House of Commons

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 of Session 2015–16

Ordered by the House of Commons to be printed 8 September 2015

HC 455
Published on 16 September 2015
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

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

Nicola Blackwood MP (*Conservative, Oxford West and Abingdon*) *(Chair)*
Victoria Borwick MP (*Conservative, Kensington*)
Jim Dowd MP (*Labour, Lewisham West and Penge*)
Chris Green MP (*Conservative, Bolton West*)
Liz McInnes MP (*Labour, Heywood and Middleton*)
Dr Tania Mathias MP (*Conservative, Twickenham*)
Carol Monaghan MP (*Scottish National Party, Glasgow North West*)
Graham Stringer MP (*Labour, Blackley and Broughton*)
Derek Thomas MP (*Conservative, St Ives*)
Matt Warman MP (*Conservative, Boston and Skegness*)
Daniel Zeichner MP (*Labour, Cambridge*)

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

Publications

All publications of the Committee (including press notices) and further details can be found on the Committee's web pages at www.parliament.uk/science

Committee staff

The current staff of the Committee are: Simon Fiander (Clerk); Dr Grahame Danby (Science Clerk); Dr Elizabeth Rough (Committee Specialist); Darren Hackett (Senior Committee Assistant); Julie Storey (Committee Assistant); and Nick Davies (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.

Second Special Report

On 7 March 2015 the Science and Technology Committee published its Sixth Report of Session 2014–15, *Current and future uses of biometric data and technologies* [HC 734]. On 20 August 2015 we received from the Government a letter and Response to the Report. These are appended below.

Appendix 1: Letter from Rt Hon Mike Penning MP, Minister for Policing, Crime, Criminal Justice & Victims

I am responding on behalf of the Government to the Committee's report on the current and future uses of Biometrics issued during the last Parliament. I would like to thank the Committee for its consideration of this issue and I look forward to working with you in the future.

I recognise the need to develop a strategic approach to the use and retention of biometrics. This approach should recognise that biometrics is fast-changing and provides opportunities for better secure identity verification, better public services, improved public protection and the ability to identify and stop criminals. This should be balanced against safeguarding the rights of the individual from unnecessary intrusion. The Government's Biometric Strategy will support an aligned approach on the use and retention of biometrics and how its implementation is governed.

The Committee flagged 12 conclusions and recommendations. I have set out in an attachment to this letter the Government's response to each recommendation.

Appendix 2: Government response

Biometrics is the science of measuring and analysing biological and behavioural characteristics, used to recognise individuals repeatedly to a high degree of confidence. It is therefore reported to be the best way of verifying identities, once they are established by associating people's biometric and biographical details together. Biometrics are used extensively across Government for the purposes of crime prevention and investigation, protection of the UK's borders and the delivery of public services.

The application of biometrics in public protection provides a high degree of confidence and the increasing use of biometrics by the private sector demonstrates that biometrics could provide a more convenient way of proving identity before accessing services.

Therefore the Government believes it is important to assess properly the opportunities provided by biometrics for both public protection and citizen convenience, and to weigh these up against public concerns about the use of biometrics as an intrusion of their privacy so that biometrics can be safely used with proper safeguards.

We would like to take this opportunity to thank the Science and Technology Committee for their comprehensive report on the current and future uses of biometric data and technologies. We have provided a response to each of the recommendations made by the Committee below.

Scientific Advice on Biometrics

Recommendation 1:

The Foresight Programme's 2013 report on *Future Identities* was a missed opportunity to examine biometrics and identify the main trends, and the associated challenges, that policy-makers in this field will face in the future. Indeed, it is astounding that biometrics was deemed 'beyond the scope' of an apparently forward-looking piece of analysis when, three years earlier, the Government had been seeking to rely on biometrics as part of its identity card programme. We agree with the Biometrics Commissioner that this type of forward-looking analysis is desirable.

We recommend that Foresight builds on the evidence gathered during this inquiry and undertakes a short, "Policy Futures" study to examine systematically the emerging issues, risks and opportunities arising from developments in biometrics. This analysis should be frequently reviewed in order to keep pace with rapid advances in biometrics and should be applied by the Government to assist its preparations for, and to help it shape, how this field may unfold in the future.

The Government Office for Science and its Foresight Programme work with partners across Whitehall to ensure that evidence and strategic thinking inform the policy making process. As part of this work, the Government Chief Scientific Advisor publishes an annual report; this year's annual report will be on Forensic Science. The report will explore a range of related issues, one of which will be the opportunities and implications of innovations in biometrics.

The Government biometric strategy is still in the early stages of development and it is not possible to make firm commitments as to the scope and content at this stage. However we believe that it is likely to consider advances in biometrics and set out a roadmap for how the Government intends to utilise the emerging thinking in this field, both for public protection and citizen convenience.

Recommendation 2:

Despite a previous assurance from the Government, given over 12 months ago, that the publication of the forensics and biometric policy group's minutes was on the horizon, this has not occurred. As a result, the remit and status of the group, as well as what has

been on its agenda, remain a mystery. This continuing lack of transparency in the delivery of scientific advice to Government on biometrics is unacceptable and goes against the Government's own guidance, as set out in the 2010 *Principles of scientific advice to Government.*

To improve its transparency, we recommend that the remit, membership and outputs of the forensics and biometric policy group should be placed in the public domain immediately. A commitment should also be made to the publication of the minutes of all future meetings, unless there are overriding reasons of national security for not doing so.

In response to the Second Report of the Science and Technology Committee Session 2013-14 the previous Government said "*The Forensic Policy Group within the Home Office is leading on the development of this strategy and delivery of this strategy will inevitably result in the Forensic Policy Group changing into a wider, more representative group. Once this change has taken place the strategy and minutes of the new group will be published.*"

As the Committee has noted, that Strategy has not yet been published. In January 2015, the Government made a commitment to gather evidence in order to fully understand the desired outcomes of any strategies and to consider the future requirements. We are currently gathering evidence from police forces and forensic suppliers, consulting a wide range of stakeholders and developing options for inclusion within the strategy. Therefore whilst we are in the development phase, we will not be publishing the outputs of the meetings. We have separated the work into two strategies as discussed below in response to recommendation 3. We remain committed to publishing both the Forensic and Biometric Strategies by the end of 2015 and at that time we will consider future arrangements for overseeing delivery.

A Strategy for Biometrics

Recommendation 3:

The Government undertook to publish a joint forensics and biometrics strategy by the end of 2013. Over a year later, there is no strategy, no consensus on what it should include, and no expectation that it will be published in this Parliament. In its absence, there remains a worrying lack of clarity regarding if, and how, the Government intends to employ biometrics for the purposes of verification and identification and whether it has considered any associated ethical and legal implications.

The Government should be developing a strategy that exploits emerging biometrics while also addressing public concerns about the security of personal data and the potential for its use and misuse, with particular reference to biometric data held by the state.

We expect a comprehensive, cross-departmental forensics and biometrics strategy to be published by the Government no later than December 2015.

The Government recognises the need to develop a strategic approach to the use and retention of biometrics. This approach should recognise that biometrics is fast-changing and provides opportunities for better secure identity verification, better public services, improved public protection and the ability to identify and stop criminals. This should be balanced against safeguarding the rights of the individual from unnecessary intrusion. 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.

Testing Biometric Systems

Recommendation 4:

When biometric systems are employed by the state in ways that impact upon citizens' civil liberties, it is imperative that they are accurate and dependable. Rigorous testing and evaluation must therefore be undertaken prior to, and after, deployment, and details of performance levels published. It is highly regrettable that testing of the 'facial matching technology' employed by the police does not appear to have occurred prior to the searchable national database of custody photographs going live. While we recognise that testing biometric systems is both technically challenging and expensive, this does not mean it can be neglected.

When testing does occur, the continued use of a variety of testing protocols by suppliers makes it difficult to analyse and compare, with any degree of confidence, the performance of different systems. Following the abolition of the Biometrics Assurance Group, it is unclear who is responsible for interpreting the outcomes of biometric testing for the Government.

The Government should explain, in its response to this report, why the facial matching technology employed by the police was not rigorously tested prior to being put into operational use. We further recommend that the Government details what steps it is taking to encourage suppliers of biometric systems to comply with established UK testing standards.

Since the introduction of the first National Automated Fingerprint Identification System (NAFIS) biometric specialists in the Home Office and previous NDPB's (PITO and NPIA) have worked with suppliers and end-users to assure the accuracy of national biometric systems, both as part of the tender process and throughout the life of the contracts.

As understanding of biometric technologies has matured, a worldwide consensus has developed on ways of testing systems, resulting in the development of ISO standards. Biometrics experts at the Home Office Centre for Applied Science & Technology (CAST) are working with BSI and ISO to develop international standards for biometric testing which already include ISO 19795—Biometric Performance Testing and Reporting and ISO

TR 29189—Evaluating Examiner Assisted Biometric Systems (of which IDENT1 is an example).

To support the development and delivery of the Home Office Biometrics Programme, CAST are working with the Home Office Test and Design Consultancy Services to document the Home Office biometric accuracy testing approach to ensure consistency and transparency across the Home Office. It is expected that this document will be complete by the end of the year.

Performance levels of biometric systems cannot be characterised by a single figure. Publicising detailed results of performance is an area requiring careful consideration, as not only is the accuracy testing of large scale biometric systems very complex, so is interpreting the data. System performance is very dependent on the specifics of the application, making direct comparisons between systems difficult and in many cases meaningless. In addition, disclosing details of a system's limitations may create opportunities for those who wish to subvert it.

The Biometric Assurance Group (BAG) was primarily established to assure the ID Cards programme and was ended once the programme no longer required its services (the final BAG meeting was held on 11 June 2009). Responsibility for the design and execution of biometric tests resides with the Senior Responsible Officer of the agency procuring the system, working in conjunction with its suppliers. The extent of testing required is related to the risks associated with the operation of the system. Biometrics specialists within the HO and CAST can advise on the technical design of tests and interpretation of results. Organisations such as the National Physical Laboratory (NPL) offer a testing and evaluation service which industry takes advantage of. CAST also uses NPL services for peer review of its own evaluations.

The core facial recognition algorithm used by the Police National Database had already been tested by the US National Institute of Standards and Technology (an agency of the US Dept of Commerce) and was shown to be one of the best in terms of accuracy. Experience shows that a critical factor in obtaining good performance is ensuring that the quality of the images is maintained and measures are being implemented to address this.

Public Attitudes

Recommendation 5:

We welcome the Government's commitment to the principle of proportionality when it is considering implementing a biometric application. However, we are not convinced that the Government has clear steps in place—such as conducting mandatory privacy impact assessments—to measure consistently whether or not a specific biometric application is proportionate.

We have seen in the past how public trust in emerging technologies may be severely damaged in the absence of full and frank debate. Despite growth in commercial and Government applications of biometrics, the Government appears to have made little

effort to engage with the public regarding the increasing use of their biometric data, and what this means for them, since the scrapping of the Government's ID card scheme in 2010. This is exactly the type of issue that the Government's joint forensics and biometrics strategy should have addressed.

We recommend that the Government sets out, in its response to this report, how it plans to facilitate an open, public debate around the growth of biometric systems.

The Biometrics Strategy is currently in development and therefore we cannot make firm commitments regarding the content or scope at this stage. However, we of course understand that there are public concerns around the use and retention of biometrics and we will consider how best to undertake public consultation on this issue as our plans progress.

The Home Office sponsors an ethics group to provide scrutiny, challenge and review of ethical issues raised by forensic science, focussed on DNA. We are considering whether the same ethical oversight should be applied to the collection, use and retention of fingerprints and custody images.

Data Storage and System Security

Recommendation 6:

High profile cyber-attacks and data loss incidents have undermined the public's confidence in the ability of both Government and industry to store their data securely. Security considerations should never be an "afterthought" or an optional extra. We welcome the Minister's confirmation that the security of the Government's biometric systems is "bolted on" at the beginning of the design process. However, such assurances alone will do little to diminish the public's concerns while data losses continue to occur.

We recommend that, in its response to this report, the Government outlines the steps taken to mitigate the risk of loss, or unauthorised release, of the biometric data that it holds.

The Home Office Biometric Programme takes the security of biometrics and associated data very seriously. The Home Office systems currently holding biometric data employ a range of defence in depth measures appropriate to the value of the data. These measures are subject to regular effectiveness reporting and are subject to third-party assurance and annual assessment to ensure their fitness for purpose.

The biometrics team use a "secure by design" philosophy where security is considered at the start of the project. A risk discovery process is conducted at the start of a project. The impact of loss and corruption are captured through stakeholder workshops. The threats to the system are then analysed and appropriate controls are defined and implemented.

Although the Biometrics Strategy is currently in the early stages of development and we cannot make firm commitments regarding the content or scope, we acknowledge that

security standards and data loss are an important part of biometrics. Therefore we will take account of the Committee's recommendation as we develop the strategy further.

Recommendation 7:

Current legislation places responsibility on the institution rolling out a (biometric) system to ensure that appropriate security measures are in place when storing personal data. However, we are concerned that there is no proactive, independent oversight of whether this is occurring. Conducting a privacy impact assessment at the outset of all projects and policies that collect, retain or process personal data would help to ensure that those implementing a biometric system are fully aware of, and compliant with, the necessary security measures.

We therefore reiterate the recommendation made in our report, the Responsible Use of Data, that privacy impact assessments should be conducted at the outset of all projects and policies that collect, retain or process personal data, including biometric data.

The Information Commissioners Office (ICO) Code of Practice provides guidance as to when a Privacy Impact Assessment (PIA) should be undertaken, whilst making it clear that carrying out a PIA is not a requirement of the Data Protection Act (DPA). The ICO encourages Government departments to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle to ensure that potential problems are identified at an early stage.

PIAs are widely carried out across Government where personal data is collected, transferred or stored, including at the Home Office. Internal guidance sets out the process for all staff to follow to ensure that risks to privacy are considered an early stage to protect individuals' data and safeguard their rights of privacy. We believe that assessing and managing risks to privacy is crucial to the strategic and operational management of the Department. The Home Office has previously conducted PIAs in respect of biometrics. Prior to the launch of Mobile ID, a PIA was conducted in 2009 and this was updated in 2012.

In addition, as part of the Government's data science programme, we are developing an ethical framework to ensure we maximise the use of the greater amount of available data to create insight that can improve public policy and government operations, in a way that the public would understand and feel comfortable with.

Recommendation 8:

In our opinion, under no circumstances should the state roll out a biometric system that does not provide any scope for human intervention.

In the interests of greater transparency of data collection and use, we reiterate our earlier recommendation; namely that the Government drives the development of a set of information standards that companies can sign up to, under which they commit to explain to individuals their plans for the use of personal data (including biometric data), in clear, concise and simple terms.

The Government considers that consumer awareness and trust in how personal information is used by companies can provide benefits and reassurance to both businesses and citizens.

The Government is working with the Digital Catapult and the British Standards Institution, along with businesses and consumer representative bodies, to develop a 'Trust Framework' for commercial use of personal data. The Framework is being designed to give consumers more clarity and a greater level of control on how their data is collected, stored and used by companies. The Digital Catapult is looking to run a number of pilot projects over 2015, with the aim of completing the initial stages of the Framework by March 2016.

The government appointed a Chief Data Officer in March 2015, supported by a Government Data Standard to ensure transparency in the use of data by Government, and a common approach to data that is consistent with relevant legislation.

Legislation and Standards

Recommendation 9:

We agree with the Government and the Information Commissioner's Office that, as a principle-based framework, the Data Protection Act 1998 should provide adequate regulation in the face of developments in biometric technologies. However, we are mindful of the concerns raised by experts in the field, such as Professor Sue Black, and therefore recommend that the Government keeps this matter under review.

The Government always keep important issues of the protection of public data under review. Specifically, the European Commission published a proposal for a new Regulation on data protection on 25 January 2012 which, if adopted, will repeal and replace the 1995 Data Protection Directive on which the Data Protection Act 1998 is based. As such all data protection issues will be comprehensively reviewed in the near future.

Recommendation 10:

To avoid a biometric application once again being put into operational use in the absence of a robust governance regime, we recommend that:

a) the forensics and biometric policy group is reconstituted with a clearer mandate to analyse how developments in biometrics may compromise the effectiveness of current policy and legislation;

b) as recommended in paragraphs 35 and 36, the reconstituted group should operate in a transparent manner, be open to receiving inputs from external bodies and publish its outputs;

c) the Government, police and the Biometrics Commissioner should use these outputs to identify gaps in the legislation to be addressed ahead of any new biometric application going live.

The Forensic Policy Group has been reconstituted in order to deliver a Forensic Strategy by the end of 2015. In developing the Forensic Strategy we are consulting a wide range of stakeholders to ensure we have considered effectively the challenges and opportunities in this area.

We are developing the Biometric Strategy and we need to consider carefully the mandate for such a group to identify legislative gaps or changes. The strategy will need to support the delivery and use of biometrics by Government whilst ensuring that the legal, ethical and public sensitivities implications are effectively addressed. In order to do so, an effective governance regime will be vital.

As outlined in our response to Recommendation 2, we will not automatically publish outputs of policy discussion groups during the development stage, however we remain committed to publishing both the Forensic and Biometric Strategies by the end of 2015 and at that time we will consider future arrangements for overseeing delivery.

The role of the Biometrics Commissioner

Recommendation 11:

We agree with the Biometrics Commissioner that there is value in the provision of day-to-day, independent oversight of police use of biometrics and that such oversight should extend beyond fingerprints and DNA. We also agree that broadening the Commissioner's responsibilities would be a "more sensible" approach than establishing a new, separate commissioner covering other biometric traits.

We therefore recommend that the statutory responsibilities of the Biometrics Commissioner be extended to cover, at a minimum, the police use and retention of facial images. The implications of widening the Commissioner's role beyond facial images should also be fully explored, costed and the findings published. We further recommend that the Government clarifies where the operational boundaries lie between the Biometrics Commissioner and the Forensic Science Regulator.

The Biometrics Commissioner currently has three roles, as defined in section 20 of the Protection of Freedoms Act 2012:

1. to keep under review the retention and use by the police of DNA samples, DNA profiles and fingerprints;

2. to decide applications by the police for the extended retention of DNA profiles and fingerprints from individuals who have been arrested for, but not charged with, a qualifying offence, and;

3. to keep under review National Security Determinations which are made or renewed by Chief Officers and pursuant to which DNA profiles and/or fingerprints may be retained for national security purposes.

The Forensic Science Regulator's role was described by the then responsible Minister, when announcing the establishment of the post, as '*to advise Government and the Criminal Justice System on quality standards in the provision of forensic science. This will involve identifying the requirement for new or improved quality standards; leading on the development of new standards where necessary; providing advice and guidance so that providers will be able to demonstrate compliance with common standards, for example, in procurement and in courts; ensuring that satisfactory arrangements exist to provide assurance and monitoring of the standards and reporting on quality standards generally*'.

The Biometrics Commissioner's role therefore relates to reviewing police use of DNA and fingerprints to ensure it is proportionate, effective and in accordance with the law whereas the Forensic Science Regulator's role is to ensure that quality standards are upheld and that forensic evidence can be relied on.

As Lord Bates announced earlier this year, the Home Office is currently undertaking a policy review of the statutory basis for the retention of facial images, and consulting key stakeholders. Terms of Reference for the review were agreed following consultation with

the Information Commissioner, Biometrics Commissioner and Surveillance Camera Commissioner. As part of that review, we are considering the role of the Biometrics Commissioner, the Government will of course publish the findings of the review and consult formally as appropriate.

Quality Standards

Recommendation 12:

Standards become increasingly useful when they are widely adopted—namely required by customers and used by vendors to build standards-compliant products. As a customer, the Government can demand that its biometric systems adhere to national and international standards. While we recognise the advantages of the Government using its procurement powers in this way, and of the benefits of interoperability between biometric systems, we are also aware that there will be instances when interoperability should be prevented in order to limit access to sensitive personal information. Once again, in the absence of a comprehensive biometrics strategy, it is not clear how the Government aims to strike this delicate balance.

The Government should explain, in the interests of the responsible use of data, how it intends to manage both the risks and benefits that arise from promoting open standards and the interoperability of biometric systems.

The biometrics landscape has operated with a number of widely adopted international standards for many years, this has been vital in ensuring that governments are able to share data, where allowed and required, and has achieved significant benefits including; solving crimes, finding missing people and controlling immigration. The benefits from standardisation have helped to drive down the cost of systems. The use of open standards does not however imply that the data will be made available for unauthorised use. Where data is shared, the use of the data is strictly defined, the transit of the data is secured and the access to the data is strictly controlled through authentication and authorisation functions. In addition recipients must have robust audit controls in place to confirm the appropriate use and handling of the data.