THE IDENTITY PROJECT

RESEARCH STATUS REPORT

JANUARY 2006

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Houghton Street, London, WC2A 2AE

Letter from the Director

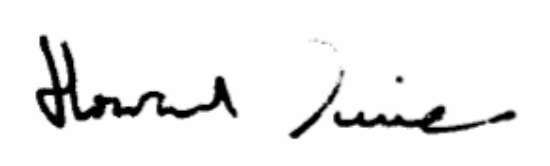
In June 2005 LSE researchers published a comprehensive costing and analysis of the government's proposed identity card scheme. This report analysed the best available evidence to determine the costs and implications arising from the proposals and concluded that the scheme would be an extremely expensive and technologically unsafe endeavour.

Since publication, the Home Office and its Ministers have attacked both the LSE and the report's authors with accusations of bias. We have been surprised by the tone of ministers' comments, which have not encouraged the kind of rational debate that proposals of this far-reaching nature surely require. The LSE has consistently stood by its researchers and the integrity of their work and continues to do so. The report was a genuine attempt to produce an informative analysis of the scheme. Many other commentators have welcomed it in that spirit.

This second report reviews the conclusions of the first, in the light of subsequent developments, and raises a wide range of new questions that we believe Parliament should carefully consider as it considers the government's revised proposals.

As this second report shows, the Government has not been very forthcoming in providing details of their proposals. The LSE team stands by the cost estimates outlined in its first report, but changes to the policy subsequently made by the Home Office make it difficult now to produce a definitive assessment of the total cost. Other government departments, if they wish to adopt the ID scheme, may opt in at a later date. Any estimates made of the cost of the current proposals may therefore significantly underestimate the total cost of the scheme in the longer term.

We believe the government's proposals can only benefit from informed and independent scrutiny of the sort this work attempts to produce. I hope the government can receive this latest contribution in that spirit and eschew the emotive language with which they responded to the first effort. The authors are not politically biased, or "mad" - at least no more so than academic researchers normally are!



Howard Davies

Table of Contents

Summary

This report outlines the current state of the LSE's research into the UK Government's identity card proposals and provides an assessment of developments since the publication of our first report in June 2005. The first section of this document outlines developments since our first report. The second assesses planning dynamics and contradictions in the government's case. The third discusses questions about the scheme that remain unanswered. The fourth recommends some ways forward.

Between June 2005 and January 2006 the LSE team continued its analysis of the Identity Cards scheme. Despite severe handicaps imposed by the Home Office (outlined in section two) we were able to assess important new material that supports and indeed strengthens the concerns raised in our first report.

The LSE research team had hoped to publish a second edition of our work in full. However, the government's refusal to disclose important information, coupled with new, conflicting evidence, has made it impossible to do so at this time.

As a result, the LSE's research team is presently unable to provide further assessment of the costs and potential benefits of the government's identity cards proposals. We do, however, stand by the figures published in our first report and believe these are the best available estimates of the true cost of the scheme. As before, we have not estimated the total integration costs throughout the public and private sector, which may be substantially higher.

The LSE announced at the House of Lords on November 9th 2005 that on the basis of statements made by the Home Office it would be adjusting downward a small number of line items in its costings (e.g. the cost of updating personal information on the national identity register). However, other line items (e.g. the cost of security measures and internal audit procedures) would have to be adjusted upwards in the light of new information. Repeated assertions by the Home Office that the LSE was substantially "wrong" in its estimates are scurrilous. The aggregated cost estimates from June 2005 remain as they were.

Dozens of questions about the scheme's architecture, goals, feasibility, stakeholder engagement and outcomes remain unanswered. Some of these questions are outlined in this report. The security of the scheme remains unstable, as are the technical arrangements for the proposal. The performance of biometric technology is increasingly questionable. We continue to contest the legality of the scheme. The financial arrangements for the proposals are almost entirely secret, raising important questions of constitutional significance.

Since the publication of our June report we have been increasingly concerned that the market based approach adopted by the government will lead to endemic identity checking, resulting in an unregulated rolling tax on citizens. By instituting a monopoly on identity architecture and placing this on a commercial footing, the Home Office risks creating a "free for all" in which organisations outside government can make substantial profits from relentless and unnecessary identity checking.

We are extremely concerned at the ongoing culture of secrecy endemic in the planning of the identity cards proposals. The Home Office has conducted most of its work in a covert fashion, refusing to disclose information that would inform debate, and conducting negotiations in a closed environment. This process is inimical to the creation of trust. This situation also makes further research on the proposals impossible.

We find it incomprehensible that Parliament has been denied crucial information about costs. We cannot see a justification for any claim of commercial secrecy and believe this assertion is misleading.

We are mystified as to why, after three in the planning, no government department has either signed up to the scheme or has provided published material on costs and benefits. We conclude that there still exists widespread uncertainty and scepticism about the proposals to an extent that may make the scheme unworkable at a level that goes beyond even that predicted in our first report.

An identity scheme of this magnitude should be managed by a department with the internal culture and experience commensurate with the scope and application of the project. The Treasury would in our view be the appropriate department to take on the work.

At the outset, the LSE Identity Project supported the implementation of an identity scheme in principle but expressed significant concerns regarding the Home Office proposal. In light of the numerous inconsistencies and conflicts that have emerged, serious unanswered concerns that remain, project dynamics that are dysfunctional and potential outcomes that may be harmful to the public interest we can now no longer support even the principle of an identity scheme owned and operated by the Home Office.

Acknowledgments

The Foundation for Information Policy Research
Professor Ross Anderson
Dionysis Demetis
Dr. Brian Gladman
Adam Joinson
Meryem Marzouki
Nick Pauro
Dr. Chris Pounder
Solenn de-Royer
Professor Angela Sasse
Sally Stares
Gus Stewart
Sarah Thatcher
Jerome Thorel
Rosemary Walsh
Professor Leslie Willcocks
for their advice, support, and reviews.

We would like to again thank the Department of Information Systems for its continuing support in hosting this project.

And we thank Professor Chrisanthi Avgerou and Professor Leslie Willcocks for joining our advisory group and further strengthening and expanding the substantial body of talent that has helped guide this project.

Advisory Group

Section I: Background and Developments

> "Like dialectic, policy analysis usually starts with plausible premises, with contestable and shifting viewpoints, not with indisputable principles or hard facts. Like dialectic, it does not produce formal proofs but only persuasive arguments. The key problem facing both dialecticians and analysts is how to base plausible inferences on values or opinions when hard facts are not available. Finally, policy analysis, like dialectic, contributes to public deliberation through criticism, advocacy, and education. Good policy analysis is more than data analysis or a modelling exercise; it also provides standards of argument and an intellectual structure for public discourse. Even when its conclusions are not accepted, its categories and language, its criticism of traditional approaches, and its advocacy of new ideas affect—even condition—the policy debate."
>
> - Giandomenico Majone, Evidence, argument and persuasion in the policy process, Yale University Press, 1989.

For decades the London School of Economics has been conducting research on a wide variety of pressing policy issues. LSE staff advise governments, serve on Royal Commissions, public bodies and government inquiries, and are seconded to national and international organisations. In the past three years alone, the LSE has conducted research and analysed policies in over 70 different projects commissioned and funded by a variety of UK Government departments and agencies amounting to more than £11m. These include studies on costing models, organising conferences and workshops, assessing policies, proposing alternative policy choices, and even exploratory research. This starkly illustrates the positive relationship between the LSE and Her Majesty's Government.

On issues relating to information policy, a variety of departments at the LSE have played prominent roles in academic and policy circles. The Identity Project is another such LSE initiative to generate understanding and inform policy debate and deliberation.

The Department of Information Systems began its research into authentication and identification systems in the 1990s. In 2003 it decided to conduct research to inform policy deliberation on biometric identification systems. Subsequently, the Department began a concerted initiative to inform the debate on the proposed identity card, first by hosting a number of public meetings on the then "entitlement card", then convening meetings with industry leaders and government departments. In 2005 this research activity culminated in the LSE's 'Identity Project'.

Over a hundred researchers and experts in technology and policy contributed to the project's first report over a concentrated period of months. The result was a three-hundred page report with over six-hundred

references and footnotes that analysed the policy landscape in the United Kingdom, as well as providing a comparative study of the identity requirements in other countries. The report questioned some of the key policy goals of the ID cards scheme, reviewed the likely effects on policing, assessed the challenges and risks in the Government's proposals, and offered an alternative scheme for public consideration.

We were heartened by the reception to the report. Many experts contacted us with their ideas, comments and suggestions. We received a high level of interest from Parliamentarians, industry representatives, technology and policy experts, and members of the general public from around the world.

We were astonished by the response from Government officials and Ministers, many of whom launched spurious, misleading and *ad hominem* attacks on the report and its authors. These sensational statements were very different from those expected during normal academic critique. 'Technically incompetent',[1] 'absurd',[2] a 'fabrication'[3] and 'highly partisan', were some of the terms used.[4]

There have followed some extraordinary and unfounded claims from Government ministers regarding our research, including 'unsubstantiated assumptions',[5] and 'plagiarism',[6] - when it was also claimed that the author of the report was LSE Visiting Fellow Simon Davies and that it should be renamed 'the Davies report'. This, even after 23 contributors to the report had written a Letter to the editor of the Daily Telegraph in July[7] refuting previous claims that the report was written by a single individual.

We were astonished by the response from Government officials and Ministers, many of whom launched spurious, misleading and *ad hominem* attacks on the report and its authors. These sensational statements were very different from those expected during normal academic critique.

In July 2005 we welcomed an official response from the Home Office.[8] However, in its response the Home Office claimed that we had inflated our cost estimates and had misrepresented the Home Office Identity Cards Scheme. The Home Office went on to claim that our alternative proposal would place personal information at risk, would not gain public trust, and had a high risk of failure. We were disappointed that the Home Office disregarded much of the report and focused almost exclusively on costs and tech-

1 'MPs narrowly back ID cards plan', BBC, June 29, 2005.

2 PM Opening Statement, Prime Minister's Monthly Press Conference, June 27, 2005.

3 'ID cards academic attacks Clarke', BBC, July 5, 2005.

4 For a summary of the government's claims see the letter to the Editor of the Times from LSE Director Howard Davies, 'LSE report on ID cards cost', July 2, 2005 at http://www.timesonline.co.uk/article/0,,59-1677135,00.html

5 Baroness Ramsay of Cartvale in Hansard, House of Lords, October 31, 2005, Column 35

6 Baroness Corston and Baroness Scotland, Hansard, House of Lords, November 16, 2005, column 1092.

7 'We're together on ID', July 7, 2005.

8 'Home Office Response to the London School of Economics' ID Cards Cost Estimates and Alternative Blueprint', July 2005, available at http://www.identitycards.gov.uk/library/Response_LSE_Alternative_Blueprint.pdf.

nological details. We were disappointed that the Home Office response to our report contained substantial material errors and misrepresentation of fact.[9]

Two examples are

- The Home Office accuses us of over-estimating the costs for 'marketing'. We have no such line-item in our costings. We only mention the term 'marketing' twice in the 300 page report: once in reference to the Home Office hiring of a marketing manager; and second when quoting from a Home Office commissioned report that provides an estimate.[10]

- The Home Office suggests that we ignored a statement from the Council of Europe Commissioner for Human Rights that they claimed was supportive of ID cards. As presented by the Home Office, his statement reads: "The issuing of some form of identifying document to all residents does not seem to me to be objectionable in principle, nor does the right to private life guaranteed by the Article 8 of the Convention preclude it. I carry an identity card myself and find it more useful than annoying". We informed the Home Office that we agreed entirely with the Commissioner's views but were surprised that they had failed to include the words of his statement that followed this selected excerpt: "What is important is the range of information stored, the range of persons with access to this information and the purposes for which the information might be used. Put simply, an identity card should be no more than its name suggests – a document containing sufficient information, and no more than is necessary, for establishing an individual's identity for relevant administrative purposes... The information should be used solely to establish identity for legitimate administrative purposes clearly specified by law and solely to the extent that those purposes require. Access to such information should, therefore, be conditioned by the same criteria."[11]

We note, however, that the Home Office's criticism of our first report has become more measured over time, possibly as a result of the soundness and logic of our calculations. The criticism has tended to become conditional and specific. For example, compared with the original claims that the report was "mad" and "fabricated", the most recent comments by Home Office Minister Baroness Scotland appear almost conciliatory:

> "A number of noble Lords, not least the noble Lord, Lord Phillips, asked about the difference between the LSE's consultation and ours. With the greatest respect to the LSE consultation, we say that it contains flaws in relation to the way in which the figures were put together…. I hope the Committee will appreciate that there are a number of reasons why we disagree with those findings and prefer our own."[12]

---

9 See our response at http://is.lse.ac.uk/IDcard/LSE_ResponseTo_HomeOffice.pdf.

10 Another report from another organisation, Kable, included marketing costs within their estimates, following the example of a Home Office commissioned-study. Though we collaborated with Kable on the costings models used, even a superficial analysis of the two reports would note the absence of the £1bn line item from the LSE report.

11 His words are available in full at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_06_05_human_rights in paragraphs 154 and 155.

12 House of Lords, December 19, 2005, Column 1564.

Updates to the Identity Report

There have been a number of developments since the release of version 1 of the Identity Project report in June 2005.

In particular we have followed the debates in Parliament and in the broader public domain. The Home Office has released further reports and statements that we have taken into consideration. These included discussions in Parliament, declarations at speeches and public events, quotations in the media, reports and official presentations. We have analysed Hansard throughout all the debates on the Bill and collected answers to parliamentary questions. We have also found a number of additional reports produced by other government departments, industry representatives and from other countries that further shed light on technology and policy dynamics relevant to this Bill. We have also benefited from the co-operation and expertise of officials, parliamentarians from all major parties, industry leaders and experts.

We were perplexed by the Home Office's continued insistence that it is absolutely right on so many of these matters. In such an extraordinarily complex arena filled with countless uncertainties the department never once conceded that it has misjudged even the slightest detail. However, in the months that followed the release of the report, controversy arose when ministers were quoted saying that the case of identity cards had been 'oversold',[13] and that many technological problems remain, e.g. there were difficulties that people with brown eyes, balding men, and labourers might be incorrectly identified by biometric systems.[14] From our experience on this matter, the only thing that we can conclude is that nothing is conclusive where applied technology is concerned, and any claims otherwise are premature at best, fantastical at worst.

We note that there have been a few relatively minor amendments to the Bill, as itemised in the recent Home Office newsletter, available at

http://www.identitycards.gov.uk/library/2005-12-20_IDENTITY-MATTERS-FOR-STAKEHOLDERS-NEWSLETTER.pdf.

The amendments to date have been mild. Our research findings on the Bill and the policy as it stands currently are presented below.

The International Landscape

The continued claims of 'international obligations' and the 'requirements' to develop biometric passports do not stand up to scrutiny., as we made clear in great detail in our first report,[15] and this work has not been challenged by the Home Office. The inclusion of all ten fingerprints and iris scans into passports is not required by international standards or American law. In claiming that the UK proposals are an international obligation the government has systematically misled the public and parliament.

In fact we could not identify a single other country that is adopting passports of this type, complexity and cost. Even the new U.S. passport will only be including a digital photograph on a contact-less chip that is

13 Guardian, 4 August 2005, p.1.

14 "ID Cards won't work if you've got brown eyes says minister', Oonagh Blackman, The Mirror, October 17, 2005.

15 Chapter 7, pp.49-96.

protected using a variety of technologies. Early on the U.S. State Department rejected using additional biometrics because they are considered overly complicated and costly. Moreover, after an open consultation process, the U.S. authorities significantly changed their plans in order to increase information privacy and security in the passport. We have seen no such open debate and deliberation on UK passports. Instead we are erroneously told that the UK is merely adhering to 'international standards' and thus Parliament has no say in this matter.

Only during the most recent debates in the House of Lords has the Home Office finally admitted that the UK is currently under no obligation from any foreign body to introduce identity cards.[16] That said the Government is actively lobbying to create such an obligation, just as it was involved in the negotiations on standards for biometric passports and the retention of communications data in Europe.[17] That is, the Home Office has been working with the EU to agree to common minimum standards for identity cards. Again the Government states that, regardless of whether or not the Bill receives Royal Assent, it will continue to work on these standards.[18]

At the same time the Government continues to claim that the UK is following suit from other EU countries that have identity cards. Both the LSE and Home Office research rejects this notion. A recent report from the Government on the identity requirements in other countries[19] supports the evidence presented in chapter 7 of our first report. Even the French Government, which hopes to implement a more limited biometric identity card, recently announced that it will now only pursue a voluntary system.

Even the French Government, which hopes to implement a more limited biometric identity card, recently announced that it will now only pursue a voluntary system.

Both our research and the Home Office study show that countries vary greatly on data collected, cost, renewal periods, uses, and even the information held on the cards. According to this research

- Only France and Spain collect fingerprints for their cards.
- At the proposed headline price of £30, the UK will have the second most expensive ID card in Europe, following Austria; while other countries charge significantly less than the proposed regime in the UK.
- Renewal periods for cards vary between 5-10 years, with most new card regimes calling for 5-year renewal, though older people are not required to renew their cards.

16 See Baroness Scotland of Asthal's statement in the House of Lords, December 12, 2005, Column 1103.

17 Whitley, E. A., & Hosein, I. (2005). Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. Telecommunications Policy, 29(11), 857-874.

18 This method of policy-making has been labelled 'policy laundering' where governments use international institutions like the EU and the UN to establish policies to then import them back home as international standards and obligations. See Hosein, Ian, 'The Sources of Laws', The Information Society, volume 20 number 3, 187-199.

19 Chart 1, update to Annex 3 of the Home Office publication 'Entitlement Cards and Identity Fraud: A Consultation Paper', published October 2005, available at http://www.identitycards.gov.uk/library/2005-08-10%20ID%20Cards%20in%20other%20countries%201.pdf.

COUNTRY	REQUIREMENT	CHARGE IN £	RENEWAL
Austria	Voluntary	39	10 years
Belgium	Compulsory	3-10	5 years
Bulgaria	Compulsory	n/a	n/a
Cyprus	Compulsory	6	10 years (5 years for younger people)
Czech Republic	Compulsory	3	10 years (5 years for younger people)
Denmark	No Card		
Estonia	Compulsory	n/a	n/a
Finland	Voluntary	28	5 years
France	Voluntary	Free	10 years (in flux)
Germany	Compulsory	6	n/a
Greece	Compulsory	Nominal	Indefinite
Hungary	Voluntary	4	Between 6 and 10 years, no renewal if over 70
Ireland	No Card		
Italy	Voluntary	4	5 years
Latvia	No Card		
Lithuania	Voluntary	0	10 years
Luxembourg	Compulsory	3 (no renewal fee)	10 years
Netherlands	Voluntary	21.50	5 years
Portugal	Voluntary	5	5-10 years, not required if over 70
Slovakia	Compulsory	0	10 years, not required if over 60
Slovenia	Voluntary	12	10 years. New card issued for every change of details.
Spain	Compulsory	4	5-10 years, not required if over 70.
Sweden	Voluntary	30	5 years

Identity Fraud

Currently, following several shifts in marketing emphasis, the justification most commonly put forward in public for introducing the ID card scheme is to combat what the Government calls 'identity theft' (although, of course, identities cannot be stolen, only used fraudulently).

The Home Office believes that identity cards will reduce

- VAT fraud by reducing fraud relating to missing traders, repayment, and reducing the shadow economy and contrived insolvency;
- excise fraud by reducing tobacco, alcohol, oil, and money smuggling;
- public services fraud for the Department of Work and Pensions by reducing residency fraud losses;
- financial fraud by preventing account takeover fraud, credit card application fraud, and reducing banking losses due to ID fraud.[20]

We have previously shown that it is impossible for identity cards to prevent much of this fraud, or at least not in a cost-effective way.

As we stated in our first report, most of what is commonly understood as 'identity theft' would not be prevented by the identity card. Our chapter on identity fraud[21] remains unchallenged by the Government and was cited at length in Parliament. Despite our detailed clarification of the Home Office figures, the department continues to erroneously claim that the card will help prevent the alleged £1.3bn worth of identity fraud per year.

Despite our detailed clarification of the Home Office figures, the department continues to erroneously claim that the card will help prevent the alleged £1.3bn worth of identity fraud per year.

Indeed, reliance upon identity authentication as the means to prevent identity fraud may not be the best way forward. For instance, Callum McCarthy, Chairman of the Financial Services Authority addressed this issue with regard to financial identity fraud, claiming that the FSA were 'Defusing the ID issue':

> "We have given – repeatedly and I hope clearly – the message that we expect firms to manage their money laundering risks effectively by placing less emphasis on ID and using the full range of [Anti-Money Laundering] tools."[22]

This statement follows from a criticism made by the Better Regulation Task Force, referring to the increased identification requirements as 'creeping regulation'.

---

20 From Annex A of 'Identity Cards Scheme - Benefits Overview, Home Office, June 2005.

21 Chapter 8, pp. 97-111.

22 Speech by Callum McCarthy, Chairman, FSA, The Congress Centre, 15 November, 2005 http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2005/1115_cm.shtml.

> "Last year many of us found our banks writing to us to ask for proof of our identity, even when we had held accounts with them for many years. It's unclear where this requirement came from, and this is one of the examples that we will be investigating in our study on regulatory creep."[23]

In fact the Better Regulation Task Force has repeatedly drawn attention to the poorly formed presentation of the case for identity checks[24]that would introduce an additional layer of red tape.[25]

The over-reliance on ID may not be ideal and is even being de-emphasised. Yet the Home Office insists that ID cards "will have a significant impact upon money laundered and a corresponding impact on criminal activities within the UK."[26]

ID requirements may actually make matters worse. Despite continuing warnings from industry and security experts, the Government insists that centralising all personal information in the National Identity Register (NIR) is the best way to protect an individual's identity.

It has been argued that the risk of identity fraud appears to increase as data that is stored centrally. There are even claims that Chip and PIN technology could make matters worse. According to Dr. Emily Finch, a researcher at the University of East Anglia, with Chip and PIN checkout staff in shops are less vigilant about transactions – an unfortunate situation that is being criminally exploited.[27] Chip and PIN serves more to change the balance of liability for fraudulent transactions, even as security problems remain[28]. This makes a stark similarity to the proposed Identity Cards scheme.

Other new developments include warnings of organised crime infiltrating leading banks in order to commit fraud.[29] The tactic, confirmed by police, involves gangs bribing staff to pass over confidential information. In another case, there was recent alarm about criminal gangs making fraudulent claims using the identities of Department of Work and Pensions staff.[30] The most recent case of lax security leading to potential identity theft involves thousands of credit card numbers, addresses, phone numbers, passport numbers of hotel guests found in a skip outside the Grand Hotel in Brighton.[31] In these cases it is hard to see how ID cards would reduce the scale of identity theft.

Such concerns may be over-emphasised. Recent research hints that the large breaches of personal information lead to very few thefts of identity. According to one firm, ID Analytics Inc., small data breaches

---

23 'Task Force Targets "Creeping Regulation"', Better Regulation Task Force, March 4, 2004.

24 c.f. Parliamentary Library Research Paper 05/43, June 13, 2005, 'The Identity Cards Bill', p.20.

25 'ID cards will hit business, watchdog warns', John Oates, The Register, December 3, 2004.

26 'Identity Cards Scheme - Benefits Overview, Home Office, June 2005, p.3.

27 'Chip and PIN blamed for making ID theft easier', Andy McCue, Silicon.com, September 5, 2005.

28 c.f. 'Chip and Spin', Ross Anderson, Mike Bond and Stephen J. Murdoch, University of Cambridge, September 2005.

29 'Warning over 'mafia' gangs infiltrating British banks', Patrick Hosking and Stewart Tendler, The Times, November 16, 2005.

30 DWP staff hit by online tax fraud', ePolitix.com, December 13, 2005 and 'Tax credit gangs 'may have defrauded millions'', Andrew Woodcock, The Independent, December 13, 2005.

31 'Risk of ID theft bonanza as thousands of credit card slips found dumped in skip', Miles Brignall and Philip Inman, The Guardian, January 9, 2006.

tend to focus more carefully on personal information that pose the greatest potential for harm to business and consumers. The latter category of attacks are used for identity theft.[32] Research from another firm, the Perpetuity Group, states that identity theft could be reduced better if UK consumers were given a free copy of their credit rating every year, as is being proposed in the U.S.[33] Giving individuals access to the means of discovering whether or not they are being impersonated is one of the most powerful means of combating this form of fraud.

> ID requirements may actually make matters worse. Despite continuing warnings from industry and security experts, the Government insists that centralising all personal information in the National Identity Register (NIR) is the best way to protect an individual's identity.

The Home Office continues to ignore sound expert advice on the risks inherent in a centralised repository of data. It has become obsessed with arguing that the technology can be made secure but has failed to grasp the simple fact that human error and criminality in a centralised system can create the gravest security threats.

Security of the system

The security of the NIR is therefore of the utmost concern. In our first report we described the nature of these risks and proposed that a more secure solution would involve a distributed model, where instead of a large centralised data store of all biometrics, the personal data of UK residents should be kept in a decentralised fashion.[34] Such a 'federated' model is the model of choice by industry.

This 'federated' approach is also the traditional design of choice in the UK Government. Personal information is kept on a number of different databases for different purposes. The Information Commissioner's Office has stated that the UK had over 40 different population registers in the public sector, ranging from tax systems, DVLA, NI, passports, etc. The power of redundancy is that when the NI databases failed a few years ago it did not bring the country to a stand-still. Arguably there is a case for some rationalisation of these systems however a significant move to centralisation carries risks.

According to Microsoft UK's National Technology Officer, Jerry Fishenden, the ID card scheme could in fact trigger "massive identity fraud on a scale beyond anything we have seen before." He warned against the central storage of biometrics because the compromising of such information would lead to the impossible scenario of having to provide new ones. He thus warned that we "should not be building systems that allow hackers to mine information so easily... Inappropriate technology design could provide new hi-tech ways of perpetrating massive identity fraud on a scale beyond anything we have seen before: the very

32 'Exploiting stolen data is a slow business', Outlaw News, Pinsent Masons, December 12, 2005.

33 'Identity Theft and Fraud: Learning from the USA', Perpetuity Research and Consultancy International, August 2005, http://www.perpetuitygroup.com/prci/acatalog/identitytheftandfraudreport.pdf.

34 Chapter 14, 187-199.

problem the system was intended to prevent." This creates what Fishenden refers to as "a honeypot effect - a highly attractive and richly rewarding target for criminals."

Since many biometrics may be readily collected without the individual's consent, centralised storage is not the only problem. When the biometric data is associated with personal information there is cause for greater concern. The link between the biometrics and personal information needs to be kept highly secure so as to prevent fraudulent use of identities.

But the centrality of all this data is part of the Home Office's design to pursue a largely illusory goal that the documents cannot be forged. Following claims from the ex-MI5 chief Dame Stella Rimington that since most documents could be forged then ID cards were 'useless', Minister Andy Burnham stated that the cards would be 'almost impossible to forge'. Dame Stella was quoted saying that although ID cards have some possible purpose, "[b]ut I don't think that anybody in the intelligence services, particularly in my former service, would be pressing for ID cards. My angle on ID cards is that they may be of some use but only if they can be made unforgeable - and all our other documentation is quite easy to forge. (...) If we have ID cards at vast expense and people can go into a back room and forge them they are going to be absolutely useless."

Even as cards are promised to be more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices.

A forged card succeeds whenever a relying party is convinced of the data it provides. This is achieved most easily under 'flash-and-go' regimes where the cards are not scrutinised to compare the individual presenting the card with the data on the card (e.g. photo). Even as cards are promised to be more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices.[35]

A central database may go some distance to ensure that issued cards are accurate and are not stolen, provided that coercion is not used and the database of invalid cards is accurate, but the costs of running such a system are likely to be prohibitively high. Only recently have countries began sharing lists of stolen and lost passports. But the Home Office statements regarding on-line verifications remains ambiguous: when challenged on forgeability, they claim or imply that all or many verifications will be done against the database, but at other times they contend that the cards will be used only as 'photo-ID', estimating only relatively few verifications against the database per card per year.

35 'Russia busts fake Kremlin ID gang', BBC, December 6, 2005.

Any system that involves significant networking with the outside world, including the 44,000 possible private sector users and the 260+ government departments[36] will have security weaknesses. There will be countless 'users' of the system who will have to be authorised to enter and change data on the register, including passport clerks at embassies around the world, employees at call centres and at the enrolment centres, to name but a few. Whether through technological means or through 'inside jobs', systems can be compromised. Yet the Government insists that this centralised solution is necessary. In fact, the Home Secretary justified the creation of a central database and a data trail of all human activity on the basis that it will prevent theft and abuse of this information.[37] Such measures have not stopped persistent abuse of the facilities of the Police National Computer, as there have been a litany of prosecutions for improper extraction of data by police staff. The cases include obtaining information for former colleagues who are now private investigators and tracking the registration information of a car parked outside their ex-spouse's home.

More recent developments cause even greater concern. The Government has recently promoted the idea of access to the Register for telephone checks if someone is not carrying their card. If such a PIN-like system is to be implemented, it will be possible to compromise these PINs.[38] This could lead to a pool of thousands of stolen PINs and IDs available to criminals/terrorists at any particular time. If there isn't to be such a PIN, however, then the public will likely protest because they will be required to either carry their card at all times or be denied services.

In trying to make the system more convenient so late in the design process - in an attempt perhaps to avoid denial of services to those who choose not to carry their card around with them at all times, or who have forgotten them – the Government appear to be building in significant security risks.

The Home Office system involves a dangerous 'Catch-22'. If changes and verifications to the NIR are not based on a biometric, further problems will follow. For instance, if individuals want access to their audit trails on the NIR, it is proposed that they could request it via a web-interface. However, this would enable identity theft and spying. If a malicious hacker wished to gain access to the map of a person's personal life, he could

1. Change her address on the NIR through various methods, e.g. social engineering, phishing.
2. File a subject access request for data on the NIR, including the log of all accesses, e.g. the list of all times her data was verified by government agencies and private sector companies. This audit trail will be sent to the new address.

As a result, the malicious hacker can have a listing of all the official transactions concerning that individual over time.

---

36 As stated in the Home Office presentation to industry, 'Procurement Strategy Market Soundings', Identity Cards Programme, Home Office, October 2005, http://www.identitycards.gov.uk/library/procurement_strategy_market_soundings.pdf.

37 Hansard, House of Commons, June 28, 2005, column 1153.

38 in techniques called 'phishing', by cold calling, spam, or websites.

Policing and ID

The use of identity cards is likely to shift the culture of policing in Britain. Our arguments on the effects that the card would have on policing have not changed. We showed that despite the claims from the Home Office that the cards will neither be compulsory to carry, nor demanded for stop and search purposes, since the publication of our report there have been repeated statements from the Association of Chief of Police Officers regarding their desire for the ID card scheme to become compulsory as soon as possible. Police organisations have repeatedly stated their hope that identity cards will 'improve' the stop and search process. And now with indications that the Register will also act as a national fingerprint database for policing purpose, this will indeed, in the words of the House of Lords Constitution Committee, cause a significant change in the constitutional relationship between the citizen and the State.[39]

On the day of Second Reading in the House of Commons the Government released a 'Benefits Overview' document outlining the strategic benefits, quantifiable benefits, and the non-quantifiable benefits of the Identity Card Bill. Among the claims here was one that the Card would allow more efficient policing.

Amongst the many arguments, the Home Office argued that there would be a reduction in the cost of crimes by enabling

- simpler fine recovery
- greater victim support (e.g. identifying the injured or deceased)
- more emotional and physical impact support (e.g. tracing missing people, identifying vulnerable and deceased people)
- efficient administration of insurance
- increased confidence of data on police databases

Crime prevention would be enabled by

- fingerprint matching up to 900,000 fingerprints collected at scenes of crime
- greater child protection measures through verifications by the criminal records bureau
- better security of identities in traffic offences.

And improved crime detection benefiting

- the citizen, as he can better conduct police document checks
- stop and search powers.[40]

Permitting police to access the fingerprints on the register, to compare them with fingerprints left at crime scenes and for intelligence purposes, is estimated to allow an increase to detection rates of between 1,900

39 Report on the Identity Cards Bill, House of Lords Select Committee on the Constitution, 3rd Report of Session 2005-06, published October 24, 2005.

40 'Identity Cards Scheme - Benefits Overview, Home Office, June 2005.

to 17,000.[41] The document also predicts that the scheme will improve intelligence gathering by "providing fast, reliable access to information on intelligence targets."[42] There are no clarifications on these points and they have not been part of the public debates.

However, by implication, this means that the police will be comparing crime scene fingerprints with those of all citizens, on the presumption that some are guilty of the crime. Moreover, given the problems with obtaining clean prints from crime scenes and the likely storage of biometric prints in template form, this mechanism is likely to lead to numbers of individuals being considered as possible matches to the crime scene prints rather than having the crime scene prints immediately and uniquely identify the particular criminal.

Our argument still stands, however, that the Home Office is designing an ID card in an unprecedented manner in order to make it a crime-fighting tool, rather than creating an infrastructure that will promote public trust.

Our argument still stands, however, that the Home Office is designing an ID card in an unprecedented manner in order to make it a crime-fighting tool, rather than creating an infrastructure that will promote public trust. The collection of fingerprints is not essential to the proper administration of an identity system, and this is why so few countries around the world actually practice it. But the Home Office intends to design Britain's identity card in the Home Office's image: a centralised database of biometric data available to the police. As we previously argued, technology transforms the relationship between the police and the public. The Joint Committee on Human Rights recently repeated their concerns that the extensive collection and retention of personal information may interfere with Article 8 rights.[43] The Home Office still refuses to consider these issues in detail.

Race, Immigration and Discrimination

Our commentary on the possible effects of the cards on race, immigration and discrimination still stands. Any analysis on these matters are affected by the ramifications of the July 7th attacks on London, particularly as a number of communities voice concerns about being disproportionately targeted for ID checks.

These concerns are supported by perhaps portentous information from France. There have been claims arising from the recent Paris riots that continual ID checks caused increased friction between the police and minority groups. Earlier riots in Paris were caused when young people were running away from police because they feared ID checks. Meanwhile in the Netherlands over 50,000 individuals have been fined over a nine-month period for not carrying ID: 4,000 of these fines were applied to children between 14 and 15.

41 'Identity Cards Scheme - Benefits Overview, Home Office, June 2005. p.14.

42 ibid.

43 Joint Committee on Human Rights, First Report of Session 2005-06.

After the London bombings there was much discussion of stop and search powers and racial profiling. The head of the British Transport Police was quoted as saying "we should not waste time searching old white ladies." The Minister of State for Policing, Security and Community Safety stepped forward to support that approach, on the condition that it was based on intelligence:

> "That's absolutely the right thing for the police to do. What it means is if your intelligence in a particular area tells you that you're looking for somebody of a particular description, perhaps with particular clothing on, then clearly you're going to exercise that power in that way. (...) I think most ordinary decent people will entirely accept that in terms of their own safety and security. (...) Clearly if we are looking for people and being operationally efficient, we have got to target the people who we think are maybe involved. (...) It is going to be disproportionate. It is going to be young men, not exclusively, but it may be disproportionate when it comes to ethnic groups. We are very sensitive to the effects that that can have and it isn't an attack on particular communities."[44]

The Minister, Hazel Blears, later clarified her statement. She argued that officers needed to explain to communities that controversial stop-and-search operations were intelligence-led; racial profiling, she said, was something she had "never, ever" endorsed.[45] If used in an intelligence-led manner, she argued that the power would be "used proportionally, fairly, and in a non-discriminatory way."[46]

There have been claims arising from the recent Paris riots that continual ID checks caused increased friction between the police and minority groups.

Parallels can be drawn with recent data emerging on the accumulation of DNA profiles in the National DNA Database. The database now holds 3 million profiles of individuals, and this number is likely to increase to 4.2 million within two years because of changes in laws that permit police to retain the DNA profiles of even those who are not charged with a crime and those who are acquitted. The database currently consists of 140,000 profiles of people whose DNA was taken on arrest but who were subsequently not charged.[47] In 2004 and 2005 alone, 230,000 juveniles were added to the databases. According to one analysis, 37% of black men have their DNA profile in the database, compared to 13% of Asian men and 9% of white men.[48] These statistics demonstrate once again the extent to which technology acts to alter the relationship between the citizen and the state, whilst simultaneously exemplifying the use of technology to indirectly enshrine racial discrimination and racial divides.

---

44 "Searches to target ethnic groups", BBC Online, July 31, 2005.

45 'Blears backs away from racial profiling, Mark Oliver and agencies, Tuesday August 2, 2005, Guardian Unlimited.

46 'Blears says Muslims should not fear racial profiling', Daily Telegraph, August 2, 2005.

47 'Huge rise in juvenile DNA samples kept by the police', Philip Johnston, The Daily Telegraph, January 9, 2006.

48 'DNA of 37% of black men held by police', James Randerson, The Guardian, January 5, 2006.

Public Trust and Opinion

In our earlier report we showed that while there have been a number of consultation processes regarding the entitlement and identity card proposals, the Home Office has hardly listened to any of the responses. The ID system proposal as it now stands is nearly identical to the one proposed more than three years ago. The Home Office has been unwilling to listen to expert opinion or take into account critical views.

The situation is similar on public opinion. In Chapter 11 of our earlier report[49] we postulated that public support would drop as the public learned more about the proposed system. This has occurred.

The Home Office continues to cite 73-83% support for the identity card proposal even though those figures reflect a survey done over a year ago. A poll conducted prior to the Second Reading in June 2005 found that support was at 55% in favour and 43% opposed.[50] After the Second Reading in the House of Commons, on July 4th 2005, a Telegraph YouGov poll asked:

> "Are you in favour of or opposed to the introduction of a national system of identity cards?"

The pollster had asked a similar question in September 2003 when the support was 78%. In the July 4th poll the support had dropped to 45%, and opposition rose from 15% to 42%.[51]

The ID system proposal as it now stands is nearly identical to the one proposed more than three years ago. The Home Office has been unwilling to listen to expert opinion or take into account critical views.

After the terrorist attacks on London on July 7th support for the card did rise and opposition dropped. According to a Telegraph YouGov poll conducted on July 8th, support for the card in the aftermath of the bombings rose by 5% and opposition dropped by 4%.[52]

Although it is arguable that much of the loss of support for the proposal can be based on public discussion and speculation on the costs of the card, a poll conducted in November 2005 by ICM Research asked questions based on the Government's own costings:

> "The Government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a: Very Good Idea, Good Idea, Bad Idea, Very Bad Idea?"

The results were that support for the proposal was still at 50% and opposition at 48%.[53]

---

49 pp. 139-144.

50 ID Card Survey prepared by ICM Research on behalf of NO2ID, June 10th-12th 2005.

51 Telegraph, published July 4, 2005.

52 Telegraph, published July 9, 2005.

53 ID Card Survey prepared by ICM Research on behalf of NO2ID, November 18-20, 2005.

These results differ starkly from a study that was commissioned by the Home Office.[54] The study involved two groups: UK citizens, argued to be 'representative' but with no BME breakdown, and 'Identity Service Users', i.e. firms and agencies who would undertake identity checks. Originally conducted during January to March 2005, due to the terrorist attacks in London the Home Office 'found it necessary to ensure that the research findings are still relevant and reflect the current public opinion.' They found that support for the card was 73% with only 17% in opposition.

Running the same questionnaire on just 250 respondents, they found that support for the card was still at 73% with only 17% in opposition. No major polling organisation would consider this a statistically significant sample, and achieving an identical response over 6 months later – especially in the light of the shifts in every other poll conducted over the same period - must call into question both the methodology of the survey and the Home Office's reliance upon its aberrant results.

The Home Office research only permitted individuals to entertain 'what-if situations' rather than asking respondents to rate or rank them, or even asking an up or down answer to a question regarding acceptance to proposals. This is a tool used in the marketing world to determine how individuals choose preferred products from a wider group of products. Therefore the form of analysis chosen measures potential demand but not satisfaction with the concept. That is, according to the report:

> "Whilst citizens are prepared to take up an offer they may not regard the offer as completely satisfactory."

Support was strong and steady, according to the report. The 'base case' presented to the sample was that the price of the ID card and passport was £93, or £50 for a stand-alone passport; and individuals had to travel 45 minutes to enrolment centres and the process took 4 weeks.

> "The base case concept is generally accepted by citizens. There are few design changes that realistically can be done which will impact significantly on demand. Having evaluated the impact of changing a number of attributes few will generate more than an additional 1-2% demand."

When the costs were presented as being nil, support rose to 83%. When costs were presented at £250, 63% said that they would be prepared to take it up. Surprisingly demand for the card remained relatively static when travel times to enrolment centres were changed. Demand remained at over 75% even as the travel time was increased from 15 minutes, to 30 minutes, and 60 minutes. It dropped only 5% when distance was increased to 90 minutes. Similarly, demand remained steady when 'turn-around time' was increased from 'same day service' to 4 weeks. These are surprising results that fly in the face of all other polls: within the confines of the study, the vast majority of the public were not dissuaded through increases in costs and inconvenience.

Similarly for the 'Identity Service Users', support was very high at 84%. The 'base case' included a flat fee for on-line verification of £0.57, a 'yes/no' verification, use of card readers, phone or website for verification, 6-15 second verification response time. Demand for the 'base case' was 65%. When costs were

54 'An assessment of awareness and demand for the Identity Cards Scheme', Home Office, October 2005.

removed, greater information accessed, and efficiency was at its height, demand was 91%. When costs were high and flexibility was at a minimum, demand dropped to 42%. These users also said that they did not mind having to pay for access to the NIR, but demand fell when they were compelled to pay for card readers. When readers were priced from £250 to £350, 71% of respondents were willing to invest but their intent dropped to 51% when the price was raised to £650-£750. The report concluded that because the variance in support was 49% between most favourable and least favourable product/case, "the take up rate is likely to vary depending on the final design of the scheme."[55]

The Home Office has also argued that support for the scheme is high amongst large firms. According to reports, the Home Office has been meeting with large firms like Royal Bank of Scotland, HBOS and Tesco to see if they would make possession of ID cards a central part of their employment practices. According to an article in the Scotsman, David Lacey, the Royal Mail executive who chairs the Private Sector User Group, told The Scotsman that major employers are "enthusiastic" about ID cards.[56]

Other studies are not so enthusiastic. Industry support, according to the London Chamber of Commerce's quarterly Monitor survey[57] shows that although 83% are anxious that another terrorist attack is 'inevitable', only 37% believed that ID cards would reduce the threat of attacks. Further findings include:

- 26% of company directors believe that introducing ID cards would prove to be beneficial to their business;
- 68% believed there would be no impact;
- 45% of firms think that ID cards would make British cities safer.

This last figure is identical to those who believe that capital punishment would have the same effect, and much less than other means such as undercover police, bus conductors and stop and search powers (60%+ support).

Meanwhile an experiment conducted by the Open University looked into public trust in the proposed scheme.[58] The OU study compared the responses to the proposed-ID scheme from the Home Office with the responses to a more decentralised and voluntary system as proposed by the LSE report.[59] While 'overall' support for an identity card in theory was 52.7% with 33.4% against and 13.9% undecided, support was quite different when respondents were able to decide between systems.

- When asked about their support for the Home Office's solution with a central database and high compulsion, those in favour dropped to 30.9%.

---

55 ibid, p.47.

56 'Biggest British firms could make ID cards compulsory for staff', James Kirkup, The Scotsman, September 24, 2005.

57 "Crime, Safety and Terrorism Survey', London Chamber of Commerce and Industry, October 2005.

58 'Privacy attitudes and ID cards: An experimental comparison of alternative approaches', Adam Joinson, Carina Paine, Tom Buchanan, Ulf-Dietrich Reips, The Open University (and the University of Westminster and University of Zurich), July 19, 2005.

59 Chapter 19, p.277-295.

- When asked about their support for a system involving a database not hosted by the Home Office and low compulsion, support for the card was 46.2%.

The OU study concludes that although support for the card is theoretically above 50%, when the Home Office proposal is outlined there is a drop in support by over 20 percentage points. The drop in support for a system that is not hosted by the Home Office and that is not compulsory is only 7 percentage points. Even those who were generally not concerned with privacy issues reached their tipping point when the highly centralised and compulsory scheme being proposed by the Home Office was described to them. This concern is moderated by alternative schemes.

The OU study concludes that although support for the card is theoretically above 50%, when the Home Office proposal is outlined there is a drop in support by over 20 percentage points.

Government IT Projects

On the IT environment in the UK and project costings, we stand by our original report (chapters 15 and 16) and the concerns about the government's ability to manage large scale IT projects and deliver them successfully, on–time and within budget. The Home Office insists that it is fully capable of managing a project of this scale.[60]

The accumulated independent evidence on large complex IT projects is that they have been and always will be high risk in terms of implementation and unanticipated costs. The key risk dimensions include high complexity, large size, innovativeness of technology, integration issues, number of units and stakeholders affected, over-ambitious time-scales, and over-reliance on technologists/IT suppliers for development and implementation.[61] The Identity Cards scheme as presently proposed is in danger of incurring all these risks, with little information on how these risks could be mitigated.

The problem is even worse than this. As the Royal Academy of Engineering and the British Computer Society make clear, complex IT projects like the Identity Cards scheme inherently incur a vast number of problems, issues and consequences that cannot be anticipated.[62] Faced with this inevitability, the present proposals read as over-confident or under-detailed on costs, management of risk, the on-going testing regime and descoping and modularising development and implementation.

---

60 For example, 28 Jun 2005 : Column 1170 Mr Clarke: "All those examples demonstrate that the public sector in general, and the Home Office in particular, has the capacity to undertake such major projects."

61 Collingridge, D, (1992) The Management Of Scale, Routledge, London; Royal Academy of Engineering/British Computer Society (2003) The Challenge of Complex IT Projects, The Royal Academy of Engineering/BCS, London; Sauer, C and Willcocks, L (2001) Building The E-Business Infrastructure, Business Intelligence, London; Willcocks, L and Griffiths, C (1997) 'Management and Risk in Major IT Projects' in Willcocks, L, Feeny, D, and Islei, G (eds.) Managing IT As A Strategic Resource. McGraw Hill, Maidenhead; Willcocks, L, Petherbridge, P and Olson, N (2003) Making IT Count: Strategy, Delivery, Infrastructure. Butterworth, Oxford.

62 Royal Academy of Engineering/British Computer Society (2003) The Challenge of Complex IT Projects, The Royal Academy of Engineering/BCS, London.

In this section we will review three recent cases of problematic technology projects that illustrate the kind of problems the ID cards scheme could face, before raising broader concerns with the underlying design of the government's Identity Card infrastructure.

The problems with PAYE codes at HM Revenue and Customs highlight problems of data integration between computer systems, the NHS 'Choose and book' system shows the potential consequences that problems with one element of a system can have for the system as a whole, whilst the DWP case highlights the consequences for the more vulnerable members of society if government infrastructures do not perform correctly.

HM Revenue and Customs

In its Annual Report for 2004/5 on HM Revenue and Customs, the National Audit Office reports various software related problems that led to incorrect payments in 2004–05.[63] Of particular relevance for ID cards are the "widespread errors in PAYE". These are estimated to have "resulted in around £575 million per annum of tax due not being pursued by the Department; and that taxpayers were not being advised of around £295 million per annum potentially repayable to them".[64] Further problems with PAYE are anticipated because of "difficulties transferring data between computer systems".[65]

> As the Royal Academy of Engineering and the British Computer Society make clear, complex IT projects like the NI scheme inherently incur a vast number of problems, issues and consequences that cannot be anticipated.

NHS

The Sunday Times reported in November 2005 that a new £20 million NHS computer project that would allow people to book appointments with their GP was in grave danger of "derailing" major NHS reforms costing £6.2 billion. The 'Choose and book' project is already at least one year late and costs are expected to rise by millions.[66]

As a result of these problems, as well as general concerns about the electronic storage of patient data, a survey of 1300 doctors has revealed a crisis of confidence in the NHS reforms.[67]

63 http://www.nao.org.uk/publications/nao_reports/05-06/0506446.pdf

64 http://www.nao.org.uk/pn/05-06/0506446.htm

65 "More PAYE tax code errors feared with new computer", Alison Steed, Daily Telegraph, January 2, 2006.

66 "NHS chaos exposed by new e-mails", Jonathon Carr-Brown, The Sunday Times, November 13, 2005]. Amongst the reasons given for the problems were repeated last–minute changes and "problems linking hospitals' and GPs' computers" http://news.bbc.co.uk/1/hi/health/4396256.stm.

67 Doctors have little faith in new NHS £6bn computer system', John Carvel, The Guardian, January 10, 2006.

Department of Work and Pensions

Problems with a call–centre system operated by EDS meant that one in three benefit claimants who telephoned a new computerised system was unable to get through. Mark Serwotka, general secretary of the Public and Commercial Services Union (PCS) said of these problems:

> "This is categorical proof that not only do the computers not work, but that when you force vulnerable people to go through call centres to access the benefits system, if there are not enough staff and computers don't work, one million people have tried to get through and can't."[68]

Earlier that week, EDS had agreed to pay HM Revenue & Customs £71m in compensation for the poor performance of its tax credits IT system.

The proposed information infrastructure

A key problem that we faced with evaluating the government's technological specifications for the ID cards scheme is that little is known about the specifics of the proposed system and, rather worryingly, new indications have emerged on a regular basis in recent months about how the system might function. For example, Andy Burnham has suggested that simple PIN controls could be used to allow people to check their details on the NIR, whilst at other times he has suggested the use of "one-time password" technology.[69] As far as we are aware, neither of these technologies have appeared in Home Office market sounding documents.

A key problem that we faced with evaluating the government's technological specifications for the ID cards scheme is that little is known about the specifics of the proposed system and, rather worryingly, new indications have emerged on a regular basis in recent months about how the system might function.

In some cases, we have been able to obtain clarification about what the government intends to do, in terms of technology, and we have incorporated this revised understanding in our work. For example, a key part of the enrolment process for the new scheme involves the checking of the biographical footprint of individuals submitting their biometrics. We had initially understood that this process would be a largely manual process, and costed it accordingly in our initial report[70] at between £10 and £20 per enrolment.[71] We now understand from the Home Office that this process is intended to be largely automated, and

68 'Third of benefit calls unanswered', BBC, November 25, 2005.

69 http://www.theregister.co.uk/2005/12/09/id_card_authentication_plans/

70 p. 229.

71 p. 243.

whilst we have further concerns about the practicalities of successfully automating this process, we reduce this cost element in part.

In order to obtain a sense of the likely form of the ID cards infrastructure we have had to rely heavily on information that has been made available via commercial soundings by the Home Office. For example, in October 2005, the Home Office undertook a procurement strategy market soundings exercise.[72] This sought to obtain information that would "help run an effective and efficient procurement programme".[73]

Although the market soundings documentation pointed out that until the Bill had received its Royal Assent no details were finalised, it did provide some informative indications as to the likely shape of the proposed system. This included: the establishment of a new agency[74] and the need for two secure data centres.[75]

According to these documents, the government expects the system to hold up to 100 million registration records in the NIR, with each record updated at least once every ten years.[76] . The current forecasts for identity verification transactions are expected to rise to 163 million per year (an average of 4 verifications per person per year) with "265 government departments and as many as 44,000 private sector organisations accredited" (i.e. formally authorised by the New Agency) to request such verifications.[77]

In December 2005, the Government presented some of the industry feedback including the statement that

> "many biometrics suppliers have limited manufacturing capacity or rely heavily on smaller partners with such constraints"

and that

> "capacity issues may arise if a leading edge biometric device is selected since its production would take longer than established devices. This is possible due to constant improvement in biometrics device technology."[78]

The Government also noted feedback in terms of expected increases in both speed and accuracy for biometrics, and elsewhere they note "this makes it dangerous to predict reader costs, although the scheme does take a view on all of these types of sensors."[79] .

---

72 http://www.identitycards.gov.uk/commercial/procurement-strategy.html

73 http://www.identitycards.gov.uk/library/procurement_strategy_market_soundings.pdf slide 6

74 http://www.identitycards.gov.uk/library/procurement_strategy_market_soundings.pdf slide 8

75 http://www.identitycards.gov.uk/library/Procurement_Strategy_Questionnaire.doc page 10

76 http://www.identitycards.gov.uk/library/Procurement_Strategy_Questionnaire.doc page 11.

77 http://www.identitycards.gov.uk/library/procurement_strategy_market_soundings.pdf page 13.

78 Procurement Strategy Market Soundings, Identity Cards Programme, Home Office, December 2005, Page 6
http://www.identitycards.gov.uk/library/Procurement_Strategy_Market_Soundings_Update-December-2005.pdf

79 http://www.identitycards.gov.uk/library/2005-12-20_IDENTITY-MATTERS-FOR-STAKEHOLDERS-NEWSLETTER.pdf page 5.

Other practical concerns were raised in the published extract of the KPMG cost methodology and cost review[80] which noted that there were few available locations for the proposed data centres and the new building time-scale is typically three years, whereas the Home Office's plans requires them to be available in two years' time.

From the large number of government agencies and commercial organisations that are expected to make use of the ID system, it is clear that the ID card scheme is not intended to be considered as a stand–alone system, but rather that it is best conceptualised as part of a government managed infrastructure providing identity checking services. Academic research on large scale information infrastructures[81] suggests that managing such infrastructures is often problematic. In particular, it raises serious questions about the Home Office's notion that "decisions on whether, when and how particular public services will make use of the ID cards scheme will be made by those services—individually or collectively as appropriate depending on how services are managed".[82] Infrastructures often constrain such decisions in unexpected ways.

The logic behind providing a single, government managed, identity verification infrastructure is easy to understand. Many government agencies currently need to verify the identity of the individuals with whom it has dealings. At the present time, each government service has its own ways of verifying the identity of individuals, with each method having different levels of quality, and the government clearly sees benefits with providing a single, high quality identity verification service.[83]

A further issue arises, however, with the question of how the details of the individual are stored in computer systems once they have been identified. For example, a National Audit Office report on the design of forms, describing the forms used to apply for attendance allowance, notes:

> "Much of the first 13 pages of the current application asks people to list existing ways in which they have a relationship with the Department for Work and Pensions. Applicants have to re–provide all this information, which should be known to DWP, because the departments could not easily look across all its different IT systems processing different benefits so as to get a synoptic picture."[84]

This statement, written before the ID card scheme was introduced to Parliament, continues with the description of a new Departmental Central Index or 'spine' system that uses the National Insurance number to identify individuals uniquely.

---

80 http://www.identitycards.gov.uk/library/2005-11-7_KPMG_Review_of_ID_Cards_Methodology.pdf

81 for example Ciborra Claudio and associates (2000), From control to drift: The dynamics of corporate information infrastructures, Oxford University Press, Oxford. Also, Sauer, C. and Willcocks, L. (2001) Building The E-Business Infrastructure, Business Intelligence, London.

82 Letter from Andy Burnham to Professor Ian Angell, November 23, 2005, http://www.identitycards.gov.uk/library/2005-11-23%20mm%20burnham-angell-public-sector-use-and-implementation-of-ID-cards-HB.pdf

83 http://www.identitycards.gov.uk/library/2005-06-27_Identity_Cards_Scheme_Benefits_Overview.pdf

84 NAO. (2003). Difficult forms: How Government agencies interact with citizens (No. HC 1145). page 23, box 2.

This example nicely illustrates both the proposed benefits and inherent costs and uncertainties associated with introducing a new information infrastructure. The logic of a single identification system that is 'virtually' foolproof is clear, because it ties the unique biometrics of an individual to a unique identification number (the NIRN) that would allow all government bodies to index the information held on that person to that (NIRN) number.

It also, however, highlights some of the practical management issues associated with the use of the proposed information infrastructure. To use the DWP example, considerable time and money has just been spent on creating the new Departmental Central Index that stores details on individuals according to their National Insurance number (NINO). As a result, all the systems that use the central index will not be able to switch across to using the NIRN without further expenditure. Moreover, during the periods of transition (from using the NINO in the Central Index to using the NIRN in the central index, and from using the NINO for those who do not have an ID card and the NIRN for those who do) there will need to be two systems in existence, with two sets of processes for handling identification and data matching. There are also likely to be complex issues associated with tidying up the data in terms of matching records that are indexed by NINO to those that are indexed by the NIRN.

Further problems can be predicted, based on written evidence to the Public Administration Select Committee by Professor Patrick Dunleavy, who notes that the Inland Revenue (now HMRC) encouraged taxpayers to use an IR–specific taxpayer number rather than National Insurance numbers that they had to pay to use.[85]

As we argued in our previous report and presented in the 'alternative scheme',[86] departments and agencies have their own unique identifiers for each record because that numbering system is best for their systems, processes and policies. Introducing a new uniform numbering system is not only going to be costly but also burdensome and most likely unnecessary.

Such problems are typical of most large scale information infrastructures and these are described in more detail below.

...departments and agencies have their own unique identifiers for each record because that numbering system is best for their systems, processes and policies. Introducing a new uniform numbering system is not only going to be costly but burdensome and most likely unnecessary.

Characteristics of information infrastructures

Information infrastructures are generally understood to consist of standardized systems and data, as well as formal communications mechanisms. They are often classified according to their reach and scope in terms of the number of activities they support and the type and variety of activities supported.

85 http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDCard_Nov05WrittenEvidence.pdf

86 Chapters 18 and 19.

Infrastructures can be classified in terms of providing a utility, a dependence or as enabling services. Utility infrastructures typically aim to reduce the cost of processing and communicating information, often taking advantage of economies of scale. They are designed not to interfere with applications and business processes. Dependence infrastructures allow for new applications to be launched across the infrastructure and so enable new processes to take place. Finally, enabling infrastructures are intended to provide as much flexibility for future expansion and use as possible.

The provision of telephone cabling, water and sewage supplies or a common log–on screen for computer systems are all examples of utility type infrastructures. Dependence infrastructures may include the introduction of groupware technologies or e–mail into an organisation, whilst the installation of internetworking is a common example of a flexible infrastructure as it allows many different activities (web browsing, e–mail, voice over IP) to take place over the same infrastructure.

It is apparent that an information infrastructure deals with questions of universal use and access, and as such requires high levels of standardisation from all potential users of the system.[87] Interoperability between systems is required and this has implications for the flexibility, resilience and security of the system. Infrastructures must also be able to cope with the dual constraints of local variety and centralised planning.

Issues of standardisation and interoperability in the case of the ID card scheme mean that if a government department is intending to use the information infrastructure to verify identity using biometrics (i.e. for situations that require a higher level of service than simply visual inspection or PIN based confirmation), they will need to provide the full range of biometric readers (fingerprints, face recognition and iris scanning) to ensure that biometrics could be captured for verification. Moreover, if these biometrics are to be compared against the central register, the quality of the biometrics obtained must be of the same standard as those collected during the registration process.

Evidence from the U.S. National Institute of Science and Technology has reported that many of the problems with misidentification of biometrics can be attributed to "lower operational quality controls" during the collection process.[88] This requires a combination of biometric readers of a similar standard to those used during the registration process, plus trained staff who are able to use the equipment properly.

Less straightforward aspects of infrastructures include the fact that they are effectively embedded into the systems that use them, and this raises important questions of transparency and reach. Infrastructures rapidly become linked to conventions of practice and effectively become a learned part of membership of an organisation that uses an infrastructure.

For example, as organisations become increasingly dependent on their e–mail infrastructure, it becomes routine for colleagues to e–mail each other rather than to telephone one another, newcomers quickly learn who can be relied upon to respond to e–mails promptly and organisational performance can be seriously hampered if this infrastructure is temporarily unavailable.

---

87 Ciborra, C., & associates. (2000). From control to drift: The dynamics of corporate information infrastructures. Oxford: Oxford University Press. Chapter 2.

88 NIST. (2005). The Myth of Goats: How many people have fingerprints that are hard to match? (No. NISTIR 7271). Archived at http://www.itl.nist.gov/iad/894.03/pact/ir_7271.pdf

Another key but not immediately apparent feature of infrastructures is that they are always built on an installed base, on the basis of what existed previously. Infrastructures are never built from scratch and they can never be changed all in one go. At a trivial level, switch over is always going to take a finite time and, for most systems, the introduction of a new infrastructure will be phased over a period of months or even years, as new equipment and processes are introduced, with associated periods of retraining and organisational adjustment.

This means that any infrastructure development project will never cover the whole of the infrastructure, but rather will need to be developed in conjunction with the constraints arising from existing aspects of the infrastructure. It is, therefore, very difficult to determine in advance what the boundaries of the infrastructure will be. Similarly, it is not straightforward to determine which parts of an infrastructure can be dropped once replacement elements have been introduced. There are many examples of infrastructure code that contain elements that have been superseded but which remain in place because of the desire not to affect other code that is successfully running.[89]

There are also examples of this problem in government projects. For example, the NAO report on the cancelled benefits card project notes:

> "This project initially proceeded on the basis of proposals from bidders that it would involve mainly the integration of existing software packages. In the event, the greater than expected complexity of the service requirement obliged Pathway to develop much more new software than they had planned. The Department's view is that Pathway knew what was required but had intended to fit the requirement to match a system they had already implemented in Eire. The extent of new software development had major implications for the degree of difficulty of the project, since this a high–risk activity with high failure rates, especially in large organisations."[90]

Information infrastructures also raise a number of economic issues that have been studied in the literature on the economics of standards and network infrastructures. One key question, which is faced by the Identity Card scheme, is how to charge for use of the infrastructure.

It would appear that the Home Office is planning to charge organisations for use of the verification service. It is not clear, however, whether these charges would be based on full cost accounting of all elements of the infrastructure. For example, should user departments simply pay for the provision of the act of verifying a particular identity, or should they also contribute towards the ongoing maintenance of the system from which they receive these indirect benefits? And should such contributions also include the process of enrolment into the system, or this cost to be solely associated with the individual who obtains the ID card, or new, more secure passport?

---

89 For an example of this see Hosein, I., Tsiavos, P., & Whitley, E. A. (2003). Regulating Architecture and Architectures of Regulation: Contributions from Information Systems. International Review of Computing Law and Technology, 17(1), 85-97.

90 NAO. (2000). The cancellation of the Benefits Payment Card project (No. HC 857). Archived at http://www.nao.org.uk/publications/nao_reports/9900857.pdf note 24 page 9.

If, as the government expects, the ID card infrastructure becomes increasingly widely used further issues of costing arise. Should the cost of use be fixed over time, or would the first departments to use the service be expected to pay a higher average cost than departments using the infrastructure once it has become an installed base? That is, if there is 1 department using the system then the cost is split over the Home Office +1 department; if there are 100 departments using the system then the fixed cost is split over Home Office + 100.

Another risk with large infrastructures is that once they become established, issues of path dependency kick in, with self–reinforcing mechanisms preventing often much needed change from arising. Thus airports are often located on the basis, in part, of existing road and rail infrastructures; the inefficient QWERTY keyboard layout is retained despite being designed to slow down the process of typing.

This means that once the ID card infrastructure is initialised, unless it is very carefully designed and black-boxed, it will be increasingly difficult to make changes to it as new biometric technologies become available.

As a result, most key decisions about information infrastructures have to be taken at times when knowledge about the factors that are affecting the decision are least known. Similarly, there is often a limited period of time when such decisions can be taken.

A further problem with any information infrastructure is the problem of 'angry orphans'. These are the functions that, inevitably, will be left behind as the new infrastructure is introduced. They may not be able to use the new infrastructure until their own systems and processes have been updated, or may not feel the need to use the new infrastructure as their existing infrastructure is performing perfectly well for their requirements.

Angry orphans can disrupt the successful implementation of an infrastructure. For example, suppose a high profile department such as the DWP evaluates the benefits of using the ID card infrastructure in addressing identity fraud (according to the Home Office, this is estimated at £20–£50 million p.a.)[91] against the costs of implementing the infrastructure outside its existing technology upgrade process (having, for example, recently invested heavily in the Departmental Central Index outlined above) and decides not to take up the ID card scheme immediately. Their lack of take up would be likely to affect the take up decisions by other departments as well, who might have a clearer case for their own use of the scheme but who are worried by the DWP decision.

Whilst the government could hope that best practice guidance by, for example, the Office of Government Commerce, would help encourage all Departments to switch to the ID card scheme, there is considerable evidence that such best practice does not always succeed in being diffused across government successfully.[92]

91 http://www.identitycards.gov.uk/library/2005-06-27_Identity_Cards_Scheme_Benefits_Overview.pdf page 8.

92 NAO. (2002/3). Purchasing and Managing Software Licences (No. HC579).

Biometrics

Our survey of the landscape of biometric technologies and implementations were presented in Chapter 13[93]. The responses to this chapter varied from appreciation for explaining in simpler terms the implications of biometrics, to rage over some omissions and misunderstandings – actual or alleged. The Home Office has reported that Dr. John Daugman of Cambridge University has pointed to a confusion between elements of retina and iris scanning in our report. However this fault had only appeared in our draft interim report and was corrected, and as a result was not part of the final report released in June 2005.

We would like to thank the Home Office for identifying a mistake that was made in one figure: we conducted an erroneous calculation on the number of individuals who would be excluded by the collection of biometrics. On page 183 we incorrectly reported that based on the results of the UK Passport Service trial 850,000 people would be unable to participate in a biometric scheme. In fact, 22,500 people would not be able to register any of their biometrics into the National Identity Register. We regret this error but would highlight the obvious fact that the equivalent of the population of a small city will be unable to participate in any way in the proposed ID scheme.

...the equivalent of the population of a small city will be unable to participate in any way in the proposed ID scheme.

Otherwise, we stand by this chapter. Our research has been further validated by more recent evidence. Though the Home Office criticises our research by citing studies (that we had already included in our chapter) that say biometrics are functional and are stable for 10 years and thus do not require renewal, we stand by other reputable studies establishing that biometric system implementations may be less certain and in need of more frequent updating. In 2002 the U.S. General Accounting Office[94] stated that "the performance of facial, fingerprint and iris recognition is unknown for systems as large as a biometric visa system".[95] The very report that the Home Office uses to refute our statements does say, on the use of biometrics, that:

> "Not only would it be one of the largest deployments to date, but aspects of its performance would be far more demanding than those of similarly sized systems; such existing systems are either not applied in the civil sector, or operate in countries where public acceptability issues are less prominent."[96]

We find the Home Office's statements of absolute certainty in the technology quite puzzling.

Our concerns about the effectiveness of biometric identification meant that we were not surprised to hear of problems with the trials where people with brown eyes, balding men, and labourers might be in-

93 pp.169-186.

94 now the 'Government Accountability Office'

95 'Using Biometrics for Border Security', GAO, November 2002.

96 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', for UKPS, DVLA, and the Home Office, by Tony Mansfield and Marek Rejman-Greene, February 2003.

correctly identified by biometric systems.[97]. We were, however, surprised to hear these problems announced by the Home Office Minister Tony McNulty, because just months earlier Mr. McNulty was heralding the results of the UK Passport Service trial, saying that:

> "Once we get onto the procurement process and delivery neither the government nor the IT sector will be found wanting."[98]

and

> "I'm confident of the robustness of the technology within the time scales we are talking about. We are not starting from a zero knowledge base. (…) The UKPS trial did teach us things that will be filtered into the process. I would be confident that the technology is in place as and when we need it."[99]

Our own research had not noticed such problems but we appreciate the clarification. The Minister goes on to argue that because of these problems the Identity Cards Scheme will need to collect multiple biometrics. We presume that this is so those with brown eyes can be verified by face recognition, bald men can be verified by fingerprints and labourers identified using iris scanning.

...while the combination of biometrics does allow for an improved performance, "the performance improvement is unlikely to be commensurate with the increased costs, and collection of the additional biometric images might be seen as unnecessarily intrusive by the public."

However, the use of multiple biometrics is problematic. A study commissioned by the Home Office, and conducted by the National Physical Laboratory and BTExact, says that while the combination of biometrics does allow for an improved performance, "the performance improvement is unlikely to be commensurate with the increased costs, and collection of the additional biometric images might be seen as unnecessarily intrusive by the public."[100] Research by Dr. John Daugman of Cambridge University also shows that combining multiple biometrics does not necessarily lead to better results, and combining them may give significantly worse performance than relying solely on one stronger biometric.[101] At the level of systems implementation the Home Office has recently admitted that:

97 "ID Cards won't work if you 've got brown eyes says minister', Oonagh Blackman, The Mirror, October 17, 2005.

98 'ID Cards on Trial: Minister defends "robust" biometrics', Andy McCue, Silicon.com, June 7, 2005.

99 'Minister says ID technology is robust', Kable's Government Computing, June 6, 2005.

100 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', for UKPS, DVLA, and the Home Office, by Tony Mansfield and Marek Rejman-Greene, February 2003.

101 c.f. http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html

> "Readers for iris, face and fingerprint are very different devices and, to date, there has been little work done to integrate them. So it makes sense to consider them separately."[102]

Combining biometrics is both theoretically and practically challenging with dubious results.

Further data and studies have emerged on the effectiveness of biometric implementations. Home Office ministers have repeatedly attacked our research prowess in Parliament. On November 15th, 2005 during Committee stage of the Identity Cards Bill,[103] Baroness Scotland of Asthal referred to a report from the U.S. National Institute of Standards and Technology (NIST) on the performance of the US-VISIT border system.[104]

> "Although it was one of the world's leading studies into the use of biometrics, the London School of Economics overlooked it in its report, which is curious because we know how assiduous that body usually is when looking at research that may be pertinent. I am surprised that the LSE does not appear to have alighted on that study. One reason why we treat the LSE study with caution is because it is just not as rigorous as one would normally come to expect."

We have not yet received a response to our query to Baroness Scotland as to which NIST report she was citing. We were also surprised that there was no reference to any such report within Home Office documentation.

We are aware of NIST reports on a 95% accuracy rate for a two-finger database search, and we have repeatedly agreed with the finding that one-to-one verification rates are far higher, in this case being 99.5%.[105] These findings are consistent with the research presented in the LSE report that indicates that 1-1 matching is far more accurate than 1-to-many. In fact we reported on research studies with even higher accuracy rates than those presented in the NIST studies that we have seen, including Home Office commissioned research.

It is worth noting that despite the NIST results from 2004, the researchers were speculating about what would be ideal for US-VISIT, which only went live in early 2004 and in full scale implementation in September 2004. Because of accuracy and database problems, the Department of Homeland Security announced in July 2005 that it is planning on moving from a 2-finger system to a 10-finger biometric collection because of the need to increase the accuracy of the system and reduce the false acceptance rate:

---

102 "Identity Matters for Stakeholders Newsletter', Home Office, December 2005 available at http://www.identitycards.gov.uk/library/2005-12-20_IDENTITY-MATTERS-FOR-STAKEHOLDERS-NEWSLETTER.pdf.

103 Column 1057 of Hansard

104 This is the border-monitoring system deployed in the U.S.; for more information please see our review of this system on pages 89-91 of our earlier report.

105 C.L. Wilson, M.D. Garris, and C.I. Watson, "Matching Performance for US-VISIT IDENT System Using Flat Fingerprints", National Institute of Standards and Technology, May 2004.

> "1:many accuracy for a 2-finger search against a 6M subject database is 95% with a false hit rate of 0.08% (exceeding US-VISIT requirements)."[106]

As an example, at the current mean rate they announced that 400 examiner verifications were required per day and this was found to be problematic. According to one statement from NIST, there was a 0.1% false hit rate on a database verification of 1.2 million fingerprints; with 24.9 million applicants this resulted in 24,900 individuals being wrongly identified as on the watchlist.[107] When deployed across the UK such a rate could be debilitating.

At the time of publishing the LSE Identity Project report in June 2005 we were not aware of the May 2005 NIST Internal Report on non-parametric analysis of fingerprint data.[108] But this study only assessed probes of 6000 fingerprint images against a gallery of 6000 images involving 36 million comparisons in order to evaluate vendors' algorithms.

Recent research from NIST has pointed to a reconceptualisation of the challenges with the collection and matching of fingerprints.[109] This more recent research also argues that attempts to generalise the US-VISIT experience to other environments, as the Home Office has done repeatedly in public and in Parliament, is likely be problematic because of the limited types of people who cross the U.S. border. That is, populations that have a greater proportion of manual labourers or elderly who can be expected to have a greater proportion of hard to match fingerprints.

Further news from the U.S. is equally illuminating. The Department of Justice completed its audit of the investigation into Brandon Mayfield.[110] As we reported earlier,[111] Brandon Mayfield, a U.S. lawyer and former soldier was arrested for his alleged role in the Madrid Bombings. A fingerprint found at the scene of the terrorist attack was compared to the fingerprints in the U.S. fingerprint database, the Integrated Automated Fingerprint Identification System (IAFIS). U.S. officials found a 'certain' match with Mayfield's. Later analysis, after two weeks of imprisonment, found that the fingerprints were in fact not the same, and Mayfield was freed. The audit, released in January 2006 found that there was an 'unusual similarity' between the two fingerprints, and that such a scenario is 'extremely rare'. But the report also notes that there was an overconfidence in the power of the fingerprint identification system.[112] That is,

> "Larger fingerprint databases, however, may give rise to more of these situations. (...) IAFIS is designed to find candidate fingerprints having the most minutiae arrangements similar to the encoded minutiae from the latent print. These candidates should include the correct match

---

106 'Less Than 10-Print Processing', Presentation by Neal Latta, US-VISIT IDENT Program Manager, Department of Homeland Security.
http://fingerprint.nist.gov/standard/workshop1/presentations/Latta-LessThan10.pdf

107 Statistics as of April 20, 2005, see page 4 of http://fingerprint.nist.gov/standard/workshop1/presentations/Latta-LessThan10.pdf

108 Jin Chu Wu, Charles L. Wilson, "Nonparametric Analysis of Fingerprint Data", NIST, May 2005.

109 Austin Hicklin, Brad Ulery, Craig Watson, "The Myth of Goats: How many people have fingerprints that are hard to match?", NIST, September 2005.

110 A Review of the FBI's Handling of the Brandon Mayfield Case, Office of the Inspector General, U.S. Department of Justice, Unclassified Executive Summary, January 2006.

111 p.177

112 ibid, p.3

of the print (if it is in the FBI database) but will also include the closest possible non-matches. ... The enormous size of the IAFIS database and the power of the IAFIS program can find a confusingly similar candidate print. The Mayfield case demonstrates the need for particular care in conducting latent fingerprint examinations involving IAFIS candidates because of the elevated danger of encountering a close non-match."

The Home Office has admitted that it looks forward to using the NIR to identity latent fingerprints found at the scenes of crime (up to 900,000), and so we recommend the U.S. report for review.

The effectiveness of biometrics is best tested by evaluating their implementation and usability. The UKPS conducted a study in 2004 and we reported their findings in detail.[113] Recently the German government released its own study evaluating four implementations of biometric systems: two fingerprint systems, one facial recognition system, and one iris system.[114] Though their sample of just over 2000 people was much more homogenous than the UKPS study,[115] the results are interesting.[116] Most importantly, the German study tested multiple verifications over an extended period of time where participants were asked to verify their identity daily. On enrolment, using both ICAO-compliant images and system-specific templates, the results vary widely.

SYSTEM	IMAGE/ TEMPLATE	FAILURE TO ENROL	SUBJECTS	FAILURES
FINGERPRINT SYSTEM 1	Image	0%	1627	0
	Template	0%	2077	0
FINGERPRINT SYSTEM 2	Image	0.25%	1620	4
	Template	0.99%	2018	20
FACE RECOGNITION SYSTEM	Image	0	1625	0
	Template	0.40%	2019	8
IRIS RECOGNITION SYSTEM	Image	0	1540	0
	Template	0.89%	2017	18

113 pp 182-185

114 Studie: 'Untersuchung der Leistungsfahigkeit von biometrischen Verifikationssystemen - BioP II', Offentlicher Abschlussbericht, Secunet, Budesamt fur Sicherheit in der Informationstechnik, version 2.0, August 23, 2005.

115 There were no disabled users and the population were mostly educated men with few manual labourers, and 97.6% were Caucasian (p.51).

116 Please note that both the study and our conclusions regarding the study refer to specific systems, i.e. implementations of a biometric technology provided by a specific vendor in a specific environment. This is equivalent to the separation between theory and practice: 'biometric technology' refers to the theory, and 'biometric system' refers to its specific implementation and practice.

The difference between 'ICAO' and 'template' is that the ICAO standard requires the enrolment and verification against an image of our biometric, e.g. a photo of our face. A 'template' is system-specific data collected to identify your biometric, e.g. specific calculations on your facial dimensions. Templates usually provide better performance and are cheaper; but they are proprietary, and thus are restricted from being used in ICAO's international standard. Until there is a standard for exchanging information between templates, however, the risk with using templates is that it will result in vendor lock-in.

The data on enrolment shows that even on such a small scale experiment, the failure rates are still remarkably unstable. This also shows that specific implementations of the same biometric can have very different results.

The above results are promising for enrolment of face recognition. The study found significant failure rates for fingerprinting, although they are lower than reported in more representative samples, where failure rates may rise to 5%. The diagnosed reasons for failure[117] include:

- fingers were too wet, or too dry,
- people had 'too difficult fingerprints', e.g. tennis players,
- mistakes made by the enrolment staff;

and for some the report concluded that they were unable to ascertain the causes of the failure. On iris scanning the reasons for failure included

- users were not able to see well enough to identify the target area,
- users were unable to position eye well for the iris capture,
- system design prevented short people (less than 1.55 metres) from enrolling;

and again the report concluded that 'in some cases, reasons for failure could not be determined.'

The challenge in the enrolment stage is to reduce the Failure-to-Enrol rate. Once enrolment is complete, the challenge changes into ensuring a low verification failure rate.

When testing the systems ability to verify recorded biometrics verification the results from the German study were also interesting.[118] The biggest failure rates occur when the systems were first implemented. The tests were conducted over two month periods, and with increasing practice, the False Reject Rate (FRR) dropped significantly. However when the systems were used infrequently the rejection rates remained high. In the case of the tested iris recognition system, some groups were rejected 20% of the time at normal operating levels.[119] At a False Acceptance Rate (FAR) of 0.01%, the internationally accepted norm, the study shows that the face recognition systems were particularly problematic with average rejection rates varying between 6% and 18%, while fingerprint template verification systems involving frequent

117 itemised on page 94

118 presented on p.108

119 ibid, p.120.

users did well, with average rejection rates between 2% and 3.5% and the best performance being and FRR of 0.81%.

The conclusions drawn by the German study include

- People need to be very practised in order to present the biometric effectively.
- Under stringent security situations, with a False Acceptance Rate of 0.01%, the False Reject Rate for the specific iris recognition system as such that a small but significant number of users had problems. For face recognition, the error rates were high.
- There were a number of problems with the iris recognition system.
- A number of problems arose that had not been anticipated.

The report's final conclusion was that biometric systems can effectively *support* the verification of identity when confronted with an official document. This is not a full-hearted endorsement of the technology by any means: researchers did not to say that the systems can effectively *perform* the verification of identity.

Building on the study's results we can say that greater attention is needed on the importance of environmental conditions in different situations. There is no guarantee that these systems will perform similarly when used in other situations, e.g. outdoors, by a police officer, or under different lighting. Generally the Germany study argued that the equipment must be better designed to support interaction with a wider range of users, and provide users with more accurate and relevant instructions and feedback. That is, a necessary condition for the successful operation of biometrics is cooperation and acceptance from the user. They also worry about the accuracy in verification of biometrics and argue that this 'urgently needs to be investigated'.

The German report also states that technical measures alone would not solve these problems. It recommended that a successful implementation would also involve adjusting organisational measures in order to make sure that recognition is successful. Policies are needed and extensive training must be supplied so that staff are aware of the various FAR and FRR, and that expectations and decisions on the verification of identity must be based on that knowledge. There is a need for more information about biometrics, and explanation of how they work, that is accessible to the general public, and a programme of measures promoting acceptance would need to be put in place.

The report also argued that security mechanisms must be added to prevent unauthorised access to the biometric on the document, e.g. basic access control and extended access control as proposed by international standards. The report also finds that system security needs to be increased in all these implementations.

We would like to draw particular attention to that last point on security. Systems require high system security and physical security otherwise a malicious hacker could manipulate biometric data that may be stolen. Unless systems are secured, attackers could take the systems apart and swap components, and it may be possible to interfere with the communications between the modules. This would permit the harvesting of biometric data and interference with the verification processes.

Therefore it is reasonable to say that in the field of biometrics, certainty is rare. Closer to home, we can also report a less than gallant response to failure. While chairing a discussion in a committee room in the House of Lords on November 7, 2005, Baroness Anelay of St Johns related a personal experience of facial recognition systems. With a group of parliamentarians, she was being given a demonstration of one such system. It failed: indeed the system in question subsequently crashed, twice. The reason? This most attractive lady was told that her face was 'too bland'.

...it is reasonable to say that in the field of biometrics, certainty is rare...

Any conclusions drawn by the Home Office stating that the systems are ready for deployment on a national scale do not reflect key studies and findings.

Any conclusions drawn by the Home Office stating that the systems are ready for deployment on a national scale do not reflect key studies and findings.

The Controversy of Costs

The LSE's research team is presently unable to provide further assessment of the costs and potential benefits of the government's identity cards proposals. In part this is due to the absence of crucial data, but equally so because expectations for the scheme itself have substantially changed between 2004 and 2005.

From the outset in 2002, the Identity Cards proposal failed to win universal support amongst central government departments. The Home Office intended the ID cards scheme to provide a gold–standard identity infrastructure for use by all government departments. One would expect that if these other government departments were confident in the Home Office's ability to deliver the scheme successfully they would have no problem being compelled to integrate their own systems with the ID cards scheme. However, the present Bill places no obligation on departments to make use of the scheme.

Not mandating the use of the ID cards scheme across government suggests major concerns with the project and goes against the stated government policy of providing joined up government. For example, documents throughout the period from the Cabinet Office's "Privacy & Data Sharing"[120] in April 2002 through to "Transformational Government"[121] in November 2005 have emphasized the government's intention of pursuing joined-up government across the public sector.

It is now clear that no such policy has been achieved. Furthermore, despite a three and a half year marketing effort to the government, the Home Office has failed to achieve formal buy-in to the scheme. In the last quarter of 2005 a series of Parliamentary questions were posed to clarify this matter.

The questions were addressed to a number of Government Departments and agencies, and generally took the form of:

120 'Privacy and data-sharing: The way forward for public services', Cabinet Office, April 2002.

121 'Transformational Government: Enabled by Technology', Cabinet Office, November 2005, Cm 6683.

> "To ask the Secretary of State, what estimate he has made of the (a) total and (b) net cost of (i) integrating the proposed identity card scheme into his Department's IT systems and (ii) the ongoing operation of the scheme within his Department."[122]

while other questions took the form of

> "To Her Majesty's Government, Whether they will publish (a) any analysis they have made of the potential use that the Department [in question] may make of the National Identity Register or identity cards introduced following enactment of the Identity Cards Bill; and (b) their estimate of the costs that will or may be incurred by the Department [in question] in connection with such use.[123]

Answers were received from:

- Department for Constitutional Affairs
- Department for Education and Skills
- Department for Environment, Food and Rural Affairs
- Department of Health
- Department of Trade and Industry
- Department of Transport
- Department of Work and Pensions
- Foreign and Commonwealth Office
- Northern Ireland, Scotland and Wales Offices
- Treasury

The responses to Parliamentary questions revealed that no department has made a decision to integrate with the scheme and none has conducted publishable research into the costs or benefits of doing so.

Indeed there appears to be indications of resistance to take-up of the ID proposals. In answer to a question on take-up and integration costs from Lynne Jones MP, Treasury stated that it anticipated 'no additional' integration costs with the scheme 'or to the on-going operation of the scheme within HM Treasury.'[124] In answer to a similarly worded question from Baroness Anelay, the same department answered that it had neither made a decision nor conducted research. These two answers prompt the quite reasonable conclusion that, at present, Treasury has no plans to integrate with the ID scheme. We would be grateful for clarification on this matter.

---

122 Asked by Lynne Jones, MP for Birmingham on November 21, 2005.

123 Asked by Baroness Anelay of St Johns and Baroness Noakes, and Baroness Seccombe

124 Answer to Lynne Jones MP from John Healy, Answered on November 24, 2005, HMT REF: 238W 05/06.

The DCA, DTI, Department for Environment, Food and Rural Affairs, and the Department of Transport all claim that they have not yet finalised current best estimates. The Northern Ireland Office, the Scotland Office, and the Wales Office declared that they have no plans to make any estimate. The Department for Education and Skills and the Department of Health stated, using the exact language of the Home Office, that

> "Not all services will require a high degree of integration between the ID Cards Scheme and other IT systems."

The Department of Health added that it has no plans to use ID cards to access the NHS Care Record Service. DFES and DWP have admitted to coming up with 'best estimates', but using the exact language of the Home Office, state that they are unable to offer detailed estimate costs to Parliament because of concerns of commercial confidentiality.

Others used a form of language apparently written by the Home Office to argue that the costs would be absorbed into the usual cycles of system upgrades and technology refreshes. Meanwhile, the Foreign and Commonwealth Office states that it is unable to estimate the potential cost until the legislation has been completed and 'policy issues relating to use of or access to ID cards overseas have been clarified.'[125]

Ministers have since June 2004 alluded on rare occasions to the "voluntary opt-in" nature of the scheme, but no substantial discussion of the dynamics or implications of this approach has ever been conducted. That the ID scheme is a proposal based on agency business case opt-in rather than it being a public sector wide policy initiative has surprised many observers.

This state of play has created a more cautious and conditional series of assertions by the Home Office. In a letter to the London School of Economics in December 2005 Home Office Minister Andy Burnham stated:

> "Decisions on **whether, when and how** particular public services will make use of the ID cards will be made by those services…" (our emphasis).

This conditional statement contrasts sharply with the more optimistic tone of earlier views. The Regulatory Impact Assessment, for example, stated:

> "The Bill allows for each service to decide **when and how** ID cards could be used…" (our emphasis).

Ministers have since June 2004 alluded on rare occasions to the "voluntary opt-in" nature of the scheme, but no substantial discussion of the dynamics or implications of this approach has ever been conducted. That the ID scheme is a proposal based on agency business case opt-in rather than it being a public sector wide policy initiative has surprised many observers.

125 Answer to Lynne Jones MP from Mr. Alexander, December 15, 2005.

In the absence of a commitment to buy in to the ID scheme, the magnitude of the scheme and its potential to derive benefits and savings are almost entirely speculative. While standing by its estimates in the June 2005 report, the LSE team cannot at this time update or refine its figures because of a lack of clarity and transparency.

We are not the only ones in this quagmire. The Better Regulation Task Force has singled out the Identity Cards Bill as an example of 'poor regulatory practice' when assessing its benefits over the costs.[126] The Bill has been referred to the National Audit Office in an attempt to 'drive up its quality'.

In the absence of a commitment to buy in to the ID scheme, the magnitude of the scheme and its potential to derive benefits and savings are almost entirely speculative.

Our costings

Despite numerous counter-claims and criticisms from the Government, and repeating what we said at the start of this report, we continue to stand by our estimates.

There is a significant difference in our estimates and those presented by the Home Office. The Home Office predicts that the scheme will cost £5.84bn over ten years. This was most recently clarified by Baroness Scotland:

> "This figure covers the costs of application processing, including processing of maintenance requests, such as changes in personal details; the running costs of enrolment centres where biometrics will be recorded; facilities to house and operate the National Identity Register; running contact centre operations; running corporate services such as HR and finance systems and the national identity scheme commissioner. The costs also include production and distribution of personalised identity cards and passports and allowances for depreciation, technology refresh and maintenance as well as contingency and optimism bias. To provide more detailed analysis of costs in advance of procurement may prejudice the department's ability to secure a value for money solution from potential suppliers."[127]

We note that the Home Office estimate only counts the costs for establishing the system within the Home Office. It does not include

- costs to other departments
- costs of readers in other Home Office agencies, e.g. for use at borders or by police
- costs of the database design

126 'Regulation watchdog counts the cost of ill-considered bills', Jean Eaglesham, The Financial Times, August 4, 2005.

127 Parliamentary Question answered by Baroness Scotland of Asthal to question posed by Lord Barnett, December 15, 2005, column WA184.

As we have previously argued, the Home Office is concealing much of the costs in other budgets such as the upgrade of UKPS services.[128]

The Home Office has lodged a number of complaints regarding our figures. We summarise the most recent criticisms below, and a more expansive explanation of the differences in our models was published in June 2005, and is in the annex of this report.

The LSE Report uses old and erroneous data.

To avoid accusations of 'fabricating data' we used figures provided by the Home Office in successive reports, consultation documents and statements. The Home Office has refused to give more detailed information, with the exception of the surprising data released to industry in October 2005 that they foresee 44,000 private sector users and 265 government departments and agencies. This is well beyond what we had foreseen.

The LSE Report wrongly states that biometrics need to be updated more than once every 10 years.

Most advanced countries' passports have a 5-year renewal cycle. Studies ranging from the GAO to the most recent German study on passport technology raise significant concerns regarding the lack of understanding in respect ageing and its effects on biometrics, e.g. facial recognition. Unless the UK wants its citizens to fail biometric verification when travelling abroad (where the test is for facial recognition) we recommend a 5-year cycle. We also contend that the market for biometric systems is still evolving (as exhibited by the recent German Government report) so a more frequent updating will improve effectiveness and security.

The LSE Report overestimates the costings for the biographical footprint and is instead covered by the costs incurred by the UK Passport Service.

The Home Office claims that this is already budgeted for because the UKPS has to conduct biographical footprint checks for all new passport holders. This is wrong: the footprint checks will be only of all NEW passport holders, i.e. first time applicants. The Home Office seems to be trying to account for costs through ambiguities and unnecessarily merging ID plans with the changes to the passport. Allied to this process, error rates in credit reference agencies are high, a problem that will require considerable analysis and correction.

The LSE Report envisions visits to the enrolment centres to make changes to the NIR.

We never made such a statement regarding all changes to the NIR. However we do expect that, for example, some changes to names and addresses or residency status will require some manual intervention through the presentation of documented evidence. Otherwise the integrity of the system and its potential for identity fraud is increased.

128 Parliamentary Question answered by Mr. McNulty to question posed by Lynne Jones, June 13, 2005, Column 150W.

The LSE Report exaggerates the number of changes to the register, stating that there will be up to 1.2bn notifications of changes over a ten-year period.

We carefully state that over ten years there may be 250m to 1.2bn changes. We are surprised by the criticism, however, because even the Home Office documentation states that they believe that there could be at least 1bn changes.[129] Our estimates mean, using current Home Office estimates, that individuals would only have a change of circumstance (e.g. change of name, address, etc.) between 2.5 and 12 times over ten years. The Home Office now estimates 10 changes. We believe that both of us are underestimating, but more importantly we don't understand why the Home Office accuses us of exaggeration whilst using similar numbers. The Home Office has not explained this contradiction in its own work.

The LSE Report overestimates marketing costs at £1bn.

We do not include marketing costs in our estimates. We look forward to hearing the Home Office's estimates.

The LSE Report overestimates the costs of establishing a national register.

We say that the register itself will cost between £300m and £430m over ten years, which is not very expensive considering the complexity involved in establishing an extensive register with critical infrastructure protection and with backup facilities. We based our figures on the cost of the NHS spine, which is of similar complexity and user base, and which was also subject to delays and cost overruns. Within our larger costings for the 'National Identity Register' we also include the integration costs for DWP and various Home Office systems (e.g. IND), to which the Home Office has not responded. The KPMG report even warned that the Home Office's two-year plan for start up is more likely to be three-years.

It is important to note that the *Home Office's estimate of £584 million over ten years does not include the cost of designing the register*, as they argue that this "is a resource set up cost".[130]

The KPMG Report supports the Home Office's costings model.

We disagree. The KPMG report reviews only a portion of the Home Office plans, i.e. 60% of the total operating costs. It excluded benefits, technical, commercial, transition or programme cases, the related business cases of changes to the UKPS practices and IND biometric residence permits. The KPMG report even notes that they lacked adequate data such as performance targets from UKPS. The report also finds that the Home Office predicts a low margin of contingency for set-up costs and calls for a more detailed risk-based approach. As a result the KPMG report doubts the full recovery of operating costs: "there will clearly be a point beyond which it will be infeasible to pass through all operating costs incurred to ID cardholders."[131] KPMG also argues that the Home Office fails to follow the recommendations of the HM Treasury Green Book.

---

129 http://www.identitycards.gov.uk/library/Procurement_Strategy_Questionnaire.doc page 11.

130 Parliamentary Question from Andy Burnham to Dr. Cable, July 6, 2005, Column 532W.

131 'Cost Methodology and Cost Review; Outline Business Case Review', published extract, KPMG, November 7, 2005.

The LSE Report underestimates card lifetime by reducing renewal period from 10 to 5 years.

We based this on an estimate from the Home Office in 2002.[132] Many countries have 5-year renewal of their identity and travel documents. Because of untested technology, new devices (e.g. RFID), and changes in security practices, we predicted that a five-year renewal, like for credit card and bank cards, would be optimal. Even the KPMG report recommended some review of the Home Office estimates, saying that the card life of 10 years was 'questionable'. Home Office statements to industry state they 'currently anticipated' a 10 year renewal period. Northrop Grumman has been warning the Home Office of a 3-5 year period.[133]

The LSE Report overestimates card replacement rates, assuming a 10% replacement rate due to loss, theft or damage per annum. Instead loss and theft rates are 2.69%.

This is incorrect. We assume a 5% damage rate, 2.7% lost or theft rate, and error rate of 1.67% (in accordance with UKPS figures). The KPMG report warned the Home Office that their own estimates on lost, damaged and faulty cards appeared low, though 'proposed revised figures appear reasonable'. We look forward to seeing the Home Office's new figures.

The LSE Report's costs of biometric readers are too high (£3000-4000) while the Home Office predicts only £250-750.

We estimate readers ranging from £275 (card readers), £500 (card and fingerprint), £750 (facial), £3500 (iris). These higher costs are similar to costs in the Home Office's RIA of the Immigration, Asylum and Nationality Bill. We see each reader being used in different situations. We see these being replaced every three years, and include costs for communications. The KPMG report has already recommended that the Home Office change its models to allow for only a five-year lifetime for mobile registration centres and 3-5 year lifetime for biometric registration devices. A recent Home Office newsletter admits they realise that they now require 'high-end single finger readers' and not 'low end mass-market sensors'.[134] We look forward to seeing the Home Office's new figures.

Based on the above, we believe that the KPMG report fully validates our estimates. For a more detailed discussion of our costings please see our explanatory memo, previously released in June 2005, in the annex.

We are eager to see the Home Office's new cost figures. Despite complaints from Parliament, the Home Office refuses to estimate how much the plans would cost other departments. According to Baroness Scotland,

---

132 Consultation Document, Section 5, 2002, paragraph 30.

133 'Memorandum submitted by Northrop Grumman', submitted to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we40.htm.

134 http://www.identitycards.gov.uk/library/2005-12-20_IDENTITY-MATTERS-FOR-STAKEHOLDERS-NEWSLETTER.pdf page 5

"We cannot whilst those negotiations are going on release data which would put us as a government in an unnecessary difficulties in relation to the tendering process."[135]

Peers even offered a secret-session to discuss the costings, but the Home Office refused.

It is important to remember that our costings included integration costs for DWP and Home Office systems, while it appears that the Home Office figure of £584 million per year, over ten years, is only the cost to the Home Office for establishing the system. As a result, their 'cost-benefit analysis' compares apples with oranges. They say that for £5.84bn they can run the scheme from which all Government services will benefit. We believe that many more costs will be incurred before these other Government services begin to even make use of the scheme.

A Sense of Inevitability to the Policy

The Home Office, and at times the Prime Minister, have pushed the notion that the identity cards policy is inevitable. The purpose of this imagery is to indicate that Parliament's consent to this scheme is merely a formality and a re-affirmation of the direction that the world is going. Such statements vary between the softer 'ID Cards are an idea whose time has come'[136] to the more emphatic claim that 'without regard to Parliament's decision on identity cards, biometric passports collecting iris, finger and face scans are an inevitability.'[137]

As we have repeatedly argued, the biometric passport is a policy that is separate and distinct from the identity card. Yet the Government insists that the two are intertwined, beginning with the sense of inevitability due to international obligation, extending to the 'requirement' to collect vast biometrics, and ending with the claim that much of the budget for identity cards can be absorbed by the budget for these biometric passports. No other country is planning on introducing a passport of the type proposed by the Home Office because no other country is trying to turn their passport infrastructure into an identity card. The Home Office has stated that whether the Bill passes or not, it will continue to work to establish international standards on identification documents.

No other country is planning on introducing a passport of the type proposed by the Home Office because no other country is trying to turn their passport infrastructure into an identity card.

The Government is trying to make the Home Office's scheme appear absolutely necessary. Most recently the Cabinet Office report 'Transformational Government: Enabled by Technology'[138] states that identity management is essential to the delivery of public services. The report places the identity card at the cen-

135 'Peers demand total ID card cost', BBC, November 16, 2005.

136 PM Opening Statement, Prime Minister's Monthly Press Conference, June 27, 2005

137 Claim made by Home Office Minister, Andy Burnham, at a meeting in the House of Lords, November 7, 2005.

138 'Transformational Government: Enabled by Technology', Cabinet Office, November 2005, Cm 6683.

tre of the Government's IT plans and budgets. Surprisingly the report does not question what form of identity infrastructure would be ideal, but instead takes the Home Office's model as a given.

Identity requirements are increasing, and this is in part due to changes in other laws and policies. The Home Office has spent three years and almost £30m[139] on developing momentum behind this scheme

The Government is ramping up requirements for identification, while the Home Office is preparing to provide the solution. The transportation and financial industries are making further demands on consumers, and employers are increasingly demanding increased personal data and proof of residency from new employees. The Home Office then argues that due to these mounting demands we are in greater need of an identity document.

Sometimes there is a backlash from consumers who resent the continued identity checks. Some regulators have even criticised the practice. However, in many of these situations these private companies are under recent legal obligations to verify such information.

Every year the momentum grows further and other laws are quietly changed. The Serious Organised Crime and Police Act of 2005 increased the verification of fingerprints and addresses,[140] and mobile fingerprint scanners have been available to all police since Autumn 2005.[141] The most recent instance of this dynamic is the consultation paper on the Co-ordinated Online Record of Electors (CORE).[142] This scheme, as proposed in the Electoral Administration Bill, will allow nationwide access to electoral registration data that will continue to be locally gathered and maintained. It would be established by secondary legislation. This scheme is highly dependent on the Identity Cards scheme: the two systems will be interconnected. The linkage between the two projects goes further: local authority officials will be required to investigate any discrepancies, i.e. to police the system to ensure that individuals are updating the information held on both registers.[143]

---

139 Parliamentary Question answered by Tony McNulty on 8th November 2005 http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmhansrd/cm051108/text/51108w17.htm

140 section 117

141 'Denying Criminals the Use of the Roads", ANPR Strategy for the Police Service, ACPO NAPR Steering Group, March 2005.

142 'The Co-ordinated Online Record of Electors (CORE) - The implementation of national access arrangements', The Department of Constitutional Affairs, December 14, 2005, http://www.dca.gov.uk/consult/core/core_cp2905.pdf.

143 'Councils to police new controversial ID card database', Conservative Party Press Release, January 2006.

Section II: Research Challenges

Serious and successful research projects require three conditions: (a) an environment of openness in which reliable and accurate information is freely available; (b) access to the full range of key stakeholders, and (c) settled points of reference within a stable research context. In the time since publication of our report in June 2005 none of these conditions has been possible. This section will explain why we are unable to present a final report on the costs and implications of the Identity Cards Bill, and why we believe no such evaluation can be made by any independent research.

A culture of secrecy

We observed in our last report that the identity cards legislation had been drafted almost in its entirety in 2002, and that consequently there had been no opportunity for genuine stakeholder engagement or consultation. This situation exists despite two formal consultations, which in effect were illusory. We do not resile from this view.

There are three important repercussions that arise from this pre-determined and "top down" approach to the identity cards proposal. The first is that the approach requires buttressing through an increasingly closed development and planning process. The second is that a disproportionately large effort is required for public relations and marketing of the scheme's more controversial and contentious aspects. The third is that few opportunities exist for alternative architectures and approaches that may achieve similar objectives.

It is clear that the planning for this project has been conducted in a centrist fashion, with most activity occurring between the Home Office and key IT vendors. The trade body "Intellect" has in effect been appointed the industry conduit for this scheme. The result is a closed process within which public education has replaced public consultation. The question of "how" the scheme can be built has become more important than "why" it should be built, "in what way" it should be built, or even "whether" it should be built.

The question of "how" the scheme can be built has become more important than "why" it should be built, "in what way" it should be built, or even "whether" it should be built.

As the scheme attracted increasing attention and criticism during 2005, government has tended to tighten even further this closed planning environment. The substantial investment of public funds in the business model being developed by PA Consulting should in our view have been an open and transparent process. Instead, PA Consulting has from our perspective been impossible to engage. Their work, whether through initiative or instruction, has been covert. This is both a lost opportunity and a negative indicator.

Such a process leads inevitably to increasing restrictions and prohibitions on relationships. In 2005 the LSE attempted to open a dialogue with Intellect, but received no response from the organisation. Our sched-

uled meeting with Treasury – which we were told was an event the department wanted to take place – was cancelled at two-hours' notice on the insistence of the Home Office. Attempts to meet other government departments have failed. The Home Office has instructed other departments that it is the lead agency on the project and reserves its right to decide on relationships with outside organisations. We are concerned that this discretion has not been applied merely to interaction with the LSE.

The Home Office also appears to have confused the processes of representation and consultation. While it is true that Home Office Ministers and officials have spoken at a wide spectrum of ID card related events, their role has been primarily to persuade audiences rather than retain an open mind on differing views. We perceive an emerging siege mentality that would be inimical to a project plan that is genuinely supported by the country as a whole. Open hostility to, for example, the views of the Information Commissioner and to 'non-aligned' industry bodies is one unfortunate result of a philosophy of closed planning.

The Home Office also appears to have confused the processes of representation and consultation. While it is true that Home Office Ministers and officials have spoken at a wide spectrum of ID card related events, their role has been primarily to persuade audiences rather than retain an open mind on differing views.

Absence of transparency

The government has failed to provide adequate information relating to this proposal, resulting in public understanding that is patchy and opaque. Key documents have been kept secret, others have been censored. Freedom of Information requests and Parliamentary questions have frequently resulted in responses that are meaningless or non-existent.

Refusal by the Home Office to release gateway reviews and the risk register have made serious risk evaluation of the project impossible. Non-disclosure of the full KPMG report has inhibited a balanced assessment of the facts relating to costings. The crucial work of PA Consulting in developing the business case is entirely secret, as are all dealings within and between departments on this subject and all dealings between government and Intellect. Only one of the FOI requests we have viewed has resulted in a meaningful or useful response.

Costs of the scheme have been hidden for reasons of "commercial sensitivity". We believe this is a deceptive justification. None of the vendor organisations we have spoken to believe that projected costs have any bearing on the bidding process. It is more likely that detailed costs have been hidden because they contain data relating to self-financing of the scheme on the basis on fees to the consumer, and are thus highly sensitive at a political level.

Conflicts and contradictions

Assertions and claims by the Home Office, particularly since June 2005, have become increasingly conditional. Of greater concern are the contradictions that have emerged in these statements. A scheme that

up until 2004 was said to be inclusive and infallible is now characterised as inconsistent and flawed. This report has already cited many contradictions and conflicting statements. Others include:

1) There are major inconsistencies in the statements made by officials and ministers concerning the performance of biometric technology. David Blunkett claimed "[biometrics] will make identity theft and multiple identity impossible, not nearly impossible, impossible"[144] and Andy Burnham who more recently claimed: "this will make it impossible - impossible is a big claim - it will make it almost impossible to forge an identity" and "the crucial strength that it brings is that an identity... can only be registered once"[145] On the other hand, the head of the Identity Card programme, Katherine Courtney has admitted: "criminals will have to work hard to get two identities and work very hard to get three."[146]

2) Baroness Scotland's promises of a highly secure off-line NIR (as described in the Lords Committee stage) contrasts starkly with Tony McNulty's statements regarding citizens conveniently updating their address details via the Internet (as stated in the Commons Third Reading). This begs the question of how the government intends to balance security and convenience, and it is most disturbing that such critical design principles have yet to be resolved.

3) Andy Burnham's written answer in December: "The ability to either confirm the validity of the card or verify information electronically against the register using secure technologies means that forged cards will be ineffective as they will be unable to make a connection to a valid record on the register" (i.e. endemic checking) vs. just 163 million verifications a year (i.e. 3 checks per annum. per card) in the Home Office Procurement Strategy Market Soundings presentation. Will every transaction be checking against the NIR and, if not, how can the Home Office guarantee the validity of the card?

4) Andy Burnham, "it is not and never has been our intention to create an elaborate database that would hold detailed personal profiles for every individual"[147] vs. Burnham in a letter to Jim Knight MP on 22/9/05, "the scheme will provide, subject to appropriate authorisation procedures, the capability for law enforcement and intelligence and security agencies to be provided with information on when a person's record on the Register has been checked or amended" - i.e. the audit trail and updates - further arguing that this would make it difficult for suspects to stay in hotels, rent accommodation, hire a car, or buy a mobile phone (which strongly implies a Home Office intention to make each of these activities subject to a recordable/disclosable ID card check).

After more than three years of planning, such fundamental contradictions and uncertainties should not arise. We remain deeply concerned that they will add to the instability of the proposal.

144 11 November 2003, Today programme

145 http://news.bbc.co.uk/1/hi/uk_politics/4445760.stm

146 http://technology.guardian.co.uk/online/comment/story/0,12449,1570018,00.html

147 Third Reading http://www.parliament.the-stationery-office.co.uk/pacm200506/cmhansrd/cm0510 18/debtext/51018-16.htm

Section III: Unanswered Questions

To what extent does the legislation place a requirement on government departments to adopt the ID provisions?

There is a disjuncture between the stated purposes for the Bill and the breadth of the implementation of the scheme across government.

A On the one hand the Government argues that the purpose of the Bill is to prevent identity fraud, combat terrorism, combat benefits fraud, prevent illegal immigration, and increase the efficiency of access to government services.

B On the other hand, the Home Office, which is sponsoring this Bill, refuses to consider whether other departments will actually use the scheme. Their most recent approach is that 'it is up to every department to decide'.

C Against this backdrop, the Home Office is envisioning that the system will be used by over 265 government departments and agencies, and up to 44,000 private sector organisations.

If the scheme is to even theoretically achieve all of its policy goals then it must surely be made compulsory (as demanded by the police) and other departments must be compelled to use it. We do not endorse such a policy, but the opt-in model appears fatally defective.

To what extent is integration with the private sector a necessary requirement (financial institutions, employers etc)?

The Home Office states that identity verification will be made available to 44,000 private sector organisations. Convincing these organisations to buy into a system that will cost them per-transaction will require some persuasion. Does the Home Office intend to introduce new regulations or legislation requiring verifications against the NIR, as it has done in other areas? How does this relate with the movement in the financial industry away from an over-reliance on identity verification?

What criteria will be used to determine which levels of NIR verification (e.g. online, biometric) will be made available to an organisation? How will their use of NIR checks be verified and audited, and at what frequency?

If up to 44,000 private sector organisations and 265+ public sector departments and agencies are to have access to the NIR then some policy is required to decide what level of personal information is disclosed to these various organisations in such as way that it is proportionate. Similarly, when verifications take place these organisations may conduct online checks, using biometrics. How does the Home Office intend to police this access to make sure that these organisations are properly implementing access to the NIR and not using NIR verification to also store information e.g. fingerprints, locally for other purposes.

To what extent and in what form will direct charging to customers apply for NIR checking by organisations?

We believe that organisations will seek to offset costs of the scheme by charging customers for accesses to the NIR. Presently there is no guidance on how and when this will occur, what quality assurance will be instituted, or whether a proportionality test will be applied for accesses. It appears likely that NIR checking may become endemic because of a combination of (a) money laundering requirements applying to a range of professional and financial services, (b) employment checking requirements, and (c) voluntary consent within a much broader spectrum of interactions. There is a risk that this process will, in effect, become a substantial new consumer tax.

Will direct charging by the private sector be capped?

The legislation makes provision for setting the cost of registration and cards through regulation, but appears to make no reference to limiting the cost of NIR access and verification. At present the market will determine the level and extent of these costs, a situation that may result in higher rather than lower transaction costs to the consumer.

How will organisations conducting NIR checks be verified and audited?

The Home Office has estimated that up to 44,000 private sector organisations may have access to the NIR. It is entirely unclear how these organisations will be registered and validated on the NIR system, or indeed how individual accesses from each organisation will be authorised. If, for example, a participating organisation has multiple branches each of which is permitted to make checks, how can an authorisation system for each employee be made in a secure and robust manner? For such a system to function in a secure way there must be an audit triangulation involving the Register, the user organisation and the individual. Each must be assured that accesses from an organisation were made by authorised personnel rather than merely via a generic authorisation code.

How will liability and non-liability be determined both for NIR checks and transactions where NIR checks are not conducted?

The question of liability has not been resolved at any level. Liability will be a major factor in determining the extent to which organisations will use the system. It will apply equally to circumstances where checks are being conducted and where a decision is taken to accept another form of identity check (such as local verification of a card or even alternative checking procedures).

How will local verification against cards be used? In what circumstances and using what technology?

The LSE Report of June 2005 stated that offline checking would involve comparison of the card-holder's characteristics with those stored on the card. This would mean investing in suitable scanners and card readers, and would therefore be suitable only for high value transactions where the card holder was present, unless the card holder owned their own fingerprint or iris scanner. An on-line check would involve comparison of the card holder's biometric characteristics against those held on the central register. This

would require that the relevant organisation purchase a scanner, a card-reader and also on an on-line connection to the authentication service.

The Home Office responded that an on-line system would prevent identity fraud and would raise the security of the entire scheme. But the costs are also raised, along with the privacy problems of the audit trail. What mechanisms will be in place for local verification? What kind of costs are envisioned?

Will there be a requirement that biometrics technology used for checking and verification will be of the same technical quality as the registration technology?

Recently the Home Office admitted that mass-market (and lower quality) biometric readers are not useful in verifying fingerprints. We would like to know its current thinking on this matter as it previously argued that biometric readers will be low cost. While we agree that the registration centres will require high-cost systems to ensure accurate collection of biometrics for enrolment, is the Home Office now considering the use of more advanced technologies at verification sites? Will the Home Office have a threshold quality level on these identity service users to ensure that the technology is good enough for adequate verification?

Will biometrics be stored on the ID card, and if so, what form will this take (hash, image etc)?

If local verification is to take place using biometrics, the biometrics will have to be stored on the card. To be compliant with ICAO standards these biometric images will have to be stored locally and transmitted through contact-less technology. These large images will require larger data storage on the chip than in most identity card schemes. This also increases the availability of personal information that may be gleaned from the card, both legally and through skimming. Concerns over this disclosure led to the U.S. Government shifting its policy to implement additional security measures on its new e-passport.

What security standards will apply to verification checking, transmission of data, and data storage?

The German study on biometrics points towards the need need to investigate the security of the technology used for enrolment and verification to ensure that they are not tampered with. The Home Office will have to ascertain the security level of all these verification points to ensure a high-integrity system. Additionally, to prevent identity fraud and the collection of biometric data by third parties, additional security measures will be required for the transmission of verification data and for the storage of the data on the register. The required security decisions must be made from the outset of the design of the scheme.

What advice has been obtained by government relating to the legality of the proposals?

In the LSE report there is an extensive review of the legal landscape ranging from the duty to identify, data protection, and the changes to the passport. This portion of the report was not criticised by the Home Office and as a result we are presuming that they share the concerns it raises. If this is not the case, we

would welcome some information on the legal grounds for this scheme, particularly in the light of the concerns from the Council of Europe Commissioner for Human Rights.

What are the current integration cost and cost/benefit estimates from each government department relating to the scheme?

Despite repeated attempts to gain access to this information we are unable even to understand what are the presumed benefits to each Government department. Their reluctance to calculate or disclose reduces our ability to conduct more research and analysis on this policy and is debilitating for the purpose of forming an informed opinion on this policy in order for it to move beyond Parliament.

Precisely how will personal information be updated on the system, and what options are being considered to expedite this procedure?

The government has indicated that personal information, such as change of address, could be updated on the Register in a simple way, perhaps via a website. There will however be many circumstances where people will be unable or unwilling to use an online function, and may choose to make changes in a more orthodox way. In what circumstances will update charges allowed by clause 37(1) of the Bill (fees in respect of functions carried out under the Act) be applied, and to what level and extent?

To what extent will the system be reliant on a Chip & PIN architecture?

Take-up and functionality of the ID card will to a large extent be dependent on the architecture and standards that are adopted for the card's chip. We are unclear about basic conditions, such as whether the chips envisioned for the card would be EMV compliant, and could thus be used within the existing chip & pin reader network.

What security measures are being considered in the event that the system will be based on chip & PIN?

It seems to us that the concept of a secure ID system using a PIN would be substantially undermined if the cards were to be used across a network of 800,000 readers and where use of the PIN occurs largely in an insecure public environment. Scope for two PINs on the chip would appear to be an essential security feature – one PIN for low level retail or service functions, and a second PIN for online or other interactions with the Register. However, the use of two PINs for a single card involves a number of additional threats at a human and at a technology level. We await further clarification from government about how these delicate security issues are to be addressed.

What limits, if any, are envisioned on use of the card by the private sector?

This issue is similar in some respects to the question of use of the Register by private companies. Once clause 6 (compulsion) is in force, there appears to be no limitation on the compulsion imposed on individuals to produce an ID card on demand (see clause 18). How does the government propose to monitor and evaluate the use of cards?

Precisely how can ID cards and the NIR be used for CRB checks, and how can the individual be integrated into the process at an administrative level?

It is claimed that the ID card will reduce the time for a check from four weeks to three days. We would like some explanation of this significant disparity in delays.

What backup systems and processes will be instituted to ensure that denial of service does not occur in the event of technology or system failure?

Such a system will have to be sophisticated using physical, logical, communications security mechanisms while maintaining a sufficiently usefulness particularly in a time of crisis.

Who owns and/or controls biometric data?

The centralisation of this data takes it beyond the individual's reach and control, and it will possibly be collected and stored in other databases.

Will the identity number be visible?

We believe that widespread visibility of an ID number will result in a rise in the extent of identity fraud. Projected identity fraud will have a significant bearing on any cost/benefit assessment. We therefore await a decision by the government on this question.

Will local verification of ID cards be subjected to oversight and audit, and if so, how?

The legislation provides for checks relating to accesses to the Register, but makes no provision for identifying and auditing local verification of cards where the Register is not interrogated. We believe that it is crucial that a secure means be found to provide a record of local verification of cards.

How will organisations determine whether a person is required to be registered on the NIR?

Following the compulsion stage, how will organisations know whether an applicant for a service is a UK national required to register for an ID card, or (say) an EU national who is not? If primary documentation other than an ID card is required, how will this be checked and verified? This question has substantial practical application. If a person who is subject to clause 6 declines to produce a card and claims to be ineligible, we are unable to see how an organisation could do other than to revert to conventional document checking.

How will government monitor the performance of ID checks within the private sector (failure of biometric technology, failure to match, failure of local card verification etc)?

It will not be easy to collect these statistics and to monitor for overuse, abuse, and failures; but these will be essential for monitoring the progress of the scheme.

Section IV: Concluding Remarks

What we find most pleasing about the reception that our earlier report received from the Home Office is that we were in good company. Organisations like the Law Society and numerous local authorities, the Scottish Parliament and the Welsh Assembly have voiced grave concerns about the Bill, and countless firms submitted comments in the Home Office's consultation processes raising similar concerns to our own. There are many similarities between the contents of our report and the reports from the Home Affairs Committee on Identity Cards[148] and the Parliamentary Library.[149]

Since June 2005 a number of other institutions have raised issues with the Bill. The Joint Committee of Human Rights, the Lords Constitutional Committee, the Delegated Powers and Regulatory Reform Committee have all expressed concerns. The Information Commissioner and the head of the Better Regulation Task Force have also pointed out areas that needed attention. The Institute of Electrical and Electronics Engineers' flagship publication declared that the Identity Cards scheme is globally the worst government technology project of 2006.

> "Why It's a Loser: The design of the system is based on unreliable and inadequate technologies that could result in privacy and security problems."[150]

These institutions are all part of the regular deliberative process through which law is supposed to be debated and decided.

At the outset, the LSE Identity Project supported the implementation of an identity scheme in principle but expressed significant concerns regarding the Home Office proposal. In light of the numerous inconsistencies and conflicts that have emerged, serious unanswered concerns that remain, project dynamics that are dysfunctional and potential outcomes that may be harmful to the public interest we can now no longer support even the principle of an identity scheme owned and operated by the Home Office.

Despite all this, however, the policy has changed hardly at all since it was first proposed three years ago. It still involves a highly centralised system. It still involves numerous biometric technologies. Its primary purposes remain unsubstantiated. Its benefits remain unclear and its costs opaque. The scheme's own advisers are worried about time slippage and the underestimation of risks.[151] Prospective users of the scheme are unwilling to state publicly the benefits they expect from use of the system.

148 House of Commons Home Affairs Committee, 'Identity Cards', Fourth Report of Session 2003-04, July 20, 2004.

149 05/43, June 13, 2005, 'The Identity Cards Bill'.

150 'Loser: Britain's Identity Crisis', Erico Guizzo, IEEE Spectrum, January 2006.

151 'Cost Methodology and Cost Review; Outline Business Case Review', published extract, KPMG, November 7, 2005.

Perhaps most alarming in all this is that the scheme is about to become central to the Government's strategy for IT. In its report on 'Transformational Government", the Government placed identity cards at the centre of its public services strategy.[152] This strategy proposes that

> "services enabled by IT must be designed around the citizen or business"

and yet the Card scheme has not changed despite consultations with each. The strategy even calls for increased co-operation across Government departments, moving towards a 'shared services culture'. The Home Office has only recently begun consulting with select Departments and agencies.

The Government's own strategy, however, is limited by what the Home Office is currently offering. The Government is forced into implementing its strategy with what is provided by the Home Office ID cards scheme. The conflict between what it wants and what it will get is seen in the following statement:

> "Government will create an holistic approach to identity management, based on a suite of identity management solutions that enable the public and private sectors to manage risk and provide cost-effective services trusted by customers and stakeholders. These will rationalise electronic gateways and citizen and business record numbers. They will converge towards biometric identity cards and the National Identity Register. This approach will also consider the practical and legal issues of making wider use of the national insurance number to index citizen records as a transition path towards an identity card. "[153]

This statement nicely illustrates the problems in the Government's position. It begins with a 'suite' of identity management solutions, and then seeks to replace them with a single, biometric driven identity scheme provided by the Home Office scheme that is designed for policing, not for providing and managing services across the Government.

This is the Henry Ford approach to IT: any colour you want so long as it is black. Here the Government is saying that it must rethink how IT is used across government, so long as it revolves around what the Home Office is offering. This statement of the Transformational Government strategy has been criticised by Professor Helen Margetts of Oxford University for its over-use of utopian ideals, creating unrealistic expectations, and pursuing the "modernist thrust [that] wins out over a considered strategy for making e-government something that citizens are likely to use."[154]

Rethinking the Direction of the ID cards scheme

From the outset, the LSE Identity Project has accepted the principle of implementing an identity scheme but has expressed grave concerns regarding the particular form of the scheme being proposed by the Home Office on a number of grounds.

Many of the perceived flaws in this proposed scheme are a result of the Home Office's continued resistance to both listening and to adhering to traditional processes and procedures of policy deliberation. The

---

152 'Transformational Government: Enabled by Technology', Cabinet Office, November 2005, Cm 6683.

153 p.13

154 "Forward-thinking in all but title", Helen Margetts, November 23, 2005.

proposed scheme is overly burdensome, dangerously centralised, and is designed only to meet the goals of the Home Office: a vast register of biometric data that will be used for policing purposes.

A more open and federated model is required for an identity scheme that will provide gains for e-government, promote access to government services, and generate trust. The Home Office has failed over three years to establish such a scheme and appears unwilling to alter its predetermined path.

We recommend that another department be made responsible for establishing an identity infrastructure for the UK. Such a department must have more experience in dealing with large IT systems with multiple users across all sectors of the Government, the private sector, and society. This is what the Government's IT strategy tries to achieve but is hindered by this Home Office-centred scheme.

Few departments have this necessary track record. In other countries that are pursuing a cross-society identity infrastructure these systems are usually run by their Treasury, Industry or Commerce departments. As examples, in Canada the Treasury is responsible for the Federal Government's identity infrastructure; in France it is the responsibility of the Minister for State Reform. The analogous departments in the United Kingdom with the requisite experience in large IT systems and interfacing with government and non-government users is the Treasury.

The Treasury has extensive experience in complex IT systems. It has 'learned by doing', through dealing with project failures and with the management of long-term implementation. It has worked with other government departments, the private sector, and regularly interacts with users in the general public.

We therefore come to the inescapable conclusion that the ID Card Scheme in the UK should be taken forward by the Treasury.

Identity management may well be "an idea whose time has come". But as with any such idea, there are a multiplicity of choices to be made, and directions to choose. After three years, the Government remains on the wrong path.

ANNEX: DOUBLE COUNTING COSTS FOR AN ID SYSTEM

June 28, 2005

In recent days, Home Office Ministers and even the Prime Minister have described the LSE cost projections as 'absurd', 'nonsense', and 'incompetent'. One Home Office Minister claimed that our costings are based on double-counting. They also dispute our assumption that identity documents will have to be renewed every four to five years.

In this document we will explain how the Government came to its costing of £93 per person over ten years. Then we will repeat our assumptions, and explain how we came to our figures on the contentious issue of double counting.

Revealing the Government's £93

To date the Government has been unwilling to release any detail regarding how they have come to their headline figure of £93. This figure was released in the May 2005 Regulatory Impact Assessment, following a prior figure of £85 in the November 2004 RIA. This cost covers the issuing of both a passport and an identity card.

We have no way of deciphering how they came to this figure. We do have figures from the UK Passport Service Corporate and Business Plans that state that the total revenue of the UKPS is expected to be £397m by 2006/2007, with full expenditures expected, and an average unit cost per passport at £67.93.

Over ten years, the UKPS figures will therefore add up to approximately £4 billion. But passports are only issued to 80% of the population, so if we scale the UKPS figures for that population, it becomes £4.8 billion. If, as stated yesterday in repeated announcements, the cost of the ID card will be 30% of the full passport cost, then we can assume that the UKPS will also need to raise its expenditures by 30%. This results in £6.25 billion over ten years.

Following the Government's assumption in the 2002 Consultation Document that there will be approximately 67.5 million cards issued over the next ten years, if we divide the UKPS costs by 67.5 million, the result is £92.60.

This assumes that the passport infrastructure can cover the entire identity system. This is a difficult assumption to justify.

How the LSE Derived its Figure

On Renewal

The Government has disputed our assumption that the cards will need to be renewed.

It is important to note that we do not reduce the passport renewal period to 5 years, as the government claims. However, many countries already do this. Canada, for instance has a five year renewal. International standards-bodies have considered making this a requirement so that new anti-counterfeiting techniques can be incorporated into passports. Nevertheless, in our costings we do not incorporate a five-year renewal as an assumption: we are giving the government the benefit of the doubt when they say that they will not reduce the life-span of passports. This is despite a statement from the head of UKPS, quoted on June 28 saying: "All we can do is keep on changing the design and we are going to have to change more frequently than every 10 years."

On identity cards the situation is quite different. Repeatedly, experts have noted that the renewal of the ID card must be between every 3-5 years. Northrop Grumman, the operator of the national fingerprint information system (Nafis) argued that cards would need to be replaced on average every three years. The Home Office consultation document of 2002 estimates that the chip on the cards would have to be replaced twice during a 10-year period, though that same document admits that the range is more likely to be every 3-5 years. The chips need replacing because of intensive use. This is one of the many reasons why credit cards have similar expiry dates.

In our costings, we merely assume that the chip card will need to be replaced every 4 years. This does not mean that individuals will have to be entirely re-enrolled; we merely account for the cost of the card with the chip (and we cost this at £4-6 per card-chip, which is far less than the Home Office's 2002 estimate of £15). We include in our estimate the need for additional cards through theft and loss, and defective cards, based on UKPS estimates and other studies.

A crude calculation of the cost of the cards themselves (without the system behind it), covering the full population of Britain over ten years is £12. This is a significant under-estimate, but for the purpose of the report we felt that this was an appropriate assumption.

The significant costs arise from the registration process, the national register, and its management, not from the renewal.

Calculating the Passport and Register Figures

Like the Home Office indicative figures, we separate out the cost of the ID card from the passport. Indeed our assumptions do differ on the larger identity system.

On the cost of the Passport itself, we break down the costs as follows:

- Cost of the passport booklet: 35.60 GBP (according to UKPS figures)

- Costs of changes to passports: 32.40 GBP (according to UKPS figures)

- Errors involve 0.25% of passports (based on UKPS figures)

- Re-issuing passports upon being lost or stolen (predicted figures)

We understand that UKPS is planning on a number of innovations in the next few years and this will account for the rise in cost in passports. According to UKPS reports, these changes include

- interview for new applicants

- changing current database from a passport-centric system to a person-centric system

- secure home delivery of passports

- placing chip in passport with a digital photograph

- basic staffing costs (presumed) to manage this new passport

We predicted that the £32.40 per passport would go toward covering these costs. While the Government seems to be arguing that this £32.40 will cover the cost of biometric enrolment, staffing the 70+ registration centres, managing the national identity register, on top of all the changes to the UKPS, we believe that this estimate is unrealistic, and we make this case carefully in the full body of the report over a number of sections. Presumably, the Government also envisions that this will cover the cost of readers throughout the Government departments outlined on the face of the bill.

We believe that there will also be a line item for 'Managing the National Identity System'. This is where we include:

- the cost of establishing a national register of all residents, with the 51 data-types as envisioned by the bill, including all the biometrics, and the registration centres for enrolment

- running costs of the enrolment process

- costs for updating information on the register (change of address, circumstances)

- costs for verification processes (e.g. when employer or government department wishes to call up to verify details)

- correction of information on the register (e.g. compliance with Data Protection Act)

- establishing the biographic footprint of all applicants through credit reporting and connections to other government systems

- other nominal costs that are inherent to large databases involving 67.5 million records.

Over ten years the cost of these operations is likely to run quite high. Already the NPL/BTexact study estimated that there would be 3000 new enrolments every day after the initial rollout. The amount of changes-of-addresses are likely to be very high as well. These operations are likely to involve increased communications costs and even a call centre.

As a result, we also have a budget line-item for staffing. While the UKPS probably envisioned some staff costs in their £32.40 increase, our understanding of the NIR requirements is that there will be many more staff members working in this new 'national identity agency'. Our estimates are conservative, however, calling for about 80 to 100 staff members over one year (including roll-over) at each centre, including the call centre, presuming between 70 and 100 such centres. We also include training for these staff members,

background checks because of the highly sensitive operations involved, and training for some of the users of the NIR or the verifiers of biometrics across Government.

Therefore, the key difference between our costings and the Home Office costings is that they believe that the Passport process will cover 70 per cent of the cost of implementing and running the Register. We believe that the changes to the UKPS are insufficient to run the Register, and rather the UKPS figures are merely sufficient for basic actions such as putting a chip in the passport, placing a biometric on the chip, transforming their current database, and secure home delivery (which alone would cost 5 GBP per person at a minimum).

Concluding Remarks

The Identity Project Report goes into much greater detail than here to explain why we believe the Government's proposed identity system will be technologically challenging, and in turn, creating costs that are likely to be higher than estimated. The Government has only provided what appears to be a 'back-of-the-envelope' costing.

In our analysis, we find that the confusion in the costings is due to the Government relying on the passport infrastructure to develop the basis of an identity card system. We show that this is contrary to international obligations and technological experience. It is also contrary to what is occurring internationally.

The UK Government is about to implement the most expensive passport system in the world. And this is being noted. New passports were announced recently in Germany. Those passports cost 59 euros, rather than the 23 euros originally cited, and from 2007 every passport will also include two index-fingerprints. There is no back-end database to the German passport.

When controversy arose in Germany regarding the cost of the passport, the Minister in charge pointed out, "that is 5.90 euros per year," adding that German passports will still remain cheaper than the international average. He then pointed out that biometric passports are going to cost 103 euros in Great Britain.