Strategy still to be delivered, we asked the Home Office about its plans for publication. Baroness Williams, the Home Office minister for countering extremism, told us in November that:

A great deal of work has been done on the [Biometrics] Strategy. It ranges across many areas of policy, some of which are developing rapidly. After reviewing it carefully, I have decided that it cannot be finalised until further work has been done in some of these areas, and so it will unfortunately not be possible to publish the Strategy until next year.⁷⁷

When the minister subsequently gave evidence to us in February 2018, she told us that she expected to publish a Biometrics Strategy in June 2018.⁷⁸ Baroness Williams told us that further work was being done on the draft Biometrics Strategy because its “scope was too wide” with different Government departments using biometrics for different purposes. She envisaged a “framework for governance and oversight”,⁷⁹ and wanted:

something that was flexible and fit for the future in this quite fast-changing area. [...] We need something in place quite urgently. It is also the reason we need to get the framework for the strategy absolutely right so that it is

73 Home Office, [Government response to the Second Report from the Science and Technology Committee: Forensic science](#), Cm 8750 (November 2013)

74 Science and Technology Committee, [Legacy: Parliament 2010–15](#), Ninth Report, Session 2014–15, HC 758

75 Science and Technology Committee, [Current and future uses of biometric data and technologies: Government Response to the Committee’s Sixth Report of Session 2014–15](#), Second Special Report, HC (2015–16) 455, p4

76 Science and Technology Committee, [Forensic Science Strategy: Government Response to the Committee’s Fourth Report](#), Second Special Report of Session 2016–17, HC 845

77 [Letter from Baroness Williams](#), 30 November 2017

78 Q85

79 Q94

not only fit for the future but that it gets those ethical and legal questions fixed within it of why we are doing what we are doing, and how we deploy our policy.”⁸⁰

36. The Government’s rationale for the more than four years’ delay in producing a Biometrics Strategy is less than convincing. We agree with the Minister that the Strategy needs to put in place a governance structure that is fit for the future and ‘fixes’ the ethical and legal questions involved, but it is those issues—notably around facial images—that make a Strategy urgently needed. *The Government must now produce the Strategy in June, without any further delay.*

Deletion of facial images from police databases

37. The High Court judgment in the 2012 ‘RMC’ case⁸¹ was critical of the governance arrangements for custody images then in place and, as the Biometrics Commissioner put it, concluded that “the retention regime was not proportionate in its treatment of unconvicted persons to the extent that it was unlawful”.⁸² Legislation is silent about the length of time for which custody images can be retained, but the Court held that the retention regime for custody images taken from un-convicted persons was incompatible with Article 8 of the European Convention on Human Rights. The Minister explained that the Court’s reasoning was based on the lack of distinction between those who were and were not convicted and the retention review periods set out in the police’s guidance.⁸³

38. The Home Office commissioned its Police Science & Technology Unit to conduct a Custody Images Review, which considered the issues raised in the RMC case and reported its findings in February 2017.⁸⁴ The Minister told us in November 2017 that the Review had concluded:

Unconvicted persons have the right to apply for deletion of their image, with a presumption in favour of deletion [...]. However, the police have the right to retain the image if there is an exceptional reason to do so, such as the person posing an ongoing risk to the public. The [Authorised Professional Practice guidance] has since been amended to reflect this.⁸⁵

In March 2017 Paul Wiles, the Biometrics Commissioner, warned that the proposed process for those not convicted of an offence to apply to the police to have their facial images deleted would be “complex, and will require a great deal of individual decision-making resulting in high compliance costs and, in spite of guidance, may lead to forces exercising their discretion differently, thereby resulting in a postcode lottery”.⁸⁶

80 Qq83–85 (see also Q144)

81 [RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department](#) [2012], EWHC 1681 (Admin). (The case involved two unconnected individuals—‘RMC’ and ‘FJ’—who had been arrested but subsequently not prosecuted, and who sought to have their custody images destroyed.)

82 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), para 300

83 [Letter from Baroness Williams](#), 30 November 2017

84 Home Office, [Review of the use and retention of custody images](#) (February 2017)

85 [Letter from Baroness Williams of Trafford](#), 30 November 2017

86 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), para 300

39. Our Home Office witnesses told us in February that systems were not integrated in a way that would allow automatic image deletion:

The removal [of facial images] will be undertaken only when there is a request; there is no mechanism at the moment automatically to connect the non-conviction to the custody image and therefore to prompt the police to make that removal. It relies at the moment on a request being made. [...] There is no mechanism for prompting a decision to be taken on retention at that point, but there are review periods in place to ensure that, after a certain period of time, depending on the offence, the custody image's retention will be reviewed.⁸⁷

The Custody Images Review noted that images were held on a range of local custody systems which were not linked to Crown Prosecution Service or court systems, and were “not generally designed to automatically weed, review or destroy images, or to differentiate between convicted and unconvicted individuals”.⁸⁸ The Home Office explained to us that if images are deleted on local custody systems they will also be automatically deleted from the Police National Database, but not the other way round.⁸⁹

40. The Home Office acknowledged that the approach of allowing deletions on request for facial images, rather than automatically, differs from the “significantly more advanced” system used for DNA and fingerprints data. The Home Office told us that DNA and fingerprint databases are held “in only one place and are linked to information on the Police National Computer about case outcomes and conviction status” and that unique identifying numbers for each case “makes it possible to filter records relating to unconvicted persons automatically”.⁹⁰

41. The Home Office's Custody Images Review made it clear that its recommendations, adopted by the Government, sought to reflect the limitations of the current police IT systems and the potential costs of a manual internally-driven system of making deletions:

This approach balances the need to use information, data and intelligence to protect the public, against the Article 8 rights of individuals. It also takes account of the high estimated cost to the taxpayer of a full manual deletion exercise in respect of all custody images currently held. It is expected that the implementation of any new technological solutions, both local and national, will link and integrate intelligence, crime and prosecution data providing a better ability to search, access and assess custody images leading to improved risk-based retention and deletion.⁹¹

Any potential manual weeding exercise, the Minister told us, “will have significant costs and be difficult to justify given the off-setting reductions that [police] forces would be required to find in order to fund it”.⁹²

87 Qq132, 135 [Christophe Prince, Director for Data & Identity, Home Office]

88 Home Office, [Review of the use and retention of custody images](#) (February 2017), para 1.4

89 [Letter from Baroness Williams](#), 28 March 2018 (also [BSF002](#))

90 [Letter from Baroness Williams](#), 28 March 2018 (also [BSF002](#)); Qq150–151 [Christophe Prince, Director for Data & Identity, Home Office]

91 Home Office, [Review of the use and retention of custody images](#) (February 2017), paras 1.13–1.14

92 [Letter from Baroness Williams](#), 28 March 2018 (also [BSF002](#))

42. As part of the Home Office Biometrics Programme (HOB), a National Law Enforcement Data Programme is intended to replace legacy IT systems for storage and comparison of fingerprints, DNA and facial images currently stored on the Police National Computer and the Police National Database—existing systems which are “inflexible and expensive to change”.⁹³ The IT replacement programme would allow police officers to be able to access driving licenses images, and consideration was being given to whether passport images could also be accessed.⁹⁴ The Home Office expected the “new platform being delivered by the National Law Enforcement Data Programme to [...] enable a considerably more flexible approach to automatic deletion than is possible at present”.⁹⁵

43. There is limited data on the number of requests for facial image deletion since the Review. The Press Association established, from data received from 37 police forces, that up to October 2017 there had been 67 requests for custody image deletions and, of the 48 where decisions had been reached, 14 had been refused.⁹⁶ In the meantime, the Home Office could not provide us with statistics from police forces on the number of applications and approvals for deletions, but told us it was currently compiling them.⁹⁷ Big Brother Watch have questioned the lawfulness of the Government’s approach of not automatically deleting images,⁹⁸ as well as of the use of facial recognition technology.

44. The result of the 2012 ‘RMC’ case was a ruling that it is unlawful to hold custody images without making a distinction between those who are convicted and those who are not. The Home Office’s response has been to introduce a system for unconvicted individuals to be able to request the deletion of their images, but not an automatic deletion system. The Government’s solution reflects current weaknesses in IT systems and a concern about the potential cost of a manual deletion process that does not depend on external requests. New IT is planned, which might help automate the system in future. The Government’s approach is unacceptable because unconvicted individuals may not know that they can apply for their images to be deleted, and because those whose image has been taken should not have less protection than those whose DNA or fingerprints have been taken.

45. The Government must ensure that its planned IT upgrade under the Home Office Biometrics Programme is delivered without delay, and is used to introduce a fully automatic image deletion system for those who are not convicted. If there is any delay in introducing such a system, the Government should move to introduce a manually-processed comprehensive deletion system as a matter of urgency. The forthcoming Biometrics Strategy must address which of these possible routes will be followed. The Strategy should also set out the Home Office’s assessment of the lawfulness of its deletion-on-application response to the ‘RMC’ case, and the legal advice underpinning that assessment.

93 Minutes of the Biometrics & Forensics Ethics Group’s [meeting](#), in September 2017, para 7.1

94 Minutes of the Biometrics & Forensics Ethics Group’s [meeting](#), in September 2017. See also Q162

95 [Letter from Baroness Williams](#), 28 March 2018 (also [BSF002](#))

96 Mail online, ‘[Custody image deletion request figures revealed](#)’, 12 February 2018

97 [Letter from Baroness Williams](#), 28 March 2018 (also [BSF002](#))

98 Big Brother Watch, ‘[Misleading, incompetent and authoritarian: the Home Office’s defence of facial recognition](#)’, 19 April 2018

Facial recognition and ‘watch lists’

46. Some police forces are using images in facial recognition applications. Custody and other images stored on the Police National Database and other police force systems have been used to identify individuals in public places.⁹⁹ We discussed with the Minister how images had been used for policing the Notting Hill Carnival, Remembrance Day in Whitehall and a Six Nations rugby match in Cardiff.¹⁰⁰ The Home Office told us that the use of the technology at such events involved comparing faces in the crowds against a ‘watch list’ of people wanted by the police or previously expected to commit offences. They told us that, except where there were matches, both the watch list created for the events and the images collected at the events were subsequently deleted.¹⁰¹

47. There has been some controversy about these cases, nevertheless, including about the effectiveness of the technology and concerns that its reliability in making matches might vary when applied to people from different racial groups. As we noted in our recent report on Algorithms,¹⁰² research at MIT in the US found that widely used facial-recognition algorithms were biased because they had been ‘trained’ predominantly on images of white faces. The systems examined correctly identified the gender of white men 99% of the time, but the error rate rose for people with darker skin, reaching 35% for black women.¹⁰³ In the UK, Big Brother Watch recently reported their survey of police forces, which showed that the Metropolitan Police had a less than 2% accuracy in its automated facial recognition ‘matches’ and that only two people were correctly identified and 102 were incorrectly ‘matched’. The force had made no arrests using the technology.¹⁰⁴ The Minister told us in November 2017 that:

Our view is that facial searching plays an important role in the detection and prevention of crime. There is a clear need to strike a balance between protecting an individual’s privacy and giving the police the tools they need to keep us safe. A decision to deploy facial recognition systems is an operational one for the police. Further, the retention and use of such images by police is governed by the Code of Practice on the Management of Police Information (MoPI), and accompanying guidance set out in the College of Policing’s Authorised Professional Practice (APP).¹⁰⁵

48. The Minister agreed that “there is a line between maintaining privacy and maintaining public protection”.¹⁰⁶ The Government, she told us, “need to be absolutely clear about why they are collecting [images] and for what purpose”.¹⁰⁷ The technology, the Minister told us, was still developing and “the reason it is being piloted, rather than being used widely, is that the technology is developing”.¹⁰⁸ The Home Office Biometrics programme was still

99 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#) (March 2017)

100 Qq139–143, 157

101 [Letter from Baroness Williams](#), 28 March 2018 (also [BSF002](#))

102 Science and Technology Committee, *The use of algorithms in decision-making*, Fourth Report of Session 2017–19, HC 351

103 Joy Buolamwini, [Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification](#), *Proceedings of Machine Learning Research* 81:1–15 (2018)

104 Big Brother Watch, [Faceoff: The lawless growth of facial recognition in UK policing](#) (May 2018)

105 [Letter from Baroness Williams](#), 30 November 2017.

106 Q106

107 Q145

108 Qq142, 160, 161

evaluating the technology.¹⁰⁹ Subsequently, in May, the Information Commissioner has indicated her readiness to initiate legal action on the use of facial recognition, on data protection grounds:

There may be significant public safety benefits from using [facial recognition technology]—to enable the Police to apprehend offenders and prevent crimes from occurring. But how facial recognition technology is used in public spaces can be particularly intrusive. It’s a real step change in the way law-abiding people are monitored as they go about their daily lives [...] For the use of [facial recognition technology] to be legal, the police forces must have clear evidence to demonstrate that the use of [facial recognition technology] in public spaces is effective in resolving the problem that it aims to address, and that no less intrusive technology or methods are available to address that problem. Strengthened data protection rules coming into law next week require organisations to assess the risks of using new and intrusive technologies [...] I have identified [use of facial recognition technology] by law enforcement as a priority area for my office and I recently wrote to the Home Office and the NPCC setting out my concerns. Should my concerns not be addressed I will consider what legal action is needed to ensure the right protections are in place for the public.¹¹⁰

49. Facial image recognition provides a powerful evolving technology which could significantly help policing. There are serious concerns, however, over its current use, including its reliability and its potential for discriminatory bias. We welcome the Government’s assurances that the technology is only being used at the moment for targeting those on ‘watch lists’ rather than as a blanket approach, and that images collected from public events and the relevant watch lists are being deleted afterwards.

50. *Facial recognition technology should not be generally deployed, beyond the current pilots, until the current concerns over the technology’s effectiveness and potential bias have been fully resolved. The new facial images ‘oversight Board’ that the Minister is planning to set up (paragraph 54) will need to ensure that that condition is satisfied. But in such an important area, with public confidence critical, it must be ministers and Parliament that take the final decision on any wider deployment of the technology. The forthcoming Biometrics Strategy should include an undertaking that such a decision will not be left to be “an operational decision for the police”, and provide a Government commitment to give the House an opportunity to debate and vote on the issue.*

Oversight structures

51. There have been significant changes in the governance structures for biometrics in recent years. In 2016, oversight of fingerprints was added to the remit of the Strategy Board responsible for DNA, to become the ‘National DNA Database & Fingerprint Database Strategy Board’. It includes representatives from the police, the Home Office, the Forensics Regulator, the Biometrics Commissioner and the Information Commissioner.¹¹¹ Paul Wiles, the Biometrics Commissioner, observed that DNA has a national database and a central management and governance framework, whereas the police use of fingerprints

109 Q162

110 Elizabeth Denham, ICO blog, [Facial recognition technology and law enforcement](#) (14 May 2018)

111 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#) (March 2017), paras 11, 13

was still a much more dispersed system. He saw the extension of the Strategy Board's remit as "a welcome development since it brings fingerprints within a proper, transparent and, moreover, mature national governance structure". One of the challenges for the Strategy Board, the Commissioner believed, was "to bring the collection, use and governance of fingerprints to the same standard as that of DNA".¹¹²

52. However, the remit if the Strategy Board does not cover facial images. Paul Wiles expressed his concern in March 2017 that "so far there has been little or no public discussion in respect of the retention and use of facial images or whether or how such a regime should be governed. The development has taken place outside the oversight of the [Strategy Board]".¹¹³ He also highlighted the need to address the oversight and ethics of facial images:

The development of digital images, their storage on a national database, the use of powerful searching algorithms and the deployment of such technologies in public spaces transforms facial images into something new. Whilst even the best matching algorithms cannot reach the accuracy levels achieved by DNA, and like fingerprints require human interpretation, they are improving and are already being deployed. [...] Facial images are a powerful new biometric but the acceptance by the public of their use for crime control purposes may depend on the extent to which the governance arrangements provide assurance that their use will be in the public interest and intrusion into individual privacy is controlled and proportionate.¹¹⁴

53. The Biometrics & Forensics Ethics Group recommended in September 2017 that the public's views should be sought in relation to whether they consented to the images from their driving licenses and passports being available to police officers on the street.¹¹⁵ The Biometrics Commissioner was concerned that "unlike DNA or fingerprints, facial images can easily be taken and stored without the subject's knowledge and facial images of about 90% of the adult population already exist in passports or driving licences".¹¹⁶ He noted that in 2016 there were 19m facial images on the Police National Database, 16.6m of which were searchable using facial recognition software.¹¹⁷ This compared with 5.2m people on UK DNA databases, or 8% of the population.¹¹⁸ The national fingerprint database holds 8m unique arrestee 'ten-print' records and 2.4m unmatched finger-marks and palm-prints.¹¹⁹

54. We discussed with the Minister the possibility of the police having images available for nine-tenths of the adult population in real-time, and the potential privacy issues involved. While the current poor reliability of facial recognition technology is a concern in itself, an eventually effective system could pose different issues for privacy if linked to

112 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), paras 13, 14

113 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), para 303

114 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#) (March 2017)

115 Minutes of the Biometrics & Forensics Ethics Group [meeting](#), September 2017, para 7.7

116 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), para 305

117 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#) (March 2017), para 301. (In February 2018 the Minister estimated 21m images in total (some of which were not facial images), including 12.5m which are searchable (Qq106–110).)

118 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), para 15

119 Commissioner for the Retention and Use of Biometric Material, [Annual Report 2016](#), para 30

passport and driving licence image databases. Baroness Williams emphasised “the tenet that the police need to use the biometrics, that they have, for policing purposes”,¹²⁰ and she told us that:

I agree that independent ethical oversight of police use of biometrics is desirable, and for this reason we have extended the remit of the Biometrics & Forensics Ethics Group from DNA and fingerprints to all biometrics.¹²¹

The Minister acknowledged that governance and oversight arrangements have grown over several years and were “quite complicated”. The Home Office were considering the formation of an ‘oversight board’ for facial recognition that would bring three regulators and oversight bodies together (the Biometrics Commissioner, the Surveillance Camera Commissioner and the Information Commissioner) with the police.¹²²

55. There are important ethical issues involved in the collection, use and retention of facial images that have greater salience than for DNA, fingerprints and other biometrics, not least because facial images can easily be taken and stored without the subject’s knowledge and because (unlike DNA and fingerprints) facial images databases—passports, driving licences and custody images—already include 90% of the adult population. Recent developments in the oversight of biometrics, to include facial images, will help such issues to be addressed. We welcome the Minister’s decision to set up a facial images ‘oversight Board’. *The forthcoming Biometrics Strategy should consider the scope for further refinement in the oversight architecture, including how image databases should be managed and regulated, potentially by a dedicated ‘Regulator’ or by the Biometrics Commissioner with an extended remit.*

120 Qq166–169

121 [Letter from Baroness Williams, 30 November 2017](#). (A ‘Biometrics & Forensics Ethics Group’, an advisory non-departmental public body, provides independent advice to ministers and the Strategy Board on ethical issues concerning the operation of DNA and fingerprint databases.)

122 Qq101, 158; [Letter from Baroness Williams, 28 March 2018](#) (also [BSF002](#))

Conclusions and recommendations

1. The main result of our inquiry is that there is a need not just for the long-delayed Biometrics Strategy, but also a reassessment and revision of the 2016 Forensics Strategy. Our brief inquiry has identified an urgent and significant need for action on the governance and oversight of both forensics and biometrics. This is vitally important because these disciplines, and the way their techniques and data are used, are at the heart of our courts system and underpin essential confidence in the administration of justice. (Paragraph 5)

Forensics

2. Concerns about the sustainability of the forensics market—a problem identified many years ago—have continued, with the collapse of private sector providers in recent months. The overarching focus in the police’s forensics procurement appears to be on low price, and problems of fragmentation of forensics testing remain. The Radox case has highlighted how an unsustainable market has also affected standards in the forensics providers supporting the civil courts. *The Government should review the sustainability of the forensics market as part of a wider review of its Forensics Strategy. That should include planning for dealing with providers exiting the market, but also an assessment of the underlying causes of market unsustainability. It should consider afresh whether the fragmentation of forensics testing is a result of the unsustainability of the forensics market or a contributing factor to it, and whether the procurement approaches examined by our predecessor Committee need to change.* (Paragraph 12)
3. Accreditation of forensics providers remains vitally important in maintaining the confidence of the courts and the public in the evidence used in the justice system. The Radox case has demonstrated the importance of all forensic providers becoming fully accredited (including to the Regulator’s ‘Codes’) in accordance with the deadlines set by the Regulator. That case also highlighted how standards and accreditation cannot be fully effective unless there is rigorous auditing of compliance. The Radox case, and its links to the earlier Trimega case, also point to a more fundamental disconnect of the forensics standards and regulatory systems between the criminal justice system (which is covered by the Regulator’s remit) and the civil courts system (which is not). (Paragraph 23)
4. *The Regulator should work with UKAS to strengthen the auditing of standards compliance, to include validation of test results as well as governance structures and processes; the effectiveness of which would be bolstered by the Regulator being given statutory enforcement powers, which we discuss below. The Ministry of Justice should work with the Home Office and the Forensics Regulator to examine the scope for the Regulator’s remit to be extended to the civil courts forensics system, or for a similar regulator to be established with a similar remit, to bring a comprehensive and enforceable standards system to that sector also.* (Paragraph 24)
5. We welcome the Government’s commitment to make the Regulator a ‘prescribed person’ under the whistle-blowing legislation. *That should happen as soon as her position is put on a statutory footing.* (Paragraph 25)

6. The Forensics Regulator needs statutory powers to allow her to ensure that providers seek accreditation and that standards are delivered. Governments have stated a desire over several years to introduce statutory powers, with varying degrees of enthusiasm, and the Government has now lent support to a Private Members' Bill. *The Government, having supported the drafting of the current Forensic Science Regulator Bill, should now give it time in its legislative programme in order for it to make progress. It should then ensure rapid implementation following Royal Assent.* (Paragraph 28)
7. The Forensics Strategy requires re-evaluation. The weaknesses identified by our predecessor Committee in 2016 remain, and have since been exacerbated by accreditation delays, the Radox case and some forensics companies failing. The work underway under the 'Transforming Police Forensics' programme, intended to help shape future forensics services, is still underway two years after the Forensics Strategy was published. *The Government should revise, re-issue and consult on a new Forensics Strategy; one that addresses the forensics requirements of both the civil and criminal justice systems.* (Paragraph 33)

Biometrics

8. The Government's rationale for the more than four years' delay in producing a Biometrics Strategy is less than convincing. We agree with the Minister that the Strategy needs to put in place a governance structure that is fit for the future and 'fixes' the ethical and legal questions involved, but it is those issues—notably around facial images—that make a Strategy urgently needed. *The Government must now produce the Strategy in June, without any further delay.* (Paragraph 36)
9. The result of the 2012 'RMC' case was a ruling that it is unlawful to hold custody images without making a distinction between those who are convicted and those who are not. The Home Office's response has been to introduce a system for unconvicted individuals to be able to request the deletion of their images, but not an automatic deletion system. The Government's solution reflects current weaknesses in IT systems and a concern about the potential cost of a manual deletion process that does not depend on external requests. New IT is planned, which might help automate the system in future. The Government's approach is unacceptable because unconvicted individuals may not know that they can apply for their images to be deleted, and because those whose image has been taken should not have less protection than those whose DNA or fingerprints have been taken. (Paragraph 44)
10. *The Government must ensure that its planned IT upgrade under the Home Office Biometrics Programme is delivered without delay, and is used to introduce a fully automatic image deletion system for those who are not convicted. If there is any delay in introducing such a system, the Government should move to introduce a manually-processed comprehensive deletion system as a matter of urgency. The forthcoming Biometrics Strategy must address which of these possible routes will be followed. The Strategy should also set out the Home Office's assessment of the lawfulness of its deletion-on-application response to the 'RMC' case, and the legal advice underpinning that assessment.* (Paragraph 45)

11. Facial image recognition provides a powerful evolving technology which could significantly help policing. There are serious concerns, however, over its current use, including its reliability and its potential for discriminatory bias. We welcome the Government's assurances that the technology is only being used at the moment for targeting those on 'watch lists' rather than as a blanket approach, and that images collected from public events and the relevant watch lists are being deleted afterwards. (Paragraph 49)
12. *Facial recognition technology should not be generally deployed, beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved. The new facial images 'oversight Board' that the Minister is planning to set up will need to ensure that that condition is satisfied. But in such an important area, with public confidence critical, it must be ministers and Parliament that take the final decision on any wider deployment of the technology. The forthcoming Biometrics Strategy should include an undertaking that such a decision will not be left to be "an operational decision for the police", and provide a Government commitment to give the House an opportunity to debate and vote on the issue.* (Paragraph 50)
13. There are important ethical issues involved in the collection, use and retention of facial images that have greater salience than for DNA, fingerprints and other biometrics, not least because facial images can easily be taken and stored without the subject's knowledge and because (unlike DNA and fingerprints) facial images databases—passports, driving licences and custody images—already include 90% of the adult population. Recent developments in the oversight of biometrics, to include facial images, will help such issues to be addressed. We welcome the Minister's decision to set up a facial images 'oversight Board'. *The forthcoming Biometrics Strategy should consider the scope for further refinement in the oversight architecture, including how image databases should be managed and regulated, potentially by a dedicated 'Regulator' or by the Biometrics Commissioner with an extended remit.* (Paragraph 55)

Formal minutes

Wednesday 23 May 2018

Members present:

Norman Lamb, in the Chair

Vicky Ford	Carol Monaghan
Bill Grant	Damien Moore
Darren Jones	Neil O'Brien
Stephen Metcalfe	

Draft Report (*Biometrics strategy and forensic services*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 55 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Fifth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 5 June at 9.00 am

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the [inquiry publications page](#) of the Committee's website.

Tuesday 6 February 2018

Question number

Dr Gillian Tully, Forensic Science Regulator.

[Q1–81](#)

Baroness Williams of Trafford, Minister for Countering Extremism, Home Office; and **Christophe Prince**, Director for Data and Identity, Home Office.

[Q82–184](#)

Published written evidence

The following written evidence was received and can be viewed on the [inquiry publications page](#) of the Committee's website.

BSF numbers are generated by the evidence processing system and so may not be complete.

- 1 Forensic Science Regulator ([BSF0001](#))
- 2 Home Office ([BSF0002](#))
- 3 Home Office ([BSF0003](#))

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the [publications page](#) of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2017–19

First Report	Pre-appointment hearing: chair of UK Research & Innovation and executive chair of the Medical Research Council	HC 747
Second Report	Brexit, science and innovation	HC 705
Third Report	Genomics and and genome editing in the NHS	HC 349
Fourth Report	Algorithms in decision-making	HC 351
First Special Report	Science communication and engagement: Government Response to the Committee's Eleventh Report of Session 2016–17	HC 319
Second Special Report	Managing intellectual property and technology transfer: Government Response to the Committee's Tenth Report of Session 2016–17	HC 318
Third Special Report	Industrial Strategy: science and STEM skills: Government Response to the Committee's Thirteenth Report of Session 2016–17	HC 335
Fourth Special Report	Science in emergencies: chemical, biological, radiological or nuclear incidents: Government Response to the Committee's Twelfth Report of Session 2016–17	HC 561
Fifth Special Report	Brexit, science and innovation: Government Response to the Committee's Second Report	HC 1008