

**IN THE MATTER OF AN APPEAL TO THE FIRST-TIER TRIBUNAL
(INFORMATION RIGHTS) UNDER SECTION 57 OF THE FREEDOM OF
INFORMATION ACT 2000**

EA/2011/0081

BETWEEN:-

DAVID MOSS

Appellant

-and-

THE INFORMATION COMMISSIONER

First Respondent

-and-

THE HOME OFFICE

Second Respondent

**RESPONSE BY THE APPELLANT
20 SEPTEMBER 2011**

References to pages, n, in the Open Bundle, second index received on 28 July 2011, are in the form OB2:n

References to paragraphs, n, on pages, m, in the Open Bundle, second index received on 28 July 2011, are in the form OB2:m:n

References to paragraphs, n, in the Commissioner’s 24 August 2011 Response are in the form ICOResp2:n

References to paragraphs, n, in the Second Respondent’s 24 August 2011 Response are in the form HOResp2:n

1 We know that the Home Office and other government departments have invested hundreds of millions of pounds of public money in projects which depend wholly or partially for their success on either facial recognition or flat print fingerprinting, or both, working properly. And we know that the Home Office and other government departments plan to invest hundreds of millions of public pounds more, also predicated on the reliability of just these two biometrics **T1**

1.1 The biometrics-dependent projects referred to here include the National Identity Scheme (NIS), the UK Border Agency’s (UKBA) eBorders initiative, UKBA’s biometric residence permits for non-EEA residents, the Identity & Passport Service’s (IPS) ePassports, the Cabinet Office’s/DWP’s Transformational Government initiative (subsequently the Cabinet Office’s G-Digital project, part of the G-Cloud initiative, currently known as “digital by default”, which includes IdA, the identity assurance

project, previously known as “digital delivery identity assurance”), UKBA’s introduction of smart gates at UK airports, UKBA’s introduction of departure lounge facial recognition at UK airports (*OB2:100d:22 footnote 5*) and the National Policing Improvement Agency’s deployment of mobile flat print fingerprint-checking devices to police patrols (*OB2:100d:22 footnote 4*).

- 1.2 If the Appellant may respectfully suggest, it is important for the Tribunal to be scrupulously clear that it is only facial recognition and flat print fingerprinting that are on offer for these projects. They need to be clearly distinguished from and not confused with their more successful cousins – DNA, iris scans and traditional fingerprinting.
- 2 We know that no report of large-scale trials published by a respectable institution over the past 10 years or so provides any confidence that these two biometrics can deliver the benefits sought from them. That goes for *technology tests* and for *scenario tests*. And we know that no reports at all have been published which systematically examine the success or otherwise of these two biometrics in live use, there have been no *operational test* reports **T2**
- 2.1 The basis for using this figure of 10 yearsⁱ is filed in the notes to this submission.
 - 2.2 The distinction between technology, scenario and operational testsⁱⁱ is explained in the notes to this submission.
 - 2.3 If there were any reports that justified the Home Office’s investment in biometrics-dependent projects the Tribunal may legitimately expect that the Respondents would have mentioned them by now, nearly six months into the Appeal. Absent which, there are no such reports.
 - 2.4 In the absence of any respectable reports suggesting that facial recognition and flat print fingerprinting are reliable enough to do the jobs required of them, the assumption made must be, to put it loosely, that “the technology doesn’t work”.
 - 2.5 It is a matter of fact that many people find that impossible to contemplate. They assume that the technology must work. There are no reports to support this assumption, to prove that there is a positive return for the public on an investment, it is prejudice, but they assume it anyway.
 - 2.6 For example, the UKPS biometrics enrolment trial demonstrated to most observers that facial recognition and flat print fingerprinting are too unreliable to be worth investing in. The Home Office responded eccentrically by saying that the trial was not really a scenario test. They carried on investing in these biometrics regardless, by their own lights without any supporting evidence, with nothing to go on – at least, nothing they have mentioned during the course of this Appeal – but wishful thinking.

- 2.7 Again with respect, the Appellant enjoins the Tribunal seriously to countenance the possibility that the chosen biometrics do not work well enough to be useful to the public and to justify the Home Office's speculative investment of our money, to adopt a scientific scepticism in which biometrics are guilty until proven not guilty.
- 3 We know that the Home Office are not meant to waste public money. In the circumstances T1 and T2 above, as long as we stick to published sources only, it looks likely that public money has been and is being wasted by the Home Office. That is not the only way to describe the state of affairs, but it is not an obviously false way to describe it. There is a hypothesis there to test – that the Home Office have been and perhaps still are investing in biometrics-dependent projects without holding in their hands the evidence required to justify their confidence that the technology can deliver **T3**
- 3.1 If they were wasting public money until the IBM report was given to them, some time before April 2009 (*OB2:31-2*), that is a matter of public interest. It implies that the Home Office had no businesslike reasons to fund investments in biometrics-dependent projects for 7½ years or so.
- 3.2 Since that time, the Home Office claim that they *do* have a report which justifies their investment – the IBM report. If even *that* report doesn't justify these investments, then it is likely that the Home Office have continued to waste the public's money for a further 2½ years or so to date and that, too, is a matter of public interest.
- 3.3 The IBM biometrics exercise when they evaluated the products of six suppliers is a technology test. Messrs Wayman, Possolo and Mansfield have examined all the technology tests available to them and concluded in their paper (*OB2:75-5:59-67*) that:
- ... technology testing on simulated data cannot logically serve as a proxy for software performance over large, unseen, operational datasets.
- 3.4 These men have spent their lives studying biometrics and making contributions to the body of knowledge and advising the US and UK governments, among others. Their paper is an Authority and not just "some academic material" as the Home Office call it (*HOResp2:14:42*). It seems likely therefore that the IBM report doesn't justify the Home Office's investment of public funds in projects dependent on facial recognition and flat print fingerprinting for their value to the public.
- 3.5 Neither the Commissioner nor the Home Office has advanced any reason for the Tribunal to ignore the conclusions of Messrs Wayman, Possolo and Mansfield. They don't say why these three world experts are wrong. They offer no counter-arguments. The Tribunal may judge that the Respondents *have* no counter-arguments and that Messrs Wayman, Possolo and Mansfield just are right.

- 3.6 Professor Anderson, like Messrs Wayman, Possolo and Mansfield, is also a world Authority. He says, in his expert and independent testimony (*OB2:308:7*):

The banks investigated biometrics extensively from the mid-1980s to the mid-1990s and concluded that for a biometric recognition technology to be serviceable in retail banking it would have to have an insult rate (false reject rate) of no more than 0.01% and preferably 0.001%; provided this were met, a fraud rate (false accept rate) of 1% or even higher would be acceptable. (In attended operation, a fraud rate of 1% means a 99% risk that someone who attempts to impersonate a customer will be caught.) The only biometric that comes close is iris recognition ...

- 3.7 Iris recognition – the technology that comes close to meeting the retail banks' requirements but doesn't actually meet them – the Tribunal may note, is not a technology on offer from the Home Office. The technologies they do propose to rely on do not even come close to meeting the retail banks' requirements to counter fraud.
- 3.8 They didn't in the 1980s and 1990s and they still don't – as we know, the retail banks still don't use facial recognition and flat print fingerprinting in their efforts to counter money-laundering and fraud based on "identity theft". If the banks don't believe that this technology is up to the job, why do the Home Office believe that it is? What do they know that the banks don't? They don't say, no reason is given to ignore Professor Anderson's opinion on which, like Messrs Wayman, Possolo and Mansfield, he stakes his professional reputation.
- 3.9 The banks don't rely on this technology and neither do the world's business schools (*OB2:91:170*) – they tried both facial recognition and flat print fingerprinting and gave up on them. Again, no response from the Commissioner or the Home Office to this point about the business schools which was made nearly four months ago in the Appellant's Submission dated 31 May 2011.
- 3.10 After the recent riots in the UK, evidence was collected to identify the riotersⁱⁱⁱ:

Photographs, video and CCTV images will be examined by 450 detectives involved in Operation Withern. Simon Foy, a Metropolitan Police Commander, said: "We will be remorseless in our pursuit of these individuals."

- 3.11 How many biometrics companies have volunteered their facial recognition technology to help to identify the rioters and reduce the number of detectives posted to Operation Withern? As far as we know, none, despite the fact that this technology is supposed to be useful. Here is an opportunity for the biometrics community to demonstrate its worth and they don't seem to be taking it. Why should the Tribunal place its trust in the IBM report if even the biometrics community evidently don't?

- 3.12 “Biometric technology is used in both the public and private sectors to deter and detect crime, especially identity fraud”, say the Home Office in their 24 August 2011 submission (*HOResp2:74*). Which institutions use this technology? Which biometrics do they use? Facial recognition? Flat print fingerprinting? Some institutions may use biometric technology, but does it work? The Home Office offer no answers and this comment of theirs is forlorn compared with the testimony of Professor Anderson.
- 4 We know that the Home Office claim to be exempt under §§31, 41 and 43 of the Freedom of Information Act 2000 from disclosing the IBM report and that the Commissioner agrees with them and that IBM, Morpho and at least one other biometrics supplier who participated in the IBM technology test all strongly object to disclosure of the report **T4**
- 4.1 With regard to the §31 exemption, the Appellant’s case is set out in his previous submission (*OB2:100c-d:14-25*). The Appellant also reiterates his earlier position that he doesn’t want to do anything to make crime-fighting and counter-terrorism any harder than they already are (*OB2:22:18*). If the Home Office can offer some evidence that their chosen biometrics will help to reduce crime and enforce immigration controls, that is good. So far, though, they have offered no evidence of that whatever for 10 years or so and we can’t just assume that the technology works.
- 4.2 There is no sign that the Commissioner investigated the efficacy of the Home office’s chosen biometrics. He was too ready to accept that there is a valid §31 exemption. The Appellant asks accordingly that the Tribunal uphold the Appeal.
- 4.3 With regard to the §43 exemption, the Appellant’s case is set out in his previous submission (*OB2:100d-f:26-41*). The Appellant also reiterates his earlier position that he doesn’t want to do anything to open IBM to unlimited damages claims (*OB2:22:18*) – that position hasn’t changed and the Appellant objects to the suggestions made by the Home Office that he is happy to see “gratuitous” damage inflicted on the public, the Home Office, IBM, Morpho and others (*HOResp2:67,70*).
- 4.4 The Appellant’s case rests on the unprovability of counterfactual statements. The Home Office assert that if the names of the losing participants in the IBM technology test were revealed – which they haven’t been, it’s a counterfactual – then their commercial interests would be damaged. But the name of the supplier of the unreliable technology used in the UKPS biometrics enrolment trial was revealed, their turnover has increased ever since and now Safran/Morpho have paid \$1.1 billion dollars to buy a lot of technology which has been demonstrated publicly to be unreliable and taken on \$500 million of the company’s debt in addition.
- 4.5 Only an exceptionally gifted judge would have predicted that. Whatever the sense is that is required, it is not common. The Home Office’s assertion that it is possible to determine the truth value of a counterfactual

“using methods ranging from common sense and the professional experience of informed witnesses to the use of detailed and elaborate mathematical modelling by expert economists” (*HOResp2:85*) is demonstrated thereby to be false, at least in this case.

- 4.6 Seeing the results of the UKPS biometrics enrolment trial, again only an exceptional judge would have predicted that IPS would continue to propose to use flat print fingerprinting in the NIS. IPS stipulated that the maximum acceptable false non-match rate was 1% and the figure that came out of the trial was between 19% (able-bodied participants) and 20% (disabled participants). Both 19 and 20 are greater than 1, and yet IPS continued. Another case where the Home Office’s assertion is demonstrated to be false. Are there any where it is demonstrated to be true?
- 4.7 (The acknowledged world authority on counterfactuals is Professor Willard Van Orman Quine (RIP) and the Appellant commends Quine’s luminous writings^{iv} on the subject to the Home Office, the Commissioner and the Tribunal.)
- 4.8 The Appellant is steadfast in upholding intellectual property rights. IBM’s testimony asserts that six biometrics technology suppliers including Morpho decided to give “business-critical intellectual property” to IBM (*OB2:354:18*), who gave it to the Home Office. In the Appellant’s view, that was an imprudent commercial decision and a risk that it was quite unnecessary to take with their companies’ assets – the Home Office and IBM need to know *that* the suppliers’ products work, not *how* they work, they do not need to know how the products work in order to test them.
- 4.9 The Appellant has not seen the IBM report, of course, and so has to ask the Tribunal respectfully to determine if the report really does include business-critical intellectual property and, in its exceptional judgement, if IBM really would be open to claims for unlimited damages if the report were disclosed in full. The shareholders of these companies may also be interested to know whether, having unnecessarily risked the companies’ assets, the directors are in breach of their fiduciary duties.
- 4.10 The Home Office argue that suppliers will be reluctant to give them sensitive information in future if the IBM report is disclosed. Quite right, they should be reluctant. But here we have a case where the suppliers *did* give business-critical intellectual property to a rival, IBM, and to the Home Office, in the full knowledge that it was subject to the Freedom of Information Act 2000, against which a non-disclosure agreement (NDA) is not necessarily proof. So perhaps the Home Office needn’t worry too much.
- 4.11 Giving business-critical intellectual property to a rival might suggest to a judge that it is not very valuable property in the eyes of the directors. The judge might feel that he is looking not so much at Glaxo and a new drug as at an astrologer and his trade secrets.

- 4.12 The Commissioner accepted the Home Office's §43 exemption case too readily. The Appellant asks that the Tribunal uphold the Appeal.
- 4.13 With regard to the §41 exemption, we were all misled by the Home Office for a long time – the Appellant, the Commissioner, the Treasury Solicitors, Counsel and the Tribunal – until they finally agreed with the Appellant (*OB2:85-6:126-132*) that there *is* an explicit confidentiality agreement between the Home Office and IBM.
- 4.14 If the Commissioner had investigated the matter thoroughly, we wouldn't all have wasted our time debating the subsequent concoction of imputed duties of confidence. The Commissioner's investigation was deficient and the Appellant asks that the Tribunal uphold the Appeal.
- 4.15 The Commissioner failed to investigate the matter at hand – the reliability of the biometrics chosen by the Home Office – he failed to investigate the Home Office's §§31 and 43 arguments and he failed to check whether there was an explicit confidentiality agreement between the Home Office and IBM but he did find time and put in the effort to construct an elaborate case for an imputed duty of confidence. The Appellant suggests that that is the wrong allocation of the resources of the champion of the Freedom of Information Act 2000 and trusts that one benefit that will emanate from this Appeal is that the right priorities will prevail in future and the Home Office can look forward to much more onerous and genuinely testing investigations by the Commissioner.
- 4.16 The Home Office, IBM, Morpho and the others have rights. Of course. That is not contested by the Appellant. But so do the public (*OB2:49-50:11-19*). We have the right to expect the Home Office not to waste public money and the Commissioner dedicated little or no effort to evaluating that right of the public's. He acknowledged it but he didn't defend it.
- 4.17 Beyond the Freedom of Information Act 2000, the Home Office argue that the IBM report should not be disclosed because there are very few biometrics technology suppliers in the world. The number of these suppliers is not in the Home Office's gift.
- 4.18 The Home Office argue also that they could not do their job properly if the IBM report were disclosed. Since they raise this obfuscatory issue, the Appellant wishes to point out that, even with the report undisclosed:
- they failed to deploy the NIS
 - the smart gates at UK airports don't work
 - we're all paying three times too much for our ePassports
 - not a single educational establishment in the country has a card reader that can check the biometrics on UKBA's biometric residence permits
 - eBorders has severe problems
 - Raytheon are currently suing the Home Office for £500 million

- 5 We know that with the duty of confidence firmly established here, thanks to the Appellant, the IBM report must remain confidential unless the public interest in disclosure outweighs the public interest in non-disclosure – as the Commissioner says in his Decision Notice (*OB2:4:11*): “a breach of confidence would no longer be actionable if there is a defence that this breach was in the public interest” **T5**
- 5.1 The Commissioner does not explain how he came to the conclusion that the public interest in non-disclosure exceeds the public interest in disclosure. He asserts it but gives no hint of his reasoning. It is a mystery where there should be a cogent explanation. His Decision Notice is unsatisfactory from that point of view and the Appellant asks the Tribunal to uphold the Appeal.
- 5.2 The Appellant is convinced that the public interest in disclosure outweighs the public interest in non-disclosure but it’s not easy to weigh the two public interests. It’s an adult problem and not a childish matter of finding the roots of a quadratic equation.
- 5.3 It would have been usefully informative to see how the expert – the Commissioner – does it. The Appellant is hamstrung also by not having seen the IBM report. And by not knowing what are the National Biometric Identity Service (NBIS) service levels/acceptance tests Ms Keane refers to in her testimony – the IBM report is supposed to demonstrate that Morpho’s products are capable of meeting those requirements.
- 5.4 Every piece of evidence in the public domain tells us that the Home Office have been wasting our money for 10 years or so on projects which must fail, partially or completely, to the extent that they depend on facial recognition and flat print fingerprinting. The IBM report is the only obstacle to stopping this waste. Publishing it would help at last to turn the taps off. Not disclosing the report would prolong the years of waste.
- 5.5 That argument is correct. And it implies a highly critical view of the Home Office’s rôle in these projects. They are complicit, according to the Appellant, in a massive waste of public money. The Appellant wishes that he didn’t hold that view but it is unavoidable in the circumstances. Biometrics have brought out the worst in the Home Office over the past 10 years or so. The boil must be lanced to restore the health to the Home Office which the public want, need, deserve and pay for. That consideration outweighs the public interest in non-disclosure. The IBM report must be published.
- 5.6 Consider for example the Home Office’s behaviour in connection with the UKPS biometrics enrolment trial. They ignored the results of the trial, apparently determined to proceed with facial recognition and flat print fingerprinting even though they knew that these biometrics are unfit for purpose. That is not the behaviour of an upright, businesslike, scientific, logical, responsible and dignified organisation. Look at the quotations from the House of Commons Science and Technology Committee report

already cited (OB2:67-8:8). Look at the excruciating para.81 of that report. Consider that the Committee declared themselves to be “concerned” 20 times in their report, “surprised” four times, “regretful” three times, “sceptical” twice and, once, “incredulous” at the “confusion” 15 times, “inconsistency” four times and “lack of clarity” over 50 times of IPS’s plans for the NIS. The mendacity of IPS’s behaviour, abetted by the Home Office Scientific Development Branch (HOSDB), is itemised in the Appellant’s 8 January 2009 letter to HOSDB (OB2:165-78). Water off a duck’s back, the Home Office proceeded. That was five years ago. They’re still trying to hold the line.

- 5.7 Consider for example the 29 January 2009 press release issued by the Home Office, *Benefits of ID cards for Manchester*, which was misleading in at least 10 ways identified in the Appellant’s letter dated 8 February 2009 (OB2:179-87). How can the Home Office issue a press release including claims they know to be false? The letter was sent to Sir David Normington, then Permanent Secretary at the Home Office. He did nothing to have the press release corrected. How can that happen in the UK Home Office?
- 5.8 Consider the example of the smart gates installed at 10 UK airports, starting with Manchester and Stansted airports. In August 2008, the technology was described as being under test, it was a trial. By February 2009, the UKBA business plan asserted that this technology would make the UK border more secure (OB2:188-91). In June 2009, Brodie Clark^v said in a letter to the Appellant written on behalf of Sir David that the technology was still being trialled. Would it secure the border or wouldn’t it? The matter was taken up with Lin Homer, chief executive at the time of UKBA (OB2:207-16). In February 2010, Ms Homer said that UKBA still planned to evaluate the technology at all 10 airports (OB2:221 *penultimate paragraph*). Then in May 2010, John Vine CBE QPM, the Independent Chief Inspector of UKBA, published his report, *An inspection of border control at Manchester Airport^{vi}*, in which he describes a number of problems with the smart gates and then says:
- 5.29 We could find no overall plan to evaluate the success or otherwise of the facial recognition gates at Manchester Airport and would urge the Agency to do so soon as possible.
- 5.9 In the opinion of the Appellant, the public can’t tolerate this situation. Good people like Lin Homer and Brodie Clark are being suborned. The Tribunal may agree. At the very least, the Tribunal must not be drawn into the Home Office’s tangled web and be seen to condone it.
- 6 We know from the testimony submitted by the Home Office (OB2:311-50) and IBM (OB2:351-420) – what the public didn’t know before – that IBM were awarded the NBIS contract, announced in the Home Office press release dated 7 April 2009 (OB2:31-2), *because* they had allegedly demonstrated by their technology test of facial recognition and flat print fingerprinting that at least one biometrics supplier could meet the NBIS requirements^{vii} **T6**

- 6.1 This new information explains why the Home Office thought the Appellant was objecting to the NBIS contract being let to IBM and the Appellant didn't think he was (*OB2:88:148-9*).
- 6.2 The Home Office chastise the Appellant for "attacking" Mr Swain (*HOResp2:21:69*), who submitted evidence on behalf of IBM. The Appellant saw from Mr Swain's evidence that the biometrics suppliers had NDAs with IBM and that IBM nevertheless disclosed sensitive information to the Home Office. That is a contradiction which it seems legitimate to bring to the attention of the Tribunal. If the Appellant has missed that point in Mr Swain's testimony where he provides the intervening step in the argument, whereby the NDAs sanction disclosure to the Home Office, then the Appellant extends his profuse apologies to Mr Swain.

ⁱ How long have the Home Office been interested in biometrics?

It is nine years since they published their consultation document on the introduction of government-issued "entitlement cards" (subsequently "ID cards") in the UK. That was July 2002.

The "National Identity Scheme" (NIS), as it subsequently became known, relied on biometrics. Its success depended on biometrics. If the biometrics chosen were not reliable, the NIS could only fail.

The Home Office must have been working on this scheme for some time before publication. Rt Hon David Blunkett MP says in the foreword to the consultation document that 9/11 provoked great pressure for the scheme. That was 10 years ago.

It is 12 years since PA Consulting were asked to advise the government on identity management with a view to delivering "joined-up government" (*OB2:98, final paragraph*). That assignment of PA Consulting's led to, among other things, the Cabinet Office's plans for Transformational Government, a scheme which was projected one day to rely on biometrics for identity management (*OB2:173*).

Nine years? 10 years? 12 years? There is no precise answer to the opening question above. In this submission, it is assumed that 10 years or so is an acceptable approximation.

ⁱⁱ The terminology of the US National Institute of Standards and Technology is used here.

A *technology test* is a computer-based trial conducted in the lab using "simulated" data. In the case of biometrics tests, the data is normally obtained from prisoners, who can be coerced in large numbers to co-operate.

A *scenario test* is a field trial using a group of participants held to be representative of the population as a whole. The data obtained is more real, less simulated but the test is still a trial, it is not conducted in the often chaotic, high-volume conditions of an airport, say, with real travellers really trying to clear immigration.

An *operational test* is an examination of the technology under real conditions. There are obvious limitations in the case of biometrics. An impostor who has successfully cleared immigration, for example, is not going to come back and report a false positive to help the researchers to maintain accurate statistics.

ⁱⁱⁱ *The Times*, 9 August 2011, 'Public asked to name rioters on internet 'rogues gallery'', <http://www.thetimes.co.uk/tto/news/uk/crime/article3119516.ece>

^{iv} Willard Van Orman Quine, *Word & Object*, The MIT Press, Cambridge, MA:1960
Quine writes (p.222):

What sets [the strong or subjunctive conditional] apart from the ordinary conditional is not falsity of its antecedent or 'if'-clause, but the fact that the conditional can be seriously entertained and affirmed or denied in full cognizance of the falsity of the antecedent. An ordinary conditional forfeits our interest and ceases to be affirmed or denied once we are satisfied of the truth value of its antecedent.

The subjunctive conditional depends, like indirect quotation and more so, on a dramatic projection: we feign belief in the antecedent and see how convincing we then find the consequent. What traits of the real world to suppose preserved in the feigned world of the contrary-to-fact antecedent can only be guessed from a sympathetic sense of the fabulist's likely purpose in spinning his fable.

The usage of counterfactuals, he says, appears on a spectrum. At one end of the spectrum, where their truth depends on dispositions in objects which can be ascribed to generally accepted physical properties, it's alright to use counterfactuals because they can always be replaced with ordinary conditionals when we want to express ourselves precisely. Elsewhere on the spectrum, e.g. in psychology where we manifestly haven't got a clue about the underlying structure, counterfactuals must be eschewed (*ibid.*, p.225):

The further a disposition is from those that can confidently be pinned on molecular structure or something comparably firm, the more our talk of it tends to depend on a vague factor of *caeteris paribus*.

^v <http://dematerialisedid.com/BCSL/Brodie%20Clark.html>

^{vi} <http://icinspector.independent.gov.uk/wp-content/uploads/2010/03/An-inspection-of-border-control-at-Manchester-Airport.pdf>

^{vii} Nicholas Swain, IBM's Commercial Director for the Immigration and Asylum Biometric System (IABS) Programme, says in his evidence:

... The approach, methodology and test systems used were designed by IBM in conjunction with its sub-contractors. These tests used data provided by the Home Office and were designed to demonstrate that IBM's solution could meet the requirements specified by the Home Office for NBIS in terms of both facial and fingerprint matching accuracy and speed. IBM also used the tests to assist it in selecting its preferred sub-contractor. (OB2:352:10)

... [the report] was provided by IBM only to demonstrate that IBM could meet the Home Office's requirements ... (OB2:353:13)

Thereafter, on 1 May 2009, IBM signed a contract to provide NBIS with the Home Office and, shortly afterwards, entered a sub-contract with Sagem (now Morpho), one of the suppliers who participated in the Demonstration, to provide the specialist biometric software needed for NBIS. In August 2010 this contract was revised and the programme was re-named IABS. (OB2:353:14)

The sole purpose of providing the Report to the Home Office was to demonstrate that the solution proposed by IBM, including the specialist biometric software from the selected sub-contractor, could meet the specific requirements laid down by the Home Office for NBIS ... (OB2:353:17)

... Schedule 17 of the NBIS Agreement had all of the biometric performance requirements (Exhibit 6, pages 10 & 11) redacted. Demonstrating that these requirements could be met was the primary objective of the Demonstration and Report. (OB2:354:22)

... the Report was specifically focussed only on meeting the NBIS requirements.
(OB2:356:36)

And Jackie Keane, Programme Director of the Immigration & Asylum Biometric System (IABS), says in her evidence:

As part of the NBIS tender process, IPS had stipulated that bidders needed to demonstrate the ability to fulfil and comply with service level agreements identifying the requirements of the biometric systems. (OB2:313:10)

As part of this tender process IBM proposed to IPS, in support of their bid, to undertake an evaluation of biometric specialist suppliers so they could effectively evaluate whom they wished to partner with in their overall bid and prove to IPS that they could meet the facial and fingerprint matching requirements prescribed by the NIS. (OB2:313:11)
