House of Commons

Science and Technology Committee

Current and future uses of biometric data and technologies

Sixth Report of Session 2014–15

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 25 February 2015

HC 734
Published on 7 March 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.

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

Current membership

Andrew Miller (*Labour, Ellesmere Port and Neston*) *(Chair)*
Dan Byles (*Conservative, North Warwickshire*)
Jim Dowd (*Labour, Lewisham West and Penge*)
Mr David Heath (*Liberal Democrat, Somerton and Frome*)
Stephen Metcalfe (*Conservative, South Basildon and East Thurrock*)
Stephen Mosley (*Conservative, City of Chester*)
Pamela Nash (*Labour, Airdrie and Shotts*)
Sarah Newton (*Conservative, Truro and Falmouth*)
Graham Stringer (*Labour, Blackley and Broughton*)
David Tredinnick (*Conservative, Bosworth*)

The following members were also members of the committee during the parliament:
Gavin Barwell (*Conservative, Croydon Central*)
Caroline Dinenage (*Conservative, Gosport*)
Gareth Johnson (*Conservative, Dartford*)
Gregg McClymont (*Labour, Cumbernauld, Kilsyth and Kirkintilloch East*)
Stephen McPartland (*Conservative, Stevenage*)
David Morris (*Conservative, Morecambe and Lunesdale*)
Jonathan Reynolds (*Labour/Co-operative, Stalybridge and Hyde*)
Roger Williams (*Liberal Democrat, Brecon and Radnorshire*)
Hywel Williams (*Plaid Cymru, Arfon*).

Contents

Report

Summary

In its broadest sense, biometrics is the measurement and analysis of a biological characteristic (fingerprints, iris patterns, retinas, face or hand geometry) or a behavioural characteristic (voice, gait or signature). Biometric technologies use these characteristics to identify individuals automatically. Unlike identity documents or passwords, biometrics cannot be lost or forgotten since they are a part of the user and are always present at the time of identification. They are also difficult, though not impossible, to forge or share.

Three future trends in the application of biometrics were identified during the inquiry: the growth of unsupervised biometric systems, accessed via mobile devices, which verify identity; the proliferation of "second-generation" biometric technologies that can authenticate individuals covertly; and the linking of biometric data with other types of 'big data' as part of efforts to profile individuals.

Each of these trends introduces risks and benefits to individuals, to the state and to society as a whole. They also raise important ethical and legal questions relating to privacy and autonomy. We are not convinced that the Government has addressed these questions, nor are we satisfied that it has looked ahead and considered how the risks and benefits of biometrics will be managed and communicated to the public.

The Government has been largely silent on the matter since the abolition of the Government's Identity Card Programme in 2010 and the destruction of the National Identity Register. And yet, in other policy areas, including immigration and law enforcement, the use of biometric identification systems by the state has expanded. If the Government is to build public trust in biometric data and technologies, there is a need for open dialogue and greater transparency. We therefore recommend that the Government sets out how it plans to facilitate an open, public debate around the use of biometrics.

Management of the risks and benefits of biometrics should have been a core element of the Government's joint forensics and biometrics strategy. Despite undertaking to publish this document at the end of 2013, we were dismayed to find that there is still no Government strategy, no consensus on what it should include, and no expectation that it will be published in this Parliament. This is inexcusable. We expect a comprehensive, cross-departmental forensics and biometrics strategy to be published by the Government no later than December 2015.

In the absence of a biometrics strategy, there has been a worrying lack of Government oversight and regulation of aspects of this field. We were particularly concerned to hear that the police are uploading photographs taken in custody, including images of people not subsequently charged with, or convicted of, a crime, to the Police National Database and applying facial recognition software. Although the High Court ruled in 2012 that existing policy concerning the retention of custody photograph by the police was "unlawful", this gap in the legislation has persisted. At the very least, there should be day-to-day, independent oversight of the police use of all biometrics. We therefore recommend that the Biometrics Commissioner's jurisdiction should be extended beyond DNA and fingerprints to cover, at a minimum, the police use and retention of facial images.

1 Introduction

Background

1. Authenticating personal identity is an integral part of participating in modern life. From entering an office building and logging on to a networked computer, to applying for a mortgage, we are regularly faced with requests to verify who we are. More 'traditional' authentication methods rely on an individual knowing and recounting key personal details, such as their date of birth or address, and presenting documents that corroborate their answers, including a driver's licence, a birth certificate, or passport. In other contexts, an individual might be required to enter a password or PIN code, or present a security pass.

2. In most instances, the purpose of this type of identity authentication is to prevent illegal activities and to inhibit imposters from acquiring something that is protected. An identity, in other words, is valuable. In an increasingly globalised world, where we interact in virtual as well as physical spaces, our personal data can travel with ease across geographical boundaries, sometimes leaving us unsure about where, and by whom, our data is held. Furthermore, the documents, tokens and codes relied upon as proxy representations can be lost, forgotten, stolen, forged and manipulated. This is particularly problematic for citizens who, in the face of heightened concerns about national security, terrorism and identity theft, are increasingly required to be readily identifiable. Both Government and industry have attempted to address some of these problems through developing ever more sophisticated authentication practices. This report focuses on one aspect of that work; the development of a suite of techniques collectively known as 'biometrics'.

3. Biometrics has been described as the "science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person".[1] These attributes (or 'traits') include, but are not limited to, fingerprints, retinas, irises, faces, hand geometry, DNA, voice and gait. In biometric systems, they are used for automated, or semi-automated, identity recognition by comparing a trait captured in 'real-time' by a sensor (a 'live template') against a copy of the same trait stored on a database, or on a token held by the user, such as a smart card (a 'stored template'). Comparison is achieved through the application of a matching algorithm and a match score is generated. The match score indicates the degree of similarity between the two templates being compared: the higher the score the more certain the system is that the two templates belong to the same person.

4. Biometric systems are thought to have a number of advantages over traditional methods of verifying identity: they cannot be lost or forgotten since they usually require the individual to be present at the time of identification and they are difficult to copy, forge or share. With the exception of photo ID passes, the use of biometric systems has, until comparatively recently, been confined to law-enforcement, national security and military contexts. As the technologies have matured, and the financial and computational resources required have become more widely available, the use of biometric systems has spread into more commercial and consumer-focused applications. Accompanying this growth in

[1] Anil K Jain and Arun Ross, Introduction to Biometrics in Handbook of Biometrics by Anil K. Jain, Patrick Flynn, Arun A. Ross (New York, 2008) p1

commercial applications of biometrics has been a shift in their deployment by the state. Our predecessors examined the use of biometrics in the Government's Identity Card Programme in 2006.[2] Among other things, this programme established a 'National Identity Register' which recorded individuals' "biometric information".[3] However, the *Identity Documents Act 2010* subsequently made provision to repeal the *Identity Cards Act 2006* and destroy all the information, including biometric data, recorded in the National Identity Register.[4]

5. Two years later, further regulation of biometric data was introduced following the passage of the *Protection of Freedoms Act 2012* (PoFA).[5] Part 1 of the Act introduced a new regime governing the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints.[6] The Act also included provisions relating to the protection of biometric information of children in schools, including a requirement to "notify and obtain consent before processing [their] biometric information".[7] To provide independent oversight of this new regime, the PoFA introduced a statutory 'Commissioner for the Retention and Use of Biometric Material' (the Biometrics Commissioner).

Our inquiry

6. On 7 August 2014, we announced our inquiry on *Current and future uses of biometric data and technologies* and sought written submissions addressing the following points:

a) How might biometric data be applied in the future? Please give examples.

b) What are the key challenges facing both Government and industry in developing, implementing and regulating new technologies that rely on biometric data? How might these be addressed?

c) How effective is current legislation governing the ownership of biometric data and who can collect, store and use it?

d) Should the Government be identifying priorities for research and development in biometric technologies? Why?

7. We received 33 written submissions and took oral evidence from 14 witnesses including:

- academics working in the fields of biometrics and forensic science;

---

2 House of Commons Science and Technology Committee, Sixth Report of Session 2005–06, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, HC 1032

3 Identity Cards Act 2006. Schedule 1

4 Identity Documents Act 2010, section 1; Identity Cards Act 2006

5 Protection of Freedoms Act 2012, Part 1

6 The biometric provisions were introduced in response to, among other things, the decision of the European Court on Human Rights in the case of *S and Marper v United Kingdom [2008]*, which held that holding DNA samples of individuals arrested, but later acquitted, or who have the charges against them dropped, is a violation of the right to privacy under the European Convention on Human Rights.

7 Protection of Freedoms Act 2012, section 26

- representatives from commercial organisations developing and implementing biometric systems;
- a civil liberties group;
- the Association of Chief Police Officers (ACPO)
- officials from the Information Commissioner's Office and the Office of the Biometrics Commissioner;
- the Government, represented by Lord Bates, Parliamentary Under-Secretary of State for Criminal Information, Home Office (hereafter "the Minister") and Marek Rejman-Greene, Senior Biometrics Adviser, Home Office.

We would like to thank everyone who contributed to the inquiry.

8. This report considers both the commercial applications of biometrics and the use of biometric systems by the state, particularly in the context of law enforcement and criminal justice. The future uses of biometrics and the Government's readiness for these applications are considered in Chapter 2, while Chapter 3 examines the diverse challenges facing both Government and industry in developing and implementing biometric systems. Chapter 4 then focuses on the effectiveness of current legislation governing the use of biometric data and questions whether it remains fit for purpose. In response to evidence received about the use of facial recognition software by the police, we particularly examine whether the Government is prepared for prospective developments in biometrics that might pose challenges to current policy and legislation.

Ethical considerations

9. Throughout this report, we are primarily concerned with the science and technology of biometrics. However, the application of biometric data and technologies undoubtedly raises ethical and legal questions related to privacy, autonomy, informed consent, confidentiality and liberty. These values are not absolute but, in liberal democracies like the UK, there is a strong presumption of not restricting them.[8] The principle of proportionality—ensuring that a balance is struck between society's need for a biometric system and an individual's privacy rights—is therefore examined in detail in Chapter 3 and guides many of the subsequent recommendations in this report.

[8] Nuffield Council on Bioethics, *The forensic use of bioinformation: ethical issues. Executive Summary*, (September 2007)

2 Future uses of biometrics

11. In early 2014, analysts forecast that the global biometrics market would grow from $8.7 billion in 2013 to nearly $27.5 billion by 2019 and register a five-year compound annual growth rate of 19.8% between 2014 and 2019. In Europe, a slightly lower compound annual growth rate of 17.25% was projected between 2013 and 2018.[9] This chapter considers the drivers of this predicted expansion and examines how biometric data might be used in the near future. It then turns to question if, and how, the Government is preparing for these trends.

Functionalities of a biometric system

12. Witnesses from industry were optimistic about growth prospects of biometrics. Pointing to the "staggering increases in the speed and accuracy of automated biometric search engines", 3M stated that the science and technology of biometrics had "advanced quickly and significantly over the past two decades"; a trend they expected "to continue or accelerate in the future".[10] Others were more circumspect in their analysis of future prospects. Professors Nixon and Kittler described the science of confirming identity by personal characteristic as being "young at present" while Innovate UK told us that the "penetration of early adopter markets such as banking [was] still required before biometric technologies [became] second nature".[11]

13. At present, biometric systems can be used in at least three different ways:

- **Verification:** ensuring that a person is who they claim to be
- **Identification:** determining who a person is (e.g. identifying a person in a crowd)
- **Screening:** determining whether a person belongs to a 'watch list' of identities.

Biometrics can be implemented as 'supervised' systems, such as at border crossings and as part of immigration control, or as 'unattended' systems that are used remotely 'on-the-go' increasingly via sensors on mobile phones. With supervised systems, the environmental surroundings (e.g. lighting, ambient conditions) are controlled and there is the opportunity for human intervention should a problem arise. For example, if the ePassport gates at Heathrow Airport, which rely on facial recognition, are not working, a passenger is still able to have his or her passport checked manually by a UK Border Agency official. The ePassport gates are also monitored by officials to prevent the system being 'spoofed'.

14. Our witnesses forecast three future trends in the application of biometrics: first, the growth of unsupervised systems that verify identity; second, the proliferation of "second-generation" biometric technologies that can authenticate individuals remotely without

9 Companies and Markets, 'Biometrics: Technologies and Global Markets', last accessed 2 February 2015; Business Wire, 'Research and Markets: European Biometrics Market 2014-2018', accessed 12 January 2015

10 3M (BIO0018) para 8; see also Identity Assurance Systems (BIO0031) para 3.1

11 Professor Nixon and Professor Kittler (BIO0010) para 9; Innovate UK (BIO0029) para 7; see also Super-identity project (BIO0015) para 11

their knowledge; and third, the linking of biometric data with other types of 'big data' as part of efforts to 'profile' individuals.

Trend 1: Mobile biometrics

15. The use of unsupervised biometric systems, accessed via sensors on mobile devices, was singled out as an area likely to experience growth in the near future. Northrop Grumman predicted that "biometric applications for […] mobile devices [would] proliferate" while the Biometrics Institute quoted its 2014 survey which identified "mobility" as the "most significant development" in biometric systems that was on the horizon, particularly through the "adoption of mobile payments".[12] Dr Richard Guest, University of Kent, anticipated that the "ubiquity of mobile devices capable of obtaining biometric samples" would "enable biometric usage in innovative contexts". He added that this would potentially represent a "paradigm shift" in which biometrics would become "an everyday", rather than an occasional, "method of assuring identity".[13]

16. A number of mobile biometrics are already in operation. Barclays, for example, announced that from 2015 it would be rolling out a biometric reader to access accounts for its corporate clients, instead of using a password or PIN. The reader will scan a finger and identify unique vein patterns.[14] The Information Commissioner's Office (ICO) also highlighted how some mobile phones and laptops now contained "fingerprint sensors to authenticate the device's owner in order to grant or deny access to the device"; a move the ICO described as placing biometric systems in "the hands of individuals", rather than restricting their use to "governments or law enforcement agencies".[15] Sir John Adye, Identity Assurance Systems, drew attention to the Apple iPhone 6 which, he noted, could be used for "Apple payments" using its 'Touch ID' ('a fingerprint identity sensor').[16] On the other hand, Ben Fairhead, 3M, pointed out that these technologies were not yet in widespread use, while Dr Guest suggested that "consumer-level" mobile biometrics—like the iPhone 6—currently had something of a "gimmick value".[17]

Trend 2: Covert identification of individuals

17. Deploying biometric systems to identify a stranger and determine who they are was another prospective trend identified by witnesses. The 'stranger' may be unaware that this type of identification is taking place. According to the National Security Alliance, "second-generation biometric technologies […] can authenticate individuals remotely without their knowledge", a point echoed by Big Brother Watch.[18] At present, covert identification is primarily achieved through facial recognition software. Northrop Grumman expected

12 Northrop Grumman (BIO0030) para 3.i; Biometrics Institute Limited (BIO0003) para 4.1

13 Super-Identity Project, University of Kent (BIO0015) para 1. Dr Guest submitted evidence jointly with two other academics: Dr Sarah Stevenage, University of Southampton and Professor Sue Black, University of Dundee

14 "Barclays taps vein biometrics in bank fraud fight", Reuters, 5 September 2014

15 Information Commissioner's Office (BIO0009) paras 11&12

16 Q46; see also https://www.apple.com/uk/iphone-6/touch-id/. According to Apple, Apple Pay works by holding your iPhone near a contactless reader, with your finger on Touch ID, in order to authorise a payment. At the time of writing, Apple Pay had been launched in the United States but was not available in Europe.

17 Q31 [Ben Fairhead]; Super-Identity Project, University of Kent (BIO 0015) para 11

18 National Security Alliance (BIO0007); Big Brother Watch (BIO0002)

"surveillance applications for finding and identifying faces in crowds" to start to "flourish with advancements in face matching algorithms, better cameras and lenses that can see and match in partial lighting conditions".[19]

18. The Government acknowledged that there was "an increasing interest in the application of automated facial recognition systems" and pointed to a "pilot project being run by Leicestershire Constabulary".[20] The project—the 'NeoFace system'—uses measurements taken from an image of a face and compares them to 92,000 images on the police force's database. The BBC have reported that the images could come from anywhere, though CCTV and police body cameras had been the most common source so far.[21] Both the Biometrics Commissioner and the Information Commissioner's Office (ICO) drew attention to this software, while the ICO suggested that "the surreptitious collection of information about individuals that they would not necessarily expect" could also come from "a fingerprint or genetic material left behind", and not just from "facial recognition in live or recorded images".[22]

19. As well as deploying this technology for national security and law-enforcement purposes, other witnesses noted that it could be used as part of consumer marketing. The Biometrics Institute highlighted the example of 'photos' being captured by CCTV in public spaces, such as casinos and shopping centres, and subsequently matched "with photos from social networking sites with the aim of identifying the individuals and selling the information to brokers to target these people with advertising campaigns about betting".[23]

Trend 3: Linking biometric data

20. In our earlier report, the *Responsible Use of Data*, we highlighted the potential offered by 'Big Data'[24] and noted that the Government, in partnership with the Economic and Social Research Council's Administrative Data Research Network, was working to "facilitate access to, and linkage of, de-identified administrative data routinely collected by government departments and other public sector organisations".[25] Linking together these different data has been strongly supported by the Government for its potential to "join the dots" and establish rich, contextualised insights that could "provide a sound evidence base to inform research, and policy development, implementation and evaluation".[26]

---

19 Northrop Grumman (BIO0030) para 3

20 The Government (BIO0035)para 3.2

21 "Leicestershire Police trial facial recognition software", BBC News Online, 15 July 2014

22 Biometrics Commissioner (BIO0027) para 7 onwards; Information Commissioner's Office (BIO0009) para 8

23 Biometrics Institute Limited (BIO0003)

24 According to the Information Commissioner's Office, Big Data is characterised "by volume, variety and velocity of data, and by the use of algorithms, using 'all' the data and repurposing data" see Information Commissioner's Office, *Big data and data protection*, (July 2014), para 1

25 House of Commons Science and Technology Committee, Fourth Report of Session 2014–15, *Responsible Use of Data*, HC 245, footnote 9

26 Civil Service Quarterly, Joining the dots, 15 October 2014, accessed 26 January 2015; Economic and Social Research Council, The Big Data Family is born - David Willetts MP announces the ESRC Big Data Network, 10 October 2013, accessed 26 January 2015

21. Some witnesses predicted that "advanced algorithmic analytics" would lead to biometric data being seen and used "as simply more available data points in a 'big data' world".[27] Professor Louise Amoore, Durham University, was clear that a "likely future trajectory" was a shift towards "the integration of biometric data" into a "much larger and rapidly growing array of digital 'big data'" in ways that were "capable of producing profiles or behavioural maps of individuals and groups".[28] British Standards Institution (BSI) similarly predicted that the identification of individuals would "be possible using a wider range of non-traditional biometric data sets and […] by combining data sets using 'Big Data' approaches".[29]

22. Professor Amoore described such developments as potentially "game-changing" on the grounds that there are:

> analytics engines […] that can mine biometric data that is available on the internet, and link that to other forms of data […] That moves us more in the direction of indicating not just who someone is but suggesting that one might be able to infer someone's intent from some of the biometric data.[30]

23. Evidence from the Super-Identity Project indicated that this potential was already being realised. Dr Richard Guest, University of Kent, noted how the project had shown that biometric data could be linked with "cyber activity and personality assessment" data in such a way that made it possible to obtain "unknown elements of identity from known elements".[31] Adidas' "Consumer DNA" system was also highlighted as a further example of data linkage. According to Professor Amoore:

> it is asking what the ideal future Adidas customer looks like. It is using YouTube videos, and it wants to know not just what this person likes to do, what music they like to listen to, what trainers they are likely to purchase, but it also wants to know when they are next present online. Part of that is knowing something about their biometric template from the facial biometric data.[32]

Government horizon scanning

24. In its written evidence, the Government acknowledged that there had been significant growth in the "use of biometric information for identification, by the state and others" and also recognised some of the trends outlined in this Chapter.[33] Considering "how emerging trends and developments might potentially affect current policy and practice" is, according to the Government, an integral part of "horizon scanning" and is "already being done in

27 Professor Amoore (BIO0006) para 1.2

28 Professor Amoore (BIO0006) paras 1.1 & 1.2; see also National Security Alliance (BIO0007) para 1.2

29 British Standards Institution (BIO0020) para 3.2

30 Q3 [Professor Amoore]

31 Super-Identity Project, University of Kent (BIO0015) para 3

32 Q17

33 The Government (BIO0035) para 1.2

government departments".[34] Our inquiry into Government horizon scanning found it to be a "potentially valuable activity" that could "enhance both short- and long-term decision-making" but we also identified "inconsistencies of practice and performance" across government departments. [35]

25. During this inquiry, the Government provided only a limited amount of detail on how emerging trends and developments might potentially affect current policy and practice in biometrics. The Minister cautioned that it was "very difficult to get out in front" in biometrics since the Government was "often reacting to particular stories, concerns and issues that come to light in the public square".[36] Indeed, where emerging technologies are concerned, we have observed successive Governments make limited efforts to get out on the front foot. Instead, the Government stated that its written evidence indicated "the direction of travel the Government [wished] to set in this area". [37] The lack of accompanying information about how this was to be achieved in practice was particularly apparent in the case of the Government's "Identity Assurance Programme" (IAP).

26. The IAP is a Cabinet Office initiative that sets "standards for verifying an individual's identity" which is intended "to be used across Government".[38] According to the Government, the IAP aims to give citizens a secure and convenient way to sign in to Government services and requires the user to set up an "identity profile" to do things such as renew a driver's licence or apply for a passport.[39] In its written evidence, the Government explained that Identity Assurance Programme "includes four levels of identity assurance, of which the highest (Level 4) is dependent upon the use of biometrics".[40] Unfortunately, it appears that the prospect of biometric verification has been announced without full consideration of how it might be implemented. Mr Marek Rejman-Greene, Home Office, told the Committee that "none" of the 25 exemplar services currently trialling the IAP required Level 4 verification. He clarified that this was "because the infrastructure [had] not been put in place as part of the [Identity Assurance Programme] scheme" before adding that "the plans for the much longer term of the identity assurance scheme [were] still being worked on".[41]

27. The Biometrics Commissioner pointed to the "value in someone looking forward and trying to identify what challenges are to come, what sort of governance arrangements are going to be needed", adding that this was both "welcome" and "desirable".[42] The Government's Foresight Programme would appear to be well-placed to provide this type of analysis. Established in 1994, Foresight is the Government Office for Science's centre for

---

34 Cabinet Office/Government Office for Science, "Horizon scanning programme: a new approach for policy making", 12 July 2013

35 Science and Technology Committee, Ninth Report of Session 2013-14, *Government horizon scanning*, HC 703, para 10 & para 25

36 Q178 [the Minister]

37 The Government (BIO0035) para 1.2

38 The Government (BIO0035) para 1.10

39 See for example: Government Digital Service, 'What is identity assurance?', accessed 12 January 2015

40 The Government (BIO0035) para 1.10

41 Q166 & Q169

42 Q102

futures analysis. Its role is to help "the UK Government to think systematically about the future" in order to "ensure today's decisions are robust to future uncertainties".[43] It is somewhat striking, then, that Foresight's 2013 report *Future Identities: changing identities in the UK* states on page 6 that biometric identities "were beyond the scope of the project" and therefore provides no evidence or advice to Government on biometrics.[44]

28. **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.**

29. ***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 value of horizon scanning in the narrower context of biometrics used in law enforcement is considered in detail in Chapter 4.

Scientific advice on biometrics

30. Building on the work of our predecessors, we have taken a close interest throughout this Parliament in making sure that the institutional design of scientific advisory bodies facilitates the delivery of robust, evidence-based advice to Government. In its 2006 report, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, a predecessor Science and Technology Committee noted that the Home Office had formalised its scientific and technical advice structures on biometrics by creating two scientific advisory committees: the Biometrics Experts Group and the Biometrics Assurance Group (BAG), with the latter chaired by the Government Chief Scientific Adviser. In addition to these advisory committees, the Home Office Biometrics Centre of Expertise was established in 2005 and based at the Home Office Scientific Development Branch (now known as the Centre for Applied Science and Technology).[45]

31. According to its 2007 annual report, the BAG provided "oversight and review" of the biometric elements of Government programmes and offered advice and "additional assurance" that the Government was making effective use of biometric technology.[46] While the BAG primarily provided advice in the context of the Government's identity cards programme, it was anticipated by the then Head of the Home Office Biometrics Centre of

---

43 Research Councils UK, 'Foresight', accessed 12 January 2015

44 Government Office for Science, *Foresight Future Identities Final Project Report* (January 2013) p 6

45 House of Commons Science and Technology Committee, Sixth Report of Session 2005–06, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, HC 1032, paras 49 & 52

46 Biometrics Assurance Group, *Annual Report 2007* (July 2008), p4

Expertise, Mr Marek Rejman-Greene, that its remit would be broadened "to look at all the other related [Government] programmes using biometrics", such as the UK visas programme.[47]

32. Appearing in front of the Committee eight years later, Mr Rejman-Greene, now Senior Biometrics Adviser, Home Office, confirmed that the BAG's remit had not, in fact, been broadened. Instead, he explained that it no longer existed:

> The biometrics assurance group was formed at the request of Parliament specifically to look at the national identity scheme. As that scheme was beginning to go into roll-out, the need for it began to be less pressing. In addition, the loss of one of the members of that biometrics assurance group […] meant we were missing a considerable part of the industry inputs. The decision was made that that was no longer as pressing. There may well be a question about whether it should come back again.[48]

In the absence of the BAG, scientific and technical advice to Government on biometrics has come from other sources. Both Andrew Tyrer, Innovate UK, and Mr Rejman-Greene called attention to the Biometrics Working Group, a "technical working group within Government which has access to specialists" who meet quarterly to talk "in a very informal format around the challenges of biometrics".[49] This appears to have evolved out of the original 'Biometrics Experts Group'.[50] Mr Alastair MacGregor, Biometrics Commissioner, and the Minister, also noted the work of the "forensics and biometric policy group" which, according to the Biometrics Commissioner, is "quite a large and wide-ranging group" concerned with "the development of a national strategy for both forensic science generally and biometrics".[51]

33. It was noticeable that the work of the forensics and biometric policy group was not directly referred to anywhere in the written evidence. We have come across this group before and have previously raised concerns about its lack of transparency and its failure to publish the minutes of its meetings.[52] The *2010 Principles of scientific advice to Government* ("the Principles") point to the need for "clear roles and responsibilities", "transparency and openness" and "independence" when providing scientific and engineering advice to Government, though their application is limited to:

> ministers and government departments, all members of Scientific Advisory Committees and Councils […] and other independent scientific and engineering advice. They do not apply to employed advisers, departmental

47 Oral evidence taken on 22 March 2006, HC (2005-06) 1032, Q283 [Mr Rejman-Greene]

48 Q147

49 Q147; Q78

50 Q147

51 Q142 & Q102

52 House of Commons Science and Technology Committee, Second Report of Session 2013–14, *Forensic science*, HC 610, para 115

> Chief Scientific Advisers or other civil servants who provide scientific or analytical advice.[53]

34. Without any information about the status of the forensics and biometric policy group—particularly with regard to its independence, or otherwise, from Government—it is not clear whether the Principles should apply. The Government predicted in its response to our 2013 report, *Forensic Science*, that the delivery of a forensics and biometrics strategy would "inevitably result" in the policy group "changing into a wider, more representative group" and added that "once this change [had] taken place the strategy and minutes of the new group [would] be published".[54] In the absence of a forensics and biometrics strategy (discussed in detail below), no such change has been forthcoming. Yet when confronted with the *status quo*, and asked whether it "would help public confidence" if the discussions of the group were "transparent", the Minister agreed that was "broadly what should happen" though he offered no explanation as to why this had, so far, failed to occur.[55]

35. **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.***

36. ***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.***

The need for a Government biometrics strategy?

37. We have longstanding concerns about the absence of a clear Government strategy and were therefore encouraged by the Government's reassurance, given in response to our 2013 report, *Forensic Science*, that it was "drawing up a biometric and forensic strategy to be completed by the end of the year [2013]".[56] It is now early 2015 and no strategy has been published. Instead, we have received a number of conflicting statements from the Government about its intentions.

38. In its written evidence, the Government stated that the "Home Office [was] working with the police and other partners to develop a Forensics and Biometrics Strategy", though

---

53 Government Office for Science, *Principles of scientific advice to government*, March 2010. The Government's recent Science and Innovation Strategy also points to the need for greater "openness" in science so that it becomes "less and less a closed community and more and more engaged with the world". See HM Treasury, Department for Business, Innovation & Skills, *Our plan for growth: science and innovation*, Cm 8980, December 2014, p 12

54 The Government Response to the Second Report from the House of Commons Science and Technology Committee Session 2013-14 HC 610: *Forensic science*, Cm 8750, November 2013, p 17

55 Q146

56 Government Response to the Second Report from the House of Commons Science and Technology Committee Session 2013-14 HC 610: *Forensic science*. November 2013 Cm 8750, p 17

it did not indicate what it might include.[57] We asked the Minister whether the biometrics strategy would take into account "the spectrum of applications" which we had heard about during our oral evidence sessions, "from access to schools or sports clubs through to issues around the criminal justice system" and whether it would "start to define where the limits are for applications within different Government sites". The Minister simply replied "yes".[58] However, when he was asked about the "absence of a strategy that was promised", he questioned the value of a national strategy, noting that "sometimes strategies are offered as a panacea and they do not always deliver". He added that "one of the things" the "cross-Government forensics and biometric policy group" was currently addressing was "whether there is a need for a strategy".[59] This was the first time we had heard it suggested that the Government biometrics and forensics strategy—a document we were previously told was due to be completed in late 2013—was now contingent on first establishing a clear "need".

39. Neither the Biometrics Commissioner, nor Chief Constable Sims, Association of Chief Police Officers (ACPO), shared the Minister's doubts about whether a Government strategy was necessary. Mr Alastair MacGregor, Biometrics Commissioner, told us that there was "value in a national strategy" in the field of biometrics.[60] He went on to emphasise that the strategy had "not just been forgotten as something that needs to be developed", rather "efforts [had] been going on to develop it" but that it had "not been easy".[61] Chief Constable Sims, ACPO, was also clear that there was still "some debate [required] to get to the point where we have an all-embracing national strategy". However, he stressed that he "absolutely" needed:

> that to happen because a whole set of significant issues and risks sit within forensic science. One or two of those have surfaced today, but there are many others. The way those risks are mitigated and managed is through that national strategy.[62]

40. In subsequent correspondence, the Minster confirmed that there was "general agreement among the [forensics and biometric policy] group that a national strategy would be helpful" but that there was "not yet a consensus view on what the strategy should focus on". On this basis, the Minister had "asked officials to do more work to ensure […] an evidence based assessment of the issues which we need to collectively address". The Minister anticipated this would take "three months, with the strategy itself to follow".[63] When later pressed to clarify if this meant the strategy would be "unfinished business by the end of this Parliament", the Minister was reluctant to give a date, simply adding "you may say that".[64]

---

57 The Government (BIO0035) para 3.4; Association of Chief Police Officers (BIO0036) para 5

58 Q144

59 Q142

60 Q102

61 Q122

62 Q121

63 The Government (BIO0038)

64 Oral evidence taken on 14 January 2015, HC (2014-15) 758, Q152-Q153

41. **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.**

42. **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.**

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

3 Development and implementation challenges

44. This chapter explores some of the challenges both Government and industry may face when developing, and implementing, the trends outlined in the preceding chapter. Witnesses identified a blend of technical and privacy challenges and we strongly urge the Government to address these matters in a national biometrics strategy.

The scientific foundations of biometric systems

45. Biometric recognition is a "probabilistic science".[65] Unlike identification systems that rely on entering a password or PIN code, which is either correct or incorrect, biometric systems are affected by "intra-class variations". These are differences between two templates of the same trait, from the same user, captured at different times. Intra-class variations arise from multiple sources: "body parts age, sensors get grimy, lighting conditions change", all of which can introduce discrepancies between the same user's biometric templates.[66] Biometric systems have to tolerate this degree of variability which, in practice, raises the prospect of false accept, and false reject, errors.[67] Dr Rice, Information Commissioner's Office, noted that there "will be very different acceptable error rates" depending upon the context: "the accuracy you would want from Heathrow airport or law enforcement would be very different from an advertising board that predicts gender".[68] In theory, the "science of biometrics" focuses on examining, and ultimately minimising, these errors. Some witnesses, however, questioned the scientific foundations of biometric systems.

46. Professors Black and NicDaeid stated that current biometric methods had "only minimal scientific grounding". According to the Professors, "the underlying solid research" was frequently "underfunded or non-existent" which had a "direct impact on the robustness of the biometric and confidence in its utilisation and its effectiveness".[69] Speaking to the Committee, Professor Black suggested that the "scientific base line" had been forgotten in the race "to meet commercial needs and security needs" and that it was now potentially time to "go back and give it a stronger foundation".[70]

47. However, Professor Louise Amoore, Durham University, suggested that the problem was not the underpinning science, *per se*, but rather how it was communicated, particularly once it became part of a biometric application. According to Professor Amoore, those writing "extraction algorithms and matching algorithms […] are quite candid that [they

65 Q5

66 Lockstep Consulting (BIO004) section 4

67 A false accept error occurs when the acquired (or 'live') template from one individual, who is not in the system, is wrongly matched to a stored template from another individual and they are mistakenly allowed access. A false reject arises when an acquired template from one individual does not match the stored template for that individual and they are wrongly denied access.

68 Q129 [Dr Rice]

69 Professor Black and Professor NicDaeid (BIO0017) paras 3&9

70 Q11 [Professor Black]

are] probabilistic" and see it as the responsibility of "the people who are buying the [biometric] system" to state "what sort of tolerance they have for the false acceptance rate versus the false reject rate". She stressed that this "doubt in the science [was] present in the room when […] writing the code" but that such doubt was "lost by the time [the code was] part of the hardware technology being used".[71]

Testing biometric systems

48. Particular attention was drawn to the rigour of the testing regime and the additional impact this had on the reliability of the biometric. Before an algorithm is deployed in a 'real-world' setting, its technical performance and accuracy (including the false accept and false reject error rates) are tested and evaluated on an artificial or simulated database containing biometric data samples. According to Innovate UK, testing biometric systems and measuring the "effectiveness of algorithms in different scenarios" is "difficult".[72] Several witnesses, for example, commented on the challenges associated with establishing "a comprehensive dataset of subjects with an unbiased population to test against".[73] Ben Fairhead, 3M, likened the process to that of a "drugs trial". He explained that "to really prove the accuracy of a new biometric modality" it needed to be tested "with a large number of different people" which, he stated, was "quite expensive"; a point reiterated by Mr Marek Rejman-Greene, Home Office.[74] Erik Bowman, Northrop Grumman, agreed and identified the lack of "availability" of large datasets for testing purposes as a potential barrier to advancing biometrics.[75]

49. Others questioned the value of laboratory testing of biometric systems. Lockstep Consulting, for example, stated that:

> testing on artificial or simulated databases tells us only about the performance of a software package on that data. There is nothing in a technology test that can validate the simulated data as a proxy for the 'real world'.[76]

Recognising this issue, the *Irish Council for Bioethics*, in its 2009 report on Biometrics, considered "post-deployment testing and fine tuning" to be "critical if the system is to obtain the performance levels observed in the laboratory when operated in the real world".[77]

50. Concerns were also raised about the independence of the testing regime. Andrew Tyrer, Innovate UK, told the Committee that a "lot of the rigour that goes into testing" was "quite often fronted by the manufacturers themselves". He went on to identify a "gap in the market […] around the testing of systems" on the grounds that there was

---

71 Q12 [Professor Amoore]

72 Innovate UK (BIO0029) para 10

73 Innovate UK (BIO0029) para 10

74 Q29 & Q148

75 Q31 [Erik Bowman]

76 Lockstep Consulting (BIO0004),section 5

77 Irish Council for Bioethics, *Biometrics: Enhancing Security or Invading Privacy?* (October 2009), p 9

currently "not a lot of independent activity".[78] Ben Fairhead's earlier analogy with "drugs trials" has particular relevance here since clinical trials are typically (though not exclusively) undertaken by commercial organisations aiming to develop a new product, rather than by an independent body. However, as we discussed in depth in our 2013 report, *Clinical Trials*, their conduct is regulated under the *2001 European Clinical Trials Directive* which was implemented in the UK in 2004 through the *Medicines for Human Use (Clinical Trials) Regulations*.[79]

51. In contrast, the testing of biometric systems is neither regulated nor universally standardised. Previous reviews of the technical literature on biometric device testing have highlighted a "wide variety of conflicting and contradictory testing protocols", including "single organisations" producing "multiple tests, each using a different test method".[80] Our predecessors in 2006, for example, found that "industry claims" about the performance of biometric systems "varied widely". They also drew attention to the role played by the Biometrics Assurance Group (BAG) in interpreting the outcomes of biometric testing, but, as noted above, the BAG no longer exists.[81]

52. When we asked if the Home Office conducted any independent testing, or whether it relied on assurances from the manufacturer, Mr Rejman-Greene, Home Office, replied that there were "occasions when we do it ourselves and occasions when we monitor the way in which suppliers undertake the testing". He added that "a standard was developed in the UK", with the hope of moving "towards a European standard". [82]

53. Exactly *when* such testing took place appeared to vary according to the system in question. For example, Mr Rejman-Greene highlighted the Immigration and Asylum Biometric System which, he told the Committee, had been "tested prior to delivery".[83] In contrast, Mr Alastair MacGregor, Biometrics Commissioner, reported that a "searchable national database of custody photographs" had "been put into operational use" by police forces in "the apparent absence of any very rigorous testing of the reliability of the facial matching technology that is being employed".[84] He added that the Home Office's Centre for Applied Science and Technology was currently "looking at the algorithm applied to images on the police national database" and that, at the moment, the software was being used for "investigatory purposes only": "No one is being prosecuted simply on the basis of, 'We've got an automatic match'".[85]

54. **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**

---

78 Q71

79 House of Commons Science and Technology Committee, Third Report of Session 2013–14, *Clinical Trials*, HC 104, paras 13-15

80 A. J. Mansfield & J.L. Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices*, NPL Report CMSC14/02, August 2002, p1

81 House of Commons Science and Technology Committee, Sixth Report of Session 2005–06, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, HC 1032, paras 18 & 51

82 Q148; see also British Standards Institution (BIO0020) Annex

83 Q148

84 Biometrics Commissioner (BIO0027) para 8.2

85 Q93; Q97

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.

55. **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.**

56. ***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.***

The facial recognition software used by police, and best practice standards, are both considered in detail in Chapter 4.

Proportionality

57. Ensuring that a biometric system is proportionate—that a balance is struck between society's need for the system and an individual's privacy rights—was identified as both a "critical issue" and a challenge that Government and industry needed to address.[86] When analysing proportionality, the European Commission's Data Protection Working Party identified a number of considerations, including whether the biometric system was "essential for satisfying that need rather than being the most convenient or cost effective", as well as whether "the resulting loss of privacy" was "proportional to any anticipated benefit". It added that if the benefit was "relatively minor", such as an "increase in convenience or a slight cost saving", then the "loss of privacy" was "not appropriate".[87]

58. Our witnesses broadly agreed with this assessment. Dr Richard Guest, University of Kent, stated that citizens should only be asked for their "high value identity biometrics as access keys to high value services".[88] Attention was drawn to the example of schools, where biometric applications have been employed as part of cashless catering systems and to borrow a library book. The Biometrics Institute recommended that schools should seek "less invasive […] solutions to those issues of library books, school lunches, attendance and bus tickets".[89] Emma Carr, Big Brother Watch, concurred, noting that schools often "could not give a direct reason as to why it was necessary for them to have [a biometric system]

86 Biometrics Institute Limited (BIO0003), para 4.3

87 Article 29 Data Protection Working Party (European Commission), *Opinion 3/2012 on developments in biometric technologies* (April 2012) p 8

88 Super-Identity Project, University of Kent (BIO0015) para 9

89 Biometrics Institute Limited (BIO0003), para 4.3

rather than another system".[90] The *Protection of Freedoms Act 2012* does include a requirement for schools to notify and obtain consent before processing a child's biometric information. It also states that schools "must ensure" that reasonable alternative arrangements are provided for pupils who do not use automated biometric recognition systems.[91] However, there is nothing in the Act which requires a school's use of biometric systems to be proportionate, nor is there any reference to proportionality in the accompanying guidance produced by the Department for Education.[92]

59. In its written evidence, the Government stated that biometric systems should demonstrate "a lawful purpose, a pressing need and proportionality".[93] When questioned how the Government ensured that these criteria were met, the Minister replied that it was "aided by the independent offices of the biometrics and information commissioners, the science advisers within the Home Office and a science council", adding that these "mechanisms" enabled things to be kept "under review".[94] However, Big Brother Watch, the Information Commissioner's Office (ICO) and Mr Rejman-Greene, Home Office, also pointed to the value of conducting a "privacy impact assessment" (PIA) at the outset of a project to determine "what privacy implications any scheme may have, as well as alternative, potentially less intrusive methods of achieving the same goal".[95]

60. We have previously recommended that PIAs "should be applied to all policies that collect, retain or process personal data".[96] This recommendation would cover biometrics; according to the ICO, biometric data is "a measure of a biological property" and given that "it can often be used to generate unique identifiers, it will often be classed as personal data".[97] Though the ICO updated its 'Code of Practice' for 'Conducting privacy impact assessments' in 2014, PIAs are not, at present, mandatory.[98] Instead, the Minister told us that "the operation of privacy impact assessments" was an area "currently under review".[99]

61. **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 revisit privacy impact assessments later in this chapter.

---

90 Q54 [Emma Carr]

91 Protection of Freedoms Act 2012, section 26 (7)

92 Department for Education, *Protection of Biometric Information of Children in Schools: Advice for proprietors, governing bodies, head teachers, principals and school staff* (December 2012)

93 The Government, (BIO0035) para 1.2

94 Q178 [the Minister]

95 Big Brother Watch (BIO0002); Information Commissioner's Office, (BIO0009) para 19; Q178 [Marek Rejman-Greene]

96 House of Commons Science and Technology Committee, Fourth Report of Session 2014–15, *Responsible Use of Data*, HC 245, para 29

97 Information Commissioner's Office (BIO0009) para 23

98 Information Commissioner's Office, *Conducting privacy impact assessments: code of practice*, (February 2014)

99 Q173

Public attitudes

62. We were repeatedly told that public attitudes towards biometric systems were largely negative. According to Sir John Adye, Identity Assurance Systems, public distrust of biometrics remained "prevalent in countries like the UK" while Professor van Zoonen, IMPRINTS, identified biometrics as "the most controversial and worrying of all means of authentication" among the British public.[100] This absence of public "faith and trust" was highlighted as a key challenge facing both the Government and industry, and a "primary inhibitor" to the development and implementation of biometric systems.[101] Pointing to events in the United States, for example, Northrop Grumman noted how the biometric industry had "been plagued with programmes that [had] proven the technology" but were discontinued "due to public outcries against misuse of its biometric images".[102]

63. Reasons given for the public's misgivings included concerns about intrusions into both their 'physical privacy' and their 'informational privacy'.[103] Drawing on the results of a survey conducted by her research group, Professor van Zoonen stated that public anxiety centred on at least three areas: first, "strong cultural associations" of biometrics with "state control and surveillance"; second, fears about losing control over personal data, with data subsequently being "lost or abused" and third, concerns about whether personal data was acquired and stored securely.[104]

64. For some witnesses, distrust of biometric systems also stemmed from the nature of the data collected and its intrinsic connection to the individual. Sir John Adye was of the view that biometric data was inherently more valuable than a password or PIN code because of its "absolute tie to the physical characteristics of people".[105] Professor Sue Black, University of Dundee, echoed Sir John's point, noting that "one's security, one's identity, is one of the things that people probably hold most dear to themselves, because it is the representation of self".[106]

65. Other witnesses suggested that an ongoing lack of communication about biometrics with the public was responsible for growing "misconceptions".[107] Dr Richard Guest, University of Kent, raised concerns that while the capabilities of biometric technologies had advanced, citizens had "not been brought along on the journey".[108] Lockstep Consulting, for example, pointed to the lack of discussion by "technologists and policy makers of the exceptions in this field, such as individuals who, for no fault of their own,

---

100 Sir John Adye (BIO0031) para 4.1; IMPRINTS (Identity Management – Public Responses to Identity Technologies and Services) (BIO0005) para 1

101 Q1 [Professor Black]; Q31 [Sir John Adye]

102 Northrop Grumman (BIO0030) para 4v

103 The Information Commissioner's Office defines physical privacy as the ability of a person to "maintain their own physical space or solitude" while informational privacy is understood to be the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. See Information Commissioner's Office, *Conducting privacy impact assessments code of practice* (February 2014), p 6

104 IMPRINTS (BIO0005) paras 3&4

105 Q36 [Sir John Adye]

106 Q7

107 International Biometrics & Identification Association (BIO0032) para IV

108 Super-Identity Project, University of Kent (BIO0015) para 6

cannot enrol in a given biometric" and thus whether biometrics may introduce, or exacerbate existing, inequalities.[109] Professor Juliet Lodge, Biometrics Institute, agreed that the Government had not been "engaging properly" with the public about biometrics since the scrapping of its ID card scheme in 2010. She added that, to date, the public had "not been terribly well informed about what a biometric is or how we can use biometrics".[110]

66. However, Dr Simon Rice, Information Commissioner's Office (ICO), told us that, while "public reaction to ID cards was not very positive," he did not think that the public had "shied away from biometrics or somehow been turned off".[111] Instead, witnesses highlighted that there had been "a huge expansion in more passive forms of take-up" of biometrics and a corresponding absence of "open dialogue and transparency when communicating with the public about biometric technology".[112] Mr Alastair MacGregor, Biometrics Commissioner, indicated that, in his view, "more people" were "concerned about Government use" of biometrics than they were about commercial uses.[113]

67. To establish and maintain public confidence in biometric systems, a number of witnesses stated that their development, operation and management should be transparent and proportionate.[114] Dr Rice agreed, adding that the ICO had a role to play in educating "policy makers and Government, as well as members of the public" through its "guidance, blogs and websites".[115] When questioned about the Government's efforts to maintain public confidence in biometrics, the Minister replied that "the more discussion and the more awareness there is, the better", adding that the Government were "looking at ways to do that". The Minister, however, stressed that Government was only part of the solution and identified Parliament, as well as the media and civil society, as needing "to engage and have a far wider debate about the issues".[116]

68. **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.**

69. ***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.***

---

109 Lockstep Consulting (BIO0004) section 2; see also Dr Edgar Whitley (BIO0025) para 15

110 Q10, Q1 [Professor Lodge]

111 Q112

112 Q1 [Professor Amoore]; Q1 [Professor Lodge]; Pippa King (BIO0028) para 5

113 Q113

114 Super-Identity Project, University of Kent (BIO0015) para 9; Lockstep Consulting (BIO0004) section 5; Biometrics Institute Limited (BIO0003)

115 Q125

116 Q181

Data storage and system security

70. Recent "breaches of security", including the "Snowden incident", have made the public increasingly sceptical about who has access to their biometric data and whether it is stored securely.[117] Research Councils UK was clear that establishing public confidence in "the storage and access arrangements around their biometric data" was key to ensuring greater public acceptance of biometrics.[118]

71. Unlike a password or PIN code, an individual's biometric characteristic cannot easily be revoked or reissued if it is compromised. Giving evidence in 2006 to our predecessors, Professor Martyn Thomas stated that the theft of an individual's biometrics created a "security nightmare" whereby somebody's biometrics were "no longer available to them to authenticate themselves for the rest of their lives".[119] It is, therefore, paramount that templates of biometric traits are stored securely. Erik Bowman, Northrop Grumman, explained that secure storage was possible:

> When the data are […] not being used or in the process of being authenticated, they can be encrypted. The template […] is a small representation of the image itself. It is fairly hard to reconstruct into the actual image. The images are kept separate along with the security scheme and can be encrypted.[120]

72. However, there was a divergence of opinion between Government and industry as to whether security was adequately integrated into biometric systems. According to Northrop Grumman, securing biometric systems was "all too often […] an afterthought" and failed to be designed and planned from the outset "due to a lack of clear requirements or cost constraints".[121] Erik Bowman, Northrop Grumman, commented that "agencies will not think all the way through a complete requirement that states you must protect the data in such a way" and will instead rely on "the systems integrator [to] figure out how to do that".[122] The Minister disagreed with this assessment, countering that it was, in fact, the "private sector that might bolt on security at the end of the process" adding that the Government "bolts on security right at the beginning of the process". He continued:

> security is probably far more hard-wired into every process of what Government does, particularly because it is dealing with national security issues, and I think people could have more confidence in that particular area of security of data. The private sector probably has some catching up to do.[123]

73. Drawing attention to the specific example of DNA and fingerprints, Mr Alastair MacGregor, Biometrics Commissioner, concurred that there was a "difference between

---

117 Super-Identity Project, University of Kent (BIO0015) para 7

118 Research Councils UK (BIO0033) para 9

119 House of Commons Science and Technology Committee, Sixth Report of Session 2005–06, *Identity Card Technologies: Scientific Advice, Risk and Evidence*, HC 1032, para 131

120 Q41 [Erik Bowman]; see also National Security Alliance (BIO0007)

121 Northrop Grumman (BIO0030) para 5

122 Q39

123 Q182

commercial organisations and what actually happens in Government" and pointed to the "huge attention" paid to "the security of that information" by Government, including restricting access to databases, like the DNA database.[124]

74. Dr Simon Rice, Information Commissioner's Office (ICO), clarified that the "standard in the Data Protection Act is that appropriate security measures must be taken", adding the "ideal" was that:

> if that biometric data is breached in some way, it should not matter to the individual. You should be able to re-enrol a person with a new biometric, and that template should not be able to be used in some other kind of system to gain access.[125]

When pressed to outline what steps the ICO takes to ensure the standard set out in the Data Protection Act is adhered to, Dr Rice stated that "it would be up to the institutions rolling out the biometric system to make sure they are storing it in that way", adding that it was not "in the legislation that the data controller must write to us for approval before they roll out a particular system".[126] The Data Protection Act is examined in further detail in Chapter 4.

75. **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.**

76. ***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.***

77. **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.**

78. ***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.***

---

124 Q116 [Alastair MacGregor]

125 Q114

126 Q115 & Q116 [Dr Rice]

Function creep

79. Templates of biometric traits may be stored on a centralised database or on portable media, such as a smart card. Large, centralised databases are essential if biometrics are to be used for the purposes of identification (as opposed to verification) yet, as the Irish Council for Bioethics reports, they are often criticised because of the potential for "function creep".[127] The European Commission describes function creep as "technology and processes introduced for one purpose [and] extended to other purposes which were not discussed or agreed upon at their implementation".[128]

80. The Biometrics Institute stated that one of the "major threats to privacy" is the "potential of re-purposing and function-creep and, especially, data linkage, both by governments and private companies".[129] The European Commission Data Protection Working Party expressed a similar view when reviewing developments in biometrics. In 2012 the Working Party voiced concerns that "the higher technical potential of new computer systems" raised the "risk of data being used against their original purpose". This included the "identification of individuals without their knowledge" and the linking of biometric data with information from other databases in ways that facilitated profiling; both of which were emerging trends identified in Chapter 2.[130]

81. Professor Louise Amoore, Durham University, described how these trends had changed the *status quo*, particularly around consent. Under the Data Protection Act, a prerequisite to using biometric data (or any 'personal data') is the requirement that the individual "is fully informed about the purposes of the processing".[131] Professor Amoore stated that less than "five years ago legislators could safely assume that a citizen would know, and be able to meaningfully consent to, the point of biometric data collection and processing".[132] Now, according to Professor Amoore, the situation had shifted since biometric data could be "analysed in conjunction with a vast array of other available 'big data', not all of which belongs to known or identifiable individuals".[133] She cautioned that the "linkage to the biometric makes all sorts of things possible", adding that this required a rethinking of "consent, and to what extent we can now reasonably say that someone has given their consent".[134]

82. As Professors Black and NicDaeid explained, a further part of the "difficulty arises from knowing the future importance of the data we collect today". For example a:

> volunteer in a research project may be willing today to allow a photograph of the back of their hand to be taken, with developments in technology and with

---

127 Irish Council for Bioethics, *Biometrics: Enhancing Security or Invading Privacy?* (October 2009), p 6

128 European Commission Directorate-General Joint Research Centre, *Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)*, Executive Summary, 2005, p 7

129 Biometrics Institute Limited (BIO0003) para 1

130 Article 29 Data Protection Working Party (European Commission), Opinion 3/2012 on developments in biometric technologies, (April 2012), p 17

131 Information Commissioner's Office (BIO0009) para 24

132 Professor Amoore (BIO0006) para 1.1

133 Professor Amoore (BIO0006) para 4.1

134 Q17

> previously unknown linkage capabilities, there may be very private information stored there which can now be released and utilised in ways never intended or imagined.[135]

83. In addition to concerns about consent, both the Information Commissioner's Office (ICO) and Professor Amoore warned that combining big data with biometric data could reduce the degree of human input into decision making and potentially give rise to:

> powerful systems making decisions about individuals based solely on their facial markers, genetic data or other biometric detail in a manner which is incompatible with the original purpose.[136]

For Professor Amoore, this represented an area where there needed "to be greater public debate about the relationship between machine recognition, algorithmic decisions and the intervention of a human person".[137] When questioned if "at least some human involvement" was being "built in" to the Government's Identity Assurance Programme if a biometric was required, Mr Rejman-Greene, Home Office, replied that he did not know "because the plans for the much longer term of the identity assurance scheme [were] still being worked on".[138] He did, however, note that if there was "an automated decision that affected the individual, it might well be counter to one of the Data Protection Act requirements, […] that you should not take that decision in a purely automated way".[139]

84. Processing personal data (including biometric data) in ways that are incompatible with the purposes specified when it was collected breaches the provisions of the Data Protection Act. The Committee previously stressed in its report, the *Responsible Use of Data*, that we consider it vital that both the public and private sectors effectively communicate how they intend to use the data of individuals. **In our opinion, under no circumstances should the state roll out a biometric system that does not provide any scope for human intervention.**

85. ***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.***

Unsupervised systems

86. Additional concerns about system security were raised in the specific context of mobile, 'unsupervised' biometric systems.[140] Sir John Adye, Identity Assurance Systems, drew a

---

135 Professor Black and Professor NicDaeid (BIO0017) para 12

136 Information Commissioner's Office (BIO0009) para 21; see also Professor Amoore (BIO0006) para 2.2. It should be noted that a specific example of this currently occurring was not provided.

137 Q5

138 Q169

139 Q168

140 The UK Cards Association (BIO0011) para 8; Identity Assurance Systems (BIO0031) para 4.1; Professor Nixon and Professor Kittler (BIO0010) para 7.1

comparison with using an ATM. He noted that while the ATM would "be supervised by the bank in some way", there was "no physical supervision of the system" if you were instead using "your smartphone, or even your PC at home".[141] According to Sir John, the development of biometric systems that rested "outside the control of the relying party" necessitated "the right kind of security and cryptographic techniques designed into the systems which are on the phones themselves". Sir John, however, was not convinced that this was currently occurring and questioned:

> what happens to my personal data when I use them on a smartphone for proving my identity. Is Google going to use that data also to target advertising at me? Is some other commercial company or maybe some hostile foreign Government going to use it to target me in some other way? I don't know. We need to find ways of getting that kind of system properly organised.[142]

87. One way of getting "properly organised", suggested by Sir John, would be through the development of international standards. According to Sir John and Dr Peter Waggett, BSI, standards for the use of biometrics on "mobile phones and any devices outside the control of the relying party" were being developed, though both witnesses acknowledged that the process took time and was not easy since it required "acceptance and buy-in from all of the different nations that are represented at the ISO level".[143] The role of both national and international standards, including adherence to them, is considered in further detail in Chapter 4.

141 Q41 [Sir John Adye]

142 Q44

143 Q45 & Q56. ISO stands for the 'International Organization for Standardization'

4 Legislation and standards

88. The evidence we received on function creep, the re-purposing of data and unsupervised biometric systems raised broader questions about whether current legislation governing the ownership of biometric data, and who can collect, store and use it, remains effective. This chapter addresses these questions and pays particular attention to the use of facial recognition software by the police on photographs that were taken in custody. This matter was highlighted to us by both the Biometrics Commissioner and the Information Commissioner's Office.

Fit for purpose?

89. Witnesses disagreed about the effectiveness of the legislation governing the use of biometric data, including the Data Protection Act (DPA). As the Information Commissioner's Office (ICO) explained, the "DPA governs the use of 'personal data'", namely "data which relates to a living individual who can be identified from that data, either directly or indirectly". Since biometric data is "a measure of a biological property" that "can often be used to generate unique identifiers" the ICO noted that "it will often be classed as personal data" with its use "governed by the Data Protection Act".[144]

90. Dr Richard Guest, University of Kent, stated that, in light of many of the challenges posed by developments in biometrics, "current legislation" was "not fit for purpose".[145] Some witnesses suggested that this could be resolved through revisions to the DPA. For example, Professor Louise Amoore, Durham University, commented that a "revised Data Protection Act capable of keeping pace with the capacities of contemporary data analytics" was required. She proposed treating all biometric data as "sensitive personal data" since "it can reveal things relating to race, ethnicity, sexual orientation" as a change that she wished to see on the grounds that, "different rules apply to processing, storage and so on".[146]

91. Others, however, felt that it was time to start again. Professor Sue Black, University of Dundee, did not think that the DPA could be changed or amended in order to cope with advances in biometrics. Instead she stated that a "whole new outlook" was required since biometrics was "running ahead of our capability to manage it".[147] 3M went further and questioned whether legislation could ever keep pace with advances in technology.[148] It anticipated that as biometric technologies "diffuse down" to smaller, non-government entities, the Government's influence in this sphere would "disappear" to the extent that it would "prove almost impossible to enforce legislation introduced to deal with the situation".[149]

144 Information Commissioner's Office (BIO0009) paras 23 & 4

145 Super-Identity Project, University of Kent (BIO0015) para 15

146 Q16-Q17

147 Q14

148 3M (BIO0018) para 5.2; see also Church and Society Council of the Church of Scotland (BIO0016)

149 3M (BIO0018) para 5.5

92. The Government disagreed, arguing that since the DPA was "a principle-based framework of statutory requirements" it should "remain relevant and applicable in the face of rapid technological advance".[150] The ICO concurred stating that the DPA was "technology-neutral and adequately flexible to ensure that biometric data can be processed in compliance with the essential legal obligations and safeguards".[151] While recognising Professor Amoore's concern that biometric data might reveal so-called "sensitive personal data", such as an "individual's race, ethnic origin or health condition", the ICO considered it to be "debatable […] whether information with the mere potential to reveal somebody's race, for example, is in itself sensitive personal data".[152] The Minister, therefore, did not believe that a "general review" of the DPA was currently necessary, though he remained "open to it". [153]

93. **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.***

Facial recognition and the retention of photographs by the police

94. Facial recognition systems can be used for verification (confirming a person is who they claim to be) or identification purposes (discovering who an otherwise unknown person is). In theory, the use of facial recognition for identification could assist the police in their investigations. However, there was a persistent lack of clarity about whether facial recognition was currently used by the police in this mode and particularly if it was being applied to photographs taken in custody.

95. The Association of Chief Police Officers (ACPO) described facial recognition as "a less well developed area of biometrics", though it noted that police have taken photographs of suspects during the custody process "for many years". ACPO stated that these images had recently "been held digitally" and were "capable of being used within the emerging science of facial recognition".[154] However, ACPO did not state in its written evidence if this "capability" was operational. Speaking to the Committee, Chief Constable Chris Sims, ACPO, clarified that he was:

> not aware of forces using facial image software at the moment. There are certainly lots of discussions and there has been some piloting, but from my perspective the technology is not yet at the maturity where it could be deployed, so issues as to how it is used sit as a future debate rather than a current one.[155]

---

150 The Government (BIO0035) para 2.4

151 Information Commissioner's Office (BIO0009) para 23

152 Information Commissioner's Office (BIO0009) para 27

153 Q172

154 Association of Chief Police Officers (BIO0036) para 2.3

155 Q90

96. Mr Alastair MacGregor, Biometrics Commissioner, told us that he was "slightly surprised by some of what [Chief Constable Sims] has said": it was his "understanding that 12 million-plus custody photographs" had been "uploaded to the PND [Police National Database] and that facial recognition software [was] being applied to them".[156] When asked to respond to Mr MacGregor's comments, Chief Constable Sims replied that he too was "surprised" by what he had heard, adding that he "certainly did not think it was an operational reality" before stressing that facial recognition was not his "area of specialty".[157]

97. Compounding this confusion was an apparent 'gap' in the legislation regarding the retention of images, and the use of facial recognition software, by the police. The Information Commissioner's Office (ICO) stated that the *Protection of Freedoms Act 2012* "does not cover photographs" and that there was "no specific legislation covering their retention or their use".[158] The Biometrics Commissioner echoed the ICO's point and questioned how "appropriate" it was for the police to put "a searchable database of custody photographs" into "operational use" in the absence of any "proper and effective regulatory regime […] beyond that provided for in the Data Protection Act 1998".[159] He added that the custody photographs loaded on to the PND included "those of hundreds of thousands of individuals who have never been charged with, let alone convicted of, an offence".[160]

98. The deficiencies of current legislation and policy relating to the retention of images by the police were clearly highlighted to the Government in 2012 in *R (RMC and FJ) v MPS* (Metropolitan Police Service). The two claimants, RMC and FJ, were arrested but subsequently not convicted of an offence and sought the destruction of their custody photographs, fingerprints and DNA samples. The Court ruled that the "defendant's existing policy concerning the retention of custody photographs (namely, to apply the MoPI Code of Practice and the MoPI guidance)" was "unlawful".[161] Rather than require "the immediate destruction of the claimants' photographs", the Court allowed "the defendant a reasonable further period within which to revise the existing policy" while clarifying that a "reasonable further period" was to be "measured in months, not years".[162] Over two and half years later, no revised policy has been published. However, when giving evidence, the Minister announced a new "a policy review of the statutory basis for the retention of facial images" on the grounds that "the chief constable, the police and the Home Office" all accepted that "the current governance of the data being held is not sufficiently covered" by existing policy and legislation.[163]

99. We are concerned that it has taken over two and half years for the Government to respond to the High Court ruling that the existing policy concerning the retention of

156 Q91

157 Q92 [Chief Constable Sims]

158 Information Commissioner's Office (BIO0009) para 32

159 Biometrics Commissioner (BIO0027) para 5 & 8.2

160 Biometrics Commissioner (BIO0027) para 9

161 MoPI stands for the Management of Police Information. The Code of Practice on the Management of Police Information was issued by the Secretary of State in July 2005 under the powers of s.39A of the Police Act 1996. By s.39A(7) of that Act, chief officers are required to have regard to the Code in discharging any function to which the Code relates.

162 R (RMC and FJ) v Metropolitan Police Service [2012] EWHC 1681

163 Q152; Q160; see also Q156

custody photographs was "unlawful". Furthermore, we were dismayed to learn that, in the known absence of an appropriate governance framework, the police have persisted in uploading custody photographs to the Police National Database, to which, subsequently, facial recognition software has been applied.

100. We fully appreciate the positive impact that facial recognition software could have on the detection and prevention of crime. However, it is troubling that the governance arrangements were not fully considered and implemented prior to the software being 'switched on'. This appears to be a further example of a lack of oversight by the Government where biometrics is concerned; a situation that could have been avoided had a comprehensive biometrics strategy been developed and published. While we welcome the Minister's announcement of a review of the statutory basis for the retention of facial images, we are concerned that similar issues could arise in the years ahead relating to voice and gait recognition, and possibly other biometric traits.

101. ***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 Biometrics Commissioner

102. The role of Biometrics Commissioner was created by *the Protection of Freedoms Act 2012*. That Act established a new regime to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints. Mr MacGregor was clear that his statutory responsibilities as Biometrics Commissioner related "only to DNA and fingerprints" though he acknowledged that the term 'biometric data' was "usually thought to include, among other things, facial images and voice patterns". He also noted that "no other commissioner or regulator" appeared to have a remit which specifically covered the use of facial and voice recognition by the police.[164]

103. We put it to Mr MacGregor that it appeared "a bit odd that the Office of the Biometrics Commissioner [did] not cover all potential biometrics".[165] While initially stressing that he was "keen not to empire-build"[166] Mr MacGregor later stated in correspondence with the Committee that:

---

164 Biometrics Commissioner (BIO0027) para 6

165 Q95

166 Q97

> strong arguments could be advanced in favour of the proposition that the jurisdiction of the Biometrics Commissioner should be extended so as to cover the police use of custody photographs (and possibly other biometric material) and that that would be a much more sensible arrangement than the appointment of some new or separate Commissioner to provide independent oversight.[167]

When asked if the Government had considered extending the responsibilities of the Biometrics Commissioner, the Minister replied that he was "going to look at this", adding that he had "heard what the biometrics commissioner said, and we have launched the review. I can say to the Committee that the role of the biometrics commissioner in response to facial images will be a key aspect of the review".[168] In subsequent correspondence with the Committee, the Minister stated that, in the longer-term, "the future provision of biometrics capability for at least the police, immigration, borders and security needs to be more coherent and integrated". He continued that the "governance and oversight of any such integration […] will be given careful consideration, particularly in relation to the role of the Biometrics Commissioner".[169]

104. **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.**

105. ***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.***

National and international standards

106. We received several submissions, particularly from industry, which argued that legislation and regulation could only go so far in ensuring that biometric systems were operated in ways that were "reliable, accurate and secure", particularly when their development and use might "transcend territorial jurisdiction".[170] It was therefore suggested that 'standards' were also necessary. The British Standards Institute (BSI) describes a standard as "a document defining best practice, established by consensus" that is "voluntary and separate from legal and regulatory systems".[171] Biometrics standards currently exist at the British, European and International level and address topics such as:

---

167 Biometrics Commissioner (BIO0037)

168 Q159

169 The Government (BIO0038)

170 3M (BIO0018) para 5.8; British Standards Institution (BIO0020) para 5.2

171 British Standards Institution (BIO0020) para 1.4 & 1.5

- modes of biometric system including fingerprints, facial recognition, voice, finger or palm
- vein and iris recognition
- interoperability and communication of biometric data
- methods for protecting against fraud and misrepresentation
- usability and accessibility of biometric systems
- society and cross-jurisdictional issues
- privacy, security and consumer protection.[172]

107. Standards can fulfil a number of complementary functions. The Government, for example, anticipated that:

> open standards for data formatting, storage, communication and access [would] form a critical element of the infrastructure for biometric information, with benefits for interoperability across Government and internationally allowing ease of access whilst maintaining security and data assurance, and increasing the efficiency of existing systems.[173]

According to Mr Marek Rejman-Greene, Home Office, having open standards also:

> enables all the details of how those systems operate to be out in the open. It allows for innovation, so you know the constraints within which to innovate; and it means, therefore, that UK companies can bid for parts of the systems that relate to the biometric component.[174]

108. Some concern was voiced about how difficult it would be to persuade commercial companies to adhere to open standards. Pointing to "the use of mobile platform and cloud-based systems" for biometrics, Dr Richard Guest, University of Kent, reported that "large technology manufacturers" were adopting "proprietary standards thereby preventing third-party use of data" which could limit new entrants to the market.[175] However, in the case of government biometric systems, Sir John Adye, Identity Assurance Systems, predicted that "with major international industries competing for government contracts", it would "be possible to encourage compliance with best practice".[176] Speaking as a supplier of biometric technologies, Ben Fairhead, 3M, agreed with Sir John's assessment. He stressed that 3M's systems had:

> to be [standards compliant] because Governments demand that the sorts of systems we supply are standards compliant. The systems we supply need to talk to other systems within a country, and sometimes between countries, so

---

172 British Standards Institution (BIO0020) para 4.2.

173 The Government (BIO0035) para 5.3

174 Q179

175 Super-Identity Project, University of Kent (BIO0015) para 12

176 Identity Assurance Systems (BIO0031) para 4.1

> they have to comply with certain data standards otherwise they could not exchange information.[177]

109. Mr Rejman-Greene confirmed that, "in terms of government systems, the first direction is almost always to try to look at open standards" but noted that there were "limitations" regarding what the Government could do "in terms of trying to impose standards on the commercial sector".[178] The Information Commissioner's Office also questioned whether system interoperability should always be encouraged, noting that, in some systems, a lack of interoperability acted as "an important privacy protecting mechanism" through ensuring that an individual's biometric was "effectively meaningless outside the system for which [it was] collected".[179] A similar point was made by the Irish Council for Bioethics in its 2009 report on biometrics. It stated that enabling greater information sharing through enhancing interoperability between biometric systems could accentuate privacy concerns on the grounds that:

> the more agencies and organisations that have access to an individual's biometric information, the greater the likelihood that this information will be used for another purpose beyond that for which it was originally collected.[180]

110. **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.**

111. ***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.***

---

177 Q50

178 Q179

179 Information Commissioner's Office (BIO0009) para 20

180 Irish Council for Bioethics, *Biometrics: Enhancing Security or Invading Privacy?* (October 2009), p 75

Conclusions and recommendations

Scientific advice on biometrics

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. (Paragraph 28)

2. 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. (Paragraph 29)

3. 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. (Paragraph 35)

4. 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. (Paragraph 36)

A strategy for biometrics

5. 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. (Paragraph 41)

6. 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. (Paragraph 42)

7. We expect a comprehensive, cross-departmental forensics and biometrics strategy to be published by the Government no later than December 2015. (Paragraph 43)

Testing biometric systems

8. 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. (Paragraph 54)

9. 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. (Paragraph 55)

10. 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. (Paragraph 56)

Public attitudes

11. 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. (Paragraph 61)

12. 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. (Paragraph 68)

13. 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. (Paragraph 69)

Data storage and system security

14. 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. (Paragraph 75)

15. 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. (Paragraph 76)

16. 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. (Paragraph 77)

17. 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. (Paragraph 78)

18. In our opinion, under no circumstances should the state roll out a biometric system that does not provide any scope for human intervention. (Paragraph 84)

19. 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. (Paragraph 85)

Legislation and standards

20. 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. (Paragraph 93)

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

- 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;
- 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;

- 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. (Paragraph 101)

The role of the Biometrics Commissioner

22. 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. (Paragraph 104)

23. 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. (Paragraph 105)

Quality standards

24. 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. (Paragraph 110)

25. 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. (Paragraph 111)

Formal Minutes

Wednesday 25 February 2015

Members present:

Andrew Miller, in the Chair

Dan Byles	Stephen Mosley
Jim Dowd	Pamela Nash
Stephen Metcalfe	Graham Stringer

Draft Report (*Current and future uses of biometric data and technologies*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 111 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Sixth 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 Monday 2 March at 4.00 pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the Committee's inquiry page at www.parliament.uk/science.

Wednesday 26 November 2014	*Question number*
Professor Juliet Lodge, Emeritus Professor of European Studies, University of Leeds, and member of the Privacy and Policy Expert Group at the Biometrics Institute, **Professor Louise Amoore**, Professor of Political Geography, Durham University, and **Professor Sue Black**, Director, Centre for Anatomy and Human Identification, University of Dundee	Q1–27
Sir John Adye, Chairman, Identity Assurance Systems, **Ben Fairhead**, Biometric Systems Engineer, 3M, and **Erik Bowman**, Systems Engineer, Northrop Grumman	Q28–51
Andrew Tyrer, Head of Enabling Technology, Innovate UK, **Emma Carr**, Director, Big Brother Watch, and **Dr Peter Waggett**, Chairman, British Standards Institution technical committee IST/44	Q52–81

Wednesday 10 December 2014	
Dr Simon Rice, Group Manager (Technology), Information Commissioner's Office, **Alastair R MacGregor QC**, Biometrics Commissioner, Office of the Biometrics Commissioner, and **Chief Constable Chris Sims**, National Policing Lead for Forensic Science, Association of Chief Police Officers	Q82–139
Lord Bates, Parliamentary Under-Secretary of State for Criminal Information, Home Office, and **Marek Rejman-Greene**, Senior Biometrics Adviser, Home Office	Q140–185

Published written evidence

The following written evidence was received and can be viewed on the Committee's inquiry web page at www.parliament.uk/science. BIO numbers are generated by the evidence processing system and so may not be complete.

1	Julian Ashbourn	BIO0001
2	Big Brother Watch	BIO0002
3	Biometrics Institute Limited	BIO0003
4	Lockstep Consulting	BIO0004
5	IMPRINTS	BIO0005
6	Professor Louise Amoore, Durham University	BIO0006
7	Natural Security Alliance	BIO0007
8	Unilink Software	BIO0008
9	Information Commissioner's Office	BIO0009
10	Professor Mark S Nixon, University of Southampton and Professor Josef Kittler, University of Surrey	BIO0010
11	The UK Cards Association	BIO0011
12	Dr Roger Morgan	BIO0012
13	James Moyes	BIO0014
14	SuperIdentity Project, University of Kent	BIO0015
15	Church and Society Council of the Church of Scotland	BIO0016
16	Professor Sue Black and Professor Niamh NicDaeid, University of Dundee	BIO0017
17	3M UK	BIO0018
18	Forensic Science Special Interest Group	BIO0019
19	British Standards Institution	BIO0020
20	Identity Policy Research, London School of Economics and Political Science	BIO0025
21	Dr Peter Hawkes	BIO0026
22	Office of the Biometrics Commissioner	BIO0027
23	Pippa King	BIO0028
24	Innovate UK	BIO0029
25	Northrop Grumman	BIO0030
26	Sir John Adye, Chairman, Identity Assurance Systems Ltd	BIO0031
27	International Biometrics & Identification Association	BIO0032
28	Research Councils UK	BIO0033
29	Sir John Pethica	BIO0034
30	Home Office	BIO0035
31	Association of Chief Police Officers	BIO0036
32	Office of the Biometrics Commissioner (supplementary to BIO0027)	BIO0037
33	Home Office (supplementary to BIO0035)	BIO0038

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the Committee's website at www.parliament.uk/science.

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2014–15

First Special Report	Communicating climate science: Government Response to the Committee's Eighth Report of Session 2013–14	HC 376
First Report	Ensuring access to working antimicrobials	HC 509 (Cm 8919)
Second Special Report	Government horizon scanning: Government Response to the Committee's Ninth Report of Session 2013–14	HC 592
Second Report	After the storm? UK blood safety and the risk of variant Creutzfeldt-Jakob Disease	HC 327 (Cm 8940)
Third Special Report	Ensuring access to working antimicrobials: Research Councils UK Response to the Committee's First Report of Session 2014–15	HC 643
Third Report	National Health Screening	HC 244 (Cm 8999)
Fourth Report	Responsible Use of Data	HC 245
Fifth Report	Advanced genetic techniques for crop improvement: regulation, risk and precaution	HC 328

Session 2013–14

First Special Report	Educating tomorrow's engineers: the impact of Government reforms on 14–19 education: Government Response to the Committee's Seventh Report of Session 2012–13	HC 102
First Report	Water quality: priority substances	HC 272–I (HC 648)
Second Special Report	Marine science: Government Response to the Committee's Ninth Report of Session 2012–13	HC 443
Third Special Report	Bridging the valley of death: improving the commercialisation of research: Government response to the Committee's Eighth Report of Session 2012–13	HC 559
Second Report	Forensic science	HC 610 (Cm 8750)
Fourth Special Report	Water quality: priority substances: Government response to the Committee's First Report of Session 2013–14	HC 648
Third Report	Clinical trials	HC 104 (Cm 8743)
Fifth Special Report	Clinical trials: Health Research Authority Response to the Committee's Third Report of Session 2013–14	HC 753
Fourth Report	Work of the European and UK Space Agencies	HC 253 (HC 1112)
Fifth Report	Pre-appointment hearing with the Government's preferred candidate for Chair of the Natural	HC 702

	Environment Research Council (NERC)	
Sixth Special Report	Forensic science: Research Councils UK Response to the Committee's Second Report of Session 2013–14	HC 843
Seventh Special Report	Clinical trials: Medical Research Council Response to the Committee's Third Report of Session 2013–14	HC 874
Sixth Report	Women in scientific careers	HC 701 (HC 1268)
Seventh Report	Pre-appointment hearing with the Government's preferred candidate for Chair of the Arts and Humanities Research Council (AHRC)	HC 989
Eighth Special Report	Work of the European and UK Space Agencies: Government Response to the Committee's Fourth Report of Session 2013–14	HC 1112
Eighth Report	Communicating climate science	HC 254 (HC 376, Session 2014–15)
Ninth Report	Government horizon scanning	HC 703 (HC 592, Session 2014–15)
Ninth Special Report	Women in scientific careers: Government Response to the Committee's Sixth Report of Session 2013–14	HC 1268

Session 2012–13

First Special Report	Science in the Met Office: Government Response to the Committee's Thirteenth Report of Session 2010–12	HC 162
First Report	Devil's bargain? Energy risks and the public	HC 428 (HC 677)
Second Report	Pre-appointment hearing with the Government's preferred candidate for Chair of the Medical Research Council	HC 510–I
Second Special Report	Engineering in government: follow-up to the 2009 report on Engineering: turning ideas into reality: Government Response to the Committee's Fifteenth Report of Session 2010–12	HC 511
Third Report	The Census and social science	HC 322 (HC 1053)
Fourth Report	Building scientific capacity for development	HC 377 (HC 907)
Fifth Report	Regulation of medical implants in the EU and UK	HC 163 (Cm 8496)
Sixth Report	Proposed merger of British Antarctic Survey and National Oceanography Centre	HC 699 (HC 906)
Third Special Report	Devil's bargain? Energy risks and the public: Government Response to the Committee's First Report of Session 2012–13	HC 677
Fourth Special Report	Building scientific capacity for development: Government and UK Collaborative on Development Sciences Response to the Committee's Fourth Report of Session 2012–13	HC 907
Fifth Special Report	Proposed merger of British Antarctic Survey and National Oceanography Centre: Natural Environment Research Council Response to the Committee's Sixth Report of Session 2012–13	HC 906
Seventh Report	Educating tomorrow's engineers: the impact of Government reforms on 14–19 education	HC 665 (HC 102, Session 2013–14)

Eighth Report	Bridging the valley of death: improving the commercialisation of research	HC 348 (HC 559, Session 2013–14)
Sixth Special Report	The Census and social science: Government and Economic and Social Research Council (ESRC) Responses to the Committee's Third Report of Session 2012–13	HC 1053
Ninth Report	Marine science	HC 727

Session 2010–12

First Special Report	The Legacy Report: Government Response to the Committee's Ninth Report of Session 2009–10	HC 370
First Report	The Reviews into the University of East Anglia's Climatic Research Unit's E-mails	HC 444 (HC 496)
Second Report	Technology and Innovation Centres	HC 618 (HC 1041)
Third Report	Scientific advice and evidence in emergencies	HC 498 (HC 1042 and HC 1139)
Second Special Report	The Reviews into the University of East Anglia's Climatic Research Unit's E-mails: Government Response to the Committee's First Report of Session 2010–12	HC 496
Fourth Report	Astronomy and Particle Physics	HC 806 (HC 1425)
Fifth Report	Strategically important metals	HC 726 (HC 1479)
Third Special Report	Technology and Innovation Centres: Government Response to the Committee's Second Report of Session 2010–12	HC 1041
Fourth Special Report	Scientific advice and evidence in emergencies: Government Response to the Committee's Third Report of Session 2010–12	HC 1042
Sixth Report	UK Centre for Medical Research and Innovation (UKCMRI)	HC 727 (HC 1475)
Fifth Special Report	Bioengineering: Government Response to the Committee's Seventh Report of 2009–10	HC 1138
Sixth Special Report	Scientific advice and evidence in emergencies: Supplementary Government Response to the Committee's Third Report of Session 2010–12	HC 1139
Seventh Report	The Forensic Science Service	HC 855 (Cm 8215)
Seventh Special Report	Astronomy and Particle Physics: Government and Science and Technology Facilities Council Response to the Committee's Fourth Report of Session 2010–12	HC 1425
Eighth Report	Peer review in scientific publications	HC 856 (HC 1535)
Eighth Special Report	UK Centre for Medical Research and Innovation (UKCMRI): Government Response to the Committee's Sixth Report of session 2010–12	HC 1475
Ninth Report	Practical experiments in school science lessons and science field trips	HC 1060–I (HC 1655)
Ninth Special Report	Strategically important metals: Government Response to the Committee's Fifth Report of Session 2010–12	HC 1479
Tenth Special Report	Peer review in scientific publications: Government and Research Councils UK Responses to the	HC 1535

	Committee's Eighth Report of Session 2010–12	
Tenth Report	Pre-appointment hearing with the Government's preferred candidate for Chair of the Technology Strategy Board	HC 1539–I
Eleventh Special Report	Practical experiments in school science lessons and science field trips: Government and Ofqual Responses to the Committee's Ninth Report of Session 2010–12	HC 1655
Eleventh Report	Alcohol guidelines	HC 1536 (Cm 8329)
Twelfth Report	Malware and cyber crime	HC 1537 (Cm 8328)
Thirteenth Report	Science in the Met Office	HC 1538
Fourteenth Report	Pre-appointment hearing with the Government's preferred candidate for Chair of the Engineering and Physical Sciences Research Council	HC 1871–I
Fifteenth Report	Engineering in government: follow-up to the 2009 report on Engineering: turning ideas into reality	HC 1667 (HC 511, Session 2012–13)