Biometrics – IPS, the Flat Earth Society and transformational cosmology

© David Moss 2009

The author wishes to thank *The Register*,
who kindly commissioned
the first version of this paper.

Until the 16th century, educated opinion, as codified by Ptolemy, held that the earth is at the centre of the universe. Then along came Copernicus.

On 29 June 2009, the Identity & Passport Service (IPS) published their latest paper on the National Identity Service (NIS). According to *Safeguarding Identity*, "the vision for the NIS is that it will become an essential part of everyday life, underpinning interactions and transactions between individuals, public services and businesses and supporting people to protect their identity" (para.3.32).

Placing the NIS at the centre of social interaction like this, makes IPS about 92 million miles wide of the mark [1].

How is the NIS supposed to achieve IPS's vainglorious objective? "Our intention is that, at the core of the information used to prove identity will be biometrics, such as photographs and fingerprints" (para.3.6).

It follows that, in the eyes of IPS, the NIS stands or falls on the reliability of the biometrics chosen. If they don't work, the NIS can't work.

When he was Home Secretary, David Blunkett told us that biometrics "will make identity theft and multiple identity impossible. Not *nearly* impossible. Impossible". That is the commonly held view.

It may be the commonly held view, but is it correct?

Not everyone agrees. Dr Tony Mansfield and Mr Marek Rejman-Greene, for example, opened their February 2003 report to the Home Office by saying the exact opposite, "biometric methods do not offer 100% certainty of authentication of individuals" (para.4).

Tony Mansfield specialises in biometric device testing at the National Physical Laboratory and Marek Rejman-Greene is the Senior Biometrics Advisor at the Home Office Scientific Development Branch (HOSDB). Who is right? Those two individuals? Or David Blunkett and all the politicians and civil servants and journalists in the UK and abroad who agree with him?

For Copernicans, the answer depends on the evidence.

There follows a review of the biometrics evidence that has come to light over the past six years.

IPS need fingerprints and facial geometry to work. Will they pass the test?

Tony Mansfield and Marek Rejman-Greene's report makes the distinction between two different jobs for biometrics – identification (section 2.1) and verification (section 2.2).

Identification is the job of proving that each person has one and only one entry on the population register. Professor John Daugman, the father of biometrics based on the iris, demonstrates easily that that job is not feasible for large populations.

Suppose that there were 60 million UK ID cardholders. To prove that each person is represented by a unique electronic identity on the population register, each biometric would have to be compared with all the rest. That would involve making 1.8 x 10^{15} comparisons.

Suppose further that the false match rate for biometrics based on either facial geometry or fingerprints was one in a million (1 x 10^{-6}). It isn't. It's worse than that. But suppose that it *was* that good, then there would be 1.8 x 10^{9} false matches for IPS to check.

It is not feasible for IPS to check 1.8 billion false matches. It is therefore not feasible for these biometrics to do their identification job.

Verification on the other hand, according to Tony Mansfield, is millions of times easier, and requires only that your facial geometry match the photograph recorded on your ID voucher (whether a passport or an ID card or a biometric visa) or that your fingerprints match the templates recorded on the voucher that you proffer to an immigration control officer, for example, or to a bank manager or to a GP, to underpin your transactions and interactions with them.

It may be millions of times easier, but can the biometrics chosen for the NIS achieve even the job of verification [2]?

Apparently not.

In 2004, the UK Passport Service (UKPS, now IPS) conducted a biometrics enrolment trial. 10,000 of us took part and a report of the trial was published in May 2005.

Under the heading *Key Findings* (para.1.2), sub-heading *Verification success rates* (para.1.2.1.4), the report says that **31%** of people could not have their identity verified using **facial recognition technology** – they were told that they did not match the photograph of them taken only five minutes before.

That was just the able-bodied participants. For the disabled, the false non-match rate was **52%** – everyone would do better to toss an unbiased coin.

And, using **flat print fingerprinting** technology [3], **19%** of the able-bodied participants could not have their identity verified, and neither could **20%** of the disabled [4].

Fingerprints didn't do very well in the UK. Will they fare better in the US?

With some people, you can give them any amount of evidence, they will continue to believe that the earth is flat.

Failure rates of 19 and 20 and 31 and 52% clearly scupper IPS's plans for the NIS. Millions of us would be unable to prove our right to work in the UK if that proof depended on biometrics, we would be unable to obtain non-emergency state healthcare and our children would be barred from state education.

Faced with revolution, the government would have to abandon the NIS. Logic, maths, science, a basic understanding of technology, businesslike common sense, an adult sense of responsibility, simple truth-telling and a desire to preserve institutional credibility and dignity all suggest that the NIS should have been abandoned on the day the biometrics enrolment trial report was published [5].

Instead, what did IPS say when the House of Commons Science and Technology Committee confronted them with these failure rates? According to the Committee's July 2006 report, IPS said that the key findings of their biometrics enrolment trial were not key findings, and that the trial was not a test of the *reliability* of biometrics, but only a test of their *usability* (para.88) [6].

If it wasn't a test of reliability, why are the reliability figures reported as key findings? Why would IPS want to test usability but not reliability? Surely they wouldn't deploy the NIS with biometrics that are congenial to everyone but just don't happen to work. And what is this distinction between reliability and usability? For 300 pages, the May 2005 report discusses usability almost entirely in terms of reliability.

Despite the polite and sensible entreaties of the Committee, no large-scale field trial of the reliability of flat print fingerprinting has been subsequently conducted by IPS. If the biometrics enrolment trial was not a reliability test, then there is still no evidence to support IPS's claim that flat print fingerprinting can deliver their vainglorious ambition [7].

Logic, maths, science, etc … all having been abandoned, IPS told the Committee, not quite that the earth is flat, but that the maximum acceptable false non-match rate for flat print fingerprinting is **1%** (para.18) and they pointed the Committee (p.126*ff*) to a May 2004 report written by the US National Institute of Standards and Technology (NIST).

Following 9/11, the newly established US Department of Homeland Security (DHS) designed US-VISIT, a biometrics-based scheme to protect the US border from infiltration by malevolent aliens. NIST conducted a computer-based trial of flat print fingerprinting to predict the success of US-VISIT. They estimated that the technology would successfully verify identity 99.5% of the time. That is equivalent to a false non-match rate of **0.5%**, well within IPS's 1% limit [8].

In December 2004, the US Office of the Inspector General (OIG) reviewed the statistics for the first year of operation of US-VISIT. On average, 118,000 people a day presented themselves to primary inspection at the borders. Primary inspection is largely a biometrics check. If the false non-match rate is 0.5%, you would expect 590 of them to fail and to be referred to secondary inspection by human beings. The actual figure was 22,350 failures. **19%**. Just like in the UKPS biometrics enrolment trial [9].

NIST provide no support for IPS. They predicted something like 0.5% and the outcome was more like 19%. The idea that the methodology used in their May 2004 report is a reliable way of forecasting the outcome in the field is thoroughly discredited [10].

Fingerprints didn't do very well in the US. Will facial geometry fare any better?

IPS may not have conducted any subsequent trials of flat print fingerprinting, but their cousins the UK Border Agency (UKBA) did start a six-month trial of biometrics based on facial recognition at Manchester airport in August 2008. 11 months later, no results have been published by UKBA [11].

When asked whether this technology works, instead of referring to the results of their own field trial, UKBA point to a report on the Face Recognition Vendor Test produced in March 2007 by … NIST [12].

This is another one of NIST's computer-based trials, not a field trial. The conclusion drawn from the report by both UKBA and HOSDB is that biometrics based on facial geometry are now reliable enough for airport security [13]. No earlier report is cited. No later report is cited. This is the single report on which UKBA and HOSDB rely. Are they right to place so much confidence in it?

The trial uses eight different sets of sample biometric data (p.35). Two of them are sets of iris scan data. Iris scans are not on offer in the NIS and those results of NIST's are therefore irrelevant. One is a set of three-dimensional face data, also not on offer in the NIS and so, again, irrelevant. Of the remaining five sets of data, four of them are taken from very few subjects – 257 subjects in the worst case, then 263, then 335, and 336 subjects in the best case. As any GCSE student can tell you, that is too small a sample for UKBA to be able to decide whether the technology would work for 60 million people in the UK.

Which leaves us with just one relevant sample dataset, of 36,000 subjects. And how well did facial recognition verify their identity? According to *Figure 20* of the NIST report (p.46), at a false match rate of 0.01%, 100 times worse than Professor Daugman's working figure, the false non-match rate varies between **8%** and **19%**, depending on which supplier's biometrics algorithm is used.

Once again, NIST provide no support to IPS or UKBA or HOSDB. A false non-match rate of between 8 and 19% does not sound like convincing evidence for the reliability of facial recognition as a biometric. Are UKBA really going to stop between 8 and 19% of passengers from boarding their flights? And remember that these figures emanate from a methodology which has already been discredited as a predictor of outcomes in the field [14].

There is one other piece of facial geometry evidence which it would be useful to see, and that is a report on the results of China's 10 million faces test, an element of Operation Golden Shield. China, like the UK, is keen on using biometrics. That report is unfortunately not available.

Where there should be evidence, the NIS relies on wishful thinking.

Here at the end of the review, the adventitious question arises *why* do politicians and civil servants all over the world continue to advocate the use of biometrics when the evidence simply doesn't support them? There is no answer. Their behaviour is inexplicable.

One thing is clear, though, and that is that biometrics cannot deliver. Identification is not feasible. Verification is laughably unreliable. And the flat earther David Blunkett is wrong. So is Tony Blair when he says that "biometrics give us the chance to have secure identity". And so is Gordon Brown when he says that biometrics "will make it possible to securely link an individual to a unique identity”.

The scale of the institutional fantasy which constitutes the NIS is grotesque [15]. Biometrics cannot underpin the NIS and so, by IPS’s logic, the NIS cannot underpin the “interactions and transactions between individuals, public services and businesses”. *Safeguarding Identity* is a false prospectus – no properly managed stock exchange would allow its shares to be listed. The NIS is guaranteed to fail [16].

Underpinning interactions and transactions between individuals, public services and businesses? Supporting people to protect their identity? The hopes for the NIS now seem a distant memory.

Notes

1 Safeguarding Identity appeared on 29 June 2009. Rt Hon Alan Johnson MP, Home Secretary, contributed one of the four forewords. He said "I fully endorse the actions set out in this strategy and look forward to supporting their delivery". Next day, 30 June 2009, he said "I want the introduction of identity cards for all British citizens to be voluntary".

But how can they be *voluntary* if the NIS "will become an *essential* part of everyday life"? Mr Johnson's position is untenable.

---

2 Verification is a source of some confusion among politicians and the media. Often, they wrongly elide the job of verifying people's identity with the job of making the NIS secure. If my flat print fingerprints match the templates stored on an ID voucher that I proffer to a policeman, say, then the biometrics have successfully completed their verification job.

But was the ID voucher issued by IPS? And even if it was, have I tampered with it since then and inserted my biometrics? The technology needed to answer those further questions and help to make the NIS secure is PKI – the public key infrastructure – and not biometrics.

Even David Blunkett gets the two confused, which is surprising considering that he had a job with a PKI company, Entrust, Inc.

---

3 The reported unreliability of fingerprinting will surprise people. Traditional rolled prints, taken by police experts, using ink, have been quite rightly trusted worldwide for a century now and they are admissible as evidence in court.

But as Messrs Mansfield and Rejman-Greene tell us, that is not the technology being used in the NIS. Instead, IPS propose to use the new technology of flat print fingerprinting (para.30, 86), which is quick and clean, it requires no expert in attendance, it appears to fail 19 or 20% of the time and it is not admissible as evidence in court.

To give these two different technologies the same name, “fingerprinting”, is literally a confidence trick.

---

4 As reported by the BBC, "the key to the power of biometrics to identify people is the amount of randomness and complexity that the biometric contains, according to Professor Daugman. 'Face recognition is inherently unreliable because there isn't nearly enough randomness in the appearance of different faces. Fingerprints are vastly better biometrics than faces,' he says, 'but better still are iris scans'".

That is a valuable explanation of Professor Daugman's there. "'Irises have about 249 degrees-of-freedom,' explains Professor Daugman, 'whereas faces have only about 20 degrees-of-freedom (independent dimensions of variation), and fingerprints have about 35'".

What do IPS have to say about the level of randomness required to make biometrics underpin the NIS? Nothing.

Before concluding, with Professor Daugman, that unlike fingerprints and facial geometry, iris scans *could* underpin the NIS, please note the problem discovered in the UKPS biometrics enrolment trial (para.1.2.1.3). **10%** of able-bodied participants were unable to register their iris scans in the first place. That figure rose to **39%** for the disabled.

In an NIS based on iris scans, these people would not appear on the population register. They would have no electronic identity. They could not be interacted with. They simply wouldn't exist.

---

5 According to the UKPS biometrics enrolment trial, the false non-match rate associated with IPS's chosen biometrics varies between 19 and 52%.

Really? Is that true?

There is an obvious counter-example – schools up and down the country use biometrics to take the register, to manage library-lending and to operate cashless canteens. Why don’t they suffer from 19-52% false non-match rates?

Schools can calibrate their biometric equipment to operate close to a zero false match rate or close to a zero false non-match rate, one or the other, but not both. There is a trade-off. If the school goes for a low false match rate, they will inevitably get a high false non-match rate and *vice versa*.

They go for a low false non-match rate so that not too many pupils starve. That's why there is no false non-matching problem to report.

But there must be a concomitant false matching problem. According to *Figure 9* of the NIST report (pp.16-17), with a low false non-match rate, the false match rate can quickly rise to 10% and even higher. Suppose that a pupil collects his or her lunch from the canteen and is identified only by his or her flat print fingerprint. Then, in a school of 1,000 pupils, it is likely that the computerised biometric canteen system can't identify which of 100 pupils in the school is the luncher and that the school is therefore wasting its money.

This trade-off is a fact of life in the biometrics industry. It is widely discussed in the academic literature, e.g. in Professor Ross Anderson's book on security engineering: "most biometric systems have a trade-off between false accept and false reject rates, often referred to in the banking industry as the *fraud* and *insult* rates". And NIST discuss the matter in their May 2004 report under the heading *Trading FRR for FAR* (section 4.3, pp18-19).

The implication is instructive – it is that ***biometric identity is discretionary***. Depending on how the operator calibrates the equipment, the biometrics might say that you are you, or they might not. That is not how we usually understand identity. IPS are using an alien version of the concept of identity.

---

6 The House of Commons Science and Technology Committee declared themselves to be "concerned", "surprised", "regretful", "sceptical" and "incredulous" at the "confusion", "inconsistency" and "lack of clarity" of IPS's plans for the NIS. The confusion, inconsistency and opacity remain, three years later. Among other things, the Committee recommended that IPS conduct large-scale field trials before choosing which biometrics to use in the NIS. They haven't.

IPS show no respect for the Committee. That part of our Constitution has failed. Where else can we turn?

Two suggestions, among many:

(a) The Advertising Standards Authority (ASA). Many of the pronouncements of politicians and civil servants about the NIS are misleading. But they cannot be investigated by the ASA because these pronouncements do not amount to advertisements. That situation is changing. IPS have hired M&C Saatchi and BBDO Abbott Mead Vickers as their above-the-line advertising agencies. These agencies have now started to produce advertisements. If any of them are in any way misleading, they can be reported to the ASA.

(b) The UK Statistics Authority (UKSA). It will have been noticed by now that there are *no* official statistics for the reliability of biometrics. The NIS is proceeding without any of the normal conditions that would be included in a service level agreement. Footnote 6(b) may be an odd place to put a major recommendation, but here it is anyway – no technology-based initiative, including the NIS, should proceed without a foundation of official statistics. Sir Michael Scholar, Chair of the UKSA, declares that "having good statistics is like having clean water and clean air. It’s the fundamental material that we depend on for an honest political debate". The UKSA have demonstrated a willingness to defend that position over the Home Office's misuse of knife crime statistics. They may prove to be valuable allies in the campaign to introduce sense into the plans for the NIS.

---

7 IPS may not have conducted any further trials of its reliability, but UKBA are already relying on flat print fingerprinting: "UKBA's biometric visa system has fingerprinted over 2.8 million people and so far has detected 3500 instances of attempted identity fraud".

If UKBA's deployment of flat print fingerprinting is detecting fraud, then that is to be applauded. But the question is whether flat print fingerprinting can be used to underpin *everyone's* interactions and transactions, nice people, as well as criminals and terrorists. The false non-match rates demonstrated in trials, 19 and 20%, suggest that they can't. Are there any figures for false non-matches available in the visa system? Apparently there are, but UKBA won't release the evidence. According to HOSDB, "we hold the false non-match rate evidence internally but it can't be released because it would make it easier for people to evade detection".

It may or may not be acceptable to exclude foreigners from the UK on the basis of evidence not admissible in UK courts. They do the same in the US, with US-VISIT. But US-VISIT only applies to non-US citizens. Unlike us in the UK, the US do not propose to rely on flaky biometrics for their own citizens. According to the House of Commons Science and Technology Committee report, "on 6 March 2006, we met informally a group of senior policy advisers from the Department of Homeland Security to discuss the identity cards programme. When questioned about the maturity of biometric technologies, the advisers agreed that currently the technology was probably not as reliable or as accurate as it might need to be for a national identity card scheme" (para.81).

---

8 It may not be immediately obvious how outrageous NIST's forecast is. In the 2004 international fingerprint verification competition, FVC2004, the best algorithm achieved a false non-match rate of **6.21%** at a false match rate of approximately 0%. Even with a false match rate of 1%, the best false non-match rate was **2.54%**, and IBM promptly formed a partnership with the winning company, Bioscrypt, Inc. No-one in 2004 had ever seen a flat print fingerprint algorithm capable of IPS's **1%** false non-match rate, let alone NIST's **0.5%**, and they still haven't.

---

9 NIST had argued that a true accept rate of 99.5% could be achieved using only two fingerprints. Once US-VISIT had demonstrated that the figure was more like 81%, they teamed up with the US Department of Justice to lobby DHS and the State Department to use 10 fingerprints instead of two.

Would that help? Would that improve the reliability of verification?

It sounds as though it should but, as Tony Mansfield will tell you, increasing the number of fingers sampled will not lead to an exponential improvement in reliability. Your fingers are not independent events, there are correlations, and if the *minutiae* on your index fingers are poorly defined they are likely to be poorly defined on your other fingers, too.

Some researchers note that it is hardly worth printing ring fingers and little fingers.

NIST found that right index fingers are inexplicably "better" than left index fingers (para.3.1.1).

Moving from two prints to 10 may not help much after all.

---

10 Messrs Mansfield and Rejman-Greene note in their report that there are exceptional problems with flat print fingerprinting (Appendix B, p.34). It is obviously hard to enrol people onto the population register if they are missing fingers and/or entire hands. It can also be hard to register older people, they say, manual labourers, East Asians and – that other unimportant minority group – ... women.

IPS have never explained what alternative arrangements will be made for these cases and the NIST report doesn't consider them. We remain in the dark, therefore, but IPS can't stay silent on the issue forever and when they do propose their alternative arrangements, the question will arise why we can't all use those alternatives and forget about biometrics altogether.

---

11 No results of their trial of facial recognition have been published by UKBA.

The BBC and the *Daily Telegraph*, however, seem to have a mole or two:

• "Sources from the UK Border Agency (UKBA) have revealed that the devices are failing to detect when two people pass through them at the same time. The system [smartgates, the Automated Clearance System (ACS)], which replaces traditional passport control measures, is undergoing a live trial at Manchester Airport, where a UKBA worker said it was suffering almost daily malfunctions. He said immigration officers had been able to accompany travellers through the scanners without an alarm being triggered, even though the booths are supposed to detect if more than one person enters at a time. 'Immigration officers have been able to tailgate passengers through the machine, without the machine picking it up,' he said ..."

• " The source said there were malfunctions taking place almost daily in the pilot project, which is thought to have cost the taxpayer several hundred thousand pounds. 'There are five pods and when one breaks down, they all break down,' he said ..."

• " The UKBA source said there were widespread concerns about the facial recognition equipment. 'There is no reliable data on the machine's ability to pick up forgeries and imposters,' he said ..."

• " A spokesman for the PCS union, which represents UKBA staff, said: 'The notion that you can replace the human intuition of highly trained immigration staff with unproven machines is dangerous. The technology is further undermined by staff sitting in front of the monitors for three hours at a time, leading to mental fatigue and a drop-off in concentration. There are major concerns about the reliability and accuracy of facial recognition technology ... We have advised our members not to train to use the equipment or to man it ..."

• "Up until the point of the official launch, it was rejecting 30 per cent of those who tried to get through it,' the UKBA worker said. 'We believe they had to recalibrate it – essentially make it easier to get through the system'".

And the *Telegraph* have tracked down another biometrics expert, like Tony Mansfield and Marek Rejman-Greene:

• "In a leaked memo, an official says the machines have been recalibrated to an 'unacceptable' level meaning travellers whose faces are shown to have only a 30 per cent likeness to their passport photographs can pass through. Rob Jenkins, an expert in facial recognition at Glasgow University's psychology department, said lowering the match level to 30 per cent would make the system almost worthless. Using facial recognition software from Sydney airport in Australia set at 30 per cent, he found the machines could not tell the difference between Osama bin Laden and the actors Kevin Spacey or even the actress Winona Ryder while Gordon Brown was indistinguishable from Mel Gibson".

---

12 In the course of their May 2004 report, claiming that flat print fingerprinting works well, NIST had this to say about the alternative, facial recognition: "Even under controlled illumination, which is not used in US-VISIT, the error rate of face is 50 times higher than the two-fingerprint results discussed here. If the case of uncontrolled illumination is considered, this factor would be 250. This means that face recognition is useful only for those cases where fingerprints of adequate quality cannot be obtained" (para.3.3).

By March 2007, NIST would have us believe, facial recognition algorithms had improved by one or even two orders of magnitude. IPS, UKBA and HOSDB may believe that. But note that the US government seems to be in no hurry to incorporate facial recognition into US-VISIT and certainly not into an ID card scheme for their own nationals.

---

13 On 19 August 2008, UKBA announced that "from this month the UK Border Agency is trialling new technology at Manchester Airport". Six months later, on 24 February 2009, UKBA announced their 10-point delivery plan. One pledge made there is, by August 2009, to have "completed delivery of new facial recognition technology in 10 terminals, giving British passengers a faster, secure route through the border".

It seems as though the uncertainty before the trial has now been replaced with confident promises of speed and security at the border.

Or has it?

Mr Brodie Clark, Head of the Border Force, says in a 26 June 2009 letter that: "The Home Secretary’s pledge to introduce gates at a total of 10 UK airport terminals by August, includes the two current sites at Manchester and Stansted. It will provide a further opportunity to test the technology on larger numbers of passengers, across a broader range of locations. It also means that the gates will be available to British and EEA citizens throughout the busy summer holiday period".

The uncertainty remains. This deployment of facial recognition at UK airports is still a test. February's 10-point delivery plan is misleading if the suggestion is that travellers will definitely benefit from increased security and processing.

---

14 Messrs Mansfield and Rejman-Greene note in their report that the reliability of biometrics based on facial geometry falls off a cliff two months after people are first photographed – "even under relatively good conditions, face recognition fails to approach the required performance" (para.52d). For the first two months in the life of any new passport, verification will be erratic. For the last 118 months, it will be impossible – that is the implication. What do NIST have to say about this problem? Nothing.

---

15 We have already noted some of the practical implications of NIS fantasy – millions of us would have trouble proving our right to work, getting state healthcare and state education. Here are three more:

• IPS have not even provided a way to collect everyone's biometrics. Italy (population 58 million) has a national network of about 8,000 ID card registration centres. The Netherlands (17m) has – or plans to have – about 4,000 centres. The UK (61m) was recommended by Tony Mansfield and Marek Rejman-Greene to set up a network of about 2,000 centres (para.105), a curiously low number, but not as low as the number IPS came up with, 69. Instead of registering people themselves, IPS expect high street retailers to do the job for them. But which high street retailer, having spent decades growing a trusted brand, will risk the anger of 20% of their customers who, having handed over their fingerprints, are told as a result that they have no right to work in the UK? Fantasy.

• If UKBA use flat print fingerprinting to check everyone coming into the country, and everyone leaving the country, UK nationals, other EEA nationals and non-EEA nationals alike, and if the technology performs as well as it does in US-VISIT, then they will have to detain about 8,000 travellers a day. The prisons are full. Where are UKBA going to put all the detainees? Fantasy.

• The process of issuing all non-EEA nationals in the UK with ID cards started in November 2008. "Their facial image and fingerprints will be taken to securely lock them to one identity", according to the Home Office press release. Unfortunately, according to the *Observer*, "Britain's first ID cards, issued last week with fingerprint and facial details, cannot be read by any official body because the government has not issued a single scanner". So what are the Home Office talking about when they say that "ID cards for foreign nationals will help secure the UK’s borders by improving immigration control and reduce identity abuses. They will also enable those here legally to prove it and prevent those here illegally from benefiting from the privileges of life in the UK"? Fantasy.

---

16 The NIS is guaranteed to fail? Anyone not convinced by the facts, figures and arguments presented here may consider that this is the febrile conclusion of a juvenile anarchist. In fact, it is the conclusion of the Office of Government Commerce, an independent office of HM Treasury: "This has all the inauspicious signs of a project continuing to be driven by an arbitrary end date rather than reality ... I conclude that we are setting ourselves up to fail".

What's more, the UK Passport Agency (UKPA, previously the Passport Office, subsequently UKPS, subsequently IPS) agree: "I wouldn't argue with a lot of this ...".

In addition to the politicians and civil servants driving the NIS, there are, of course, the consultancies, notably PA Consulting. PA give it as their opinion that biometrics is mostly hype.

And beyond the consultancies, there are the biometrics companies themselves. The history of L-1 Identity Solutions, Inc., one of the more financially successful members of the industry, provides some support for PA's view and no support for the NIS.
