The London School of Economics
& Political Science

The Identity Project

An assessment of the UK Identity Cards Bill & its implications

Interim Report

London, March 2005

The Identity Project

An assessment of the UK Identity Cards Bill & its implications

Interim Report

Project Management by

Hosted and Published by

Advisory Group

Professor Ian Angell, Convenor of the Department of Information Systems, LSE
Professor Christine Chinkin, Law Department, LSE
Professor Frank Cowell, Economics Department, LSE
Professor Keith Dowding, Government Department, LSE
Professor Patrick Dunleavy, Government Department, LSE
Professor George Gaskell, Director, Methodology Institute, LSE
Professor Christopher Greenwood QC, Convenor of the Law Department, LSE
Professor Christopher Hood, Centre for Analysis of Risk & Regulation, LSE
Professor Mary Kaldor, Centre for the Study of Global Governance, LSE
Professor Frank Land, Department of Information Systems, LSE
Professor Robin Mansell, Department of Media & Communications, LSE
Professor Tim Newburn, Social Policy Department, LSE
Professor David Piachaud, Centre for Analysis of Social Exclusion, LSE
Professor Robert Reiner, Law Department, LSE

Research Group

Research coordinator: Dr Edgar Whitley, Reader in Information Systems.

Dr Stefan Brands
Dr Ian Brown
Dan Cooper
Mike Cushman
Marc Dautlich
Federico Ferretti
Marc Gilman
Philip Harrison
Dr Gus Hosein
Jeegar Kakkad
Ariosto Matus-Perez
Dr Eileen Munro
Professor Toshimaru Ogura
Nicholas Pauro
Dr Chris Pounder
Professor Angela Sasse
Dr Susan Scott
Dr Barbara Simons
Dr Steve Smithson
Sarah Thatcher
Prodromos Tsiavos
Rosemary Walsh
Derek Wong

Acknowledgements

We would like to thank the LSE's Department of Information Systems for hosting and publishing this study. Our gratitude also goes to the research team who have worked tirelessly and under severe time constraints, and to the Advisory Board, who have supported the work from its inception. Thanks also to the Enterprise Privacy Group for undertaking the management and coordination of the project.

The LSE would also like to express its appreciation to the many people and organisations that contributed to this study, and especially to the following organisations for their participation in the business Working Groups for the report:

The Financial Times, Covington & Burling, Inland Revenue, The Department for Trade & Industry, IBM, Royal Mail, Kable, Consult Hyperion, The Confederation of British Industry, The Institute of Directors, The British Computer Society, Giesecke & Devrient, The Office of the Information Commissioner, The Information Security Forum, MasterCard, Oracle, British American Tobacco, British Telecom, The Post Office and Prudential.

Participation in the project by an individual or organisation does not imply agreement with the findings of the study in part or full.

Table of contents

Summary of conclusions

The Report *concludes* that the establishment of a secure national identity system has the potential to create significant, though limited, benefits for society. However, the proposals currently being considered by Parliament are neither safe nor appropriate. There was an overwhelming view expressed by stakeholders involved in this Report that the proposals are *too complex*, *technically unsafe*, *overly prescriptive* and *lack a foundation of public trust and confidence*. The current proposals miss key opportunities to establish a secure, trusted and cost-effective identity system and the Report therefore considers alternative models for an identity card scheme that may achieve the goals of the legislation more effectively. The concept of a national identity system is supportable, but the current proposals are not feasible.

Many of the public interest objectives of the Bill would be more effectively achieved by other means. For example, preventing identity theft may be better addressed by giving individuals greater control over the disclosure of their own personal information, while prevention of terrorism may be more effectively managed through strengthened border patrols and increased presence at borders, or allocating adequate resources for conventional police intelligence work.

The technology envisioned for this scheme is, to a large extent, untested and unreliable. No scheme on this scale has been undertaken anywhere in the world. Smaller and less ambitious systems have encountered substantial technological and operational problems that are likely to be amplified in a large-scale, national system. The use of biometrics gives rise to particular concern because this technology has never been used at such a scale.

Any system that supports critical security functions must be robust and resilient to malicious attacks. Because of its size and complexity, the identity system would require security measures at a scale that will result in substantially higher implementation and operational costs than has been estimated. The proposed use of the system for a variety of purposes, and access to it from a large number of private and public sector organisations will require unprecedented attention to security.

All identity systems carry consequential dangers as well as potential benefits. Depending on the model used, identity systems may create a range of new and unforeseen problems. These include the failure of systems, unforeseen financial costs, increased security threats and unacceptable imposition on citizens. The success of a national identity system depends on a sensitive, cautious and cooperative approach involving all key stakeholder groups including an independent and rolling risk assessment and a regular review of management practices. We are not confident that these conditions have been satisfied in the development of the Identity Cards Bill. The risk of failure in the current proposals is therefore magnified to the point where the scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals.

Introduction

The introduction of a national identity system will herald a significant shift in Britain's social and economic environment. Many fundamental concepts such as privacy, anonymity and the individual's accountability to government will be repositioned. The potential for merging, matching and sharing of personal information across the private and public sector will be made possible. For better or worse, the relationship between the individual and the State will change.

Surprisingly little research has been undertaken with specific reference to the identity card legislation currently being considered by Parliament. The aim of this study is to provide a comprehensive review of the Bill, assess the costs and implications arising from its provisions, and to suggest areas for improvement.

As this Report observes, support in principle for a national identity card is substantial. Opinion polls conducted both by organisations supporting the proposals and by groups opposing them have uniformly highlighted a headline support figure of between sixty and eighty percent of the population. This principled support should, however, be separated from issues of practicality and cost arising from the proposals. It is these latter aspects that will form the focus of this project.

There appear to be some significant potential benefits to the UK in adopting a harmonised system of identification. However, the risks and the financial implications for business and for individuals may be substantial. In producing this report we have kept foremost in mind the potential to create an identity system with limited cost and risk, but one that brings the maximum benefit to individuals and society.

This report is based on research of available evidence. It does not deal with principle or speculation.

There is a surprising degree of agreement between the findings of this report and the conclusions of the Home Affairs Committee on the draft Identity Cards Bill. This report agrees in whole or part with 79 of the 85 relevant recommendations in the HAC report. This concurrence is a crucial test of the strength and validity of both reports.

This Interim Report is not exhaustive, but we believe it does provide a comprehensive foundation for further debate about many key aspects of the government's proposals. Over the coming weeks we will continue to build on these interim findings to produce a final report that will assess a wider range of issues relating to the impact and implications of an identity scheme for the UK.

Conclusions in detail

Overview

This Report assesses the implications, costs, opportunities and consequences arising from current legislative proposals to introduce a national identity card scheme. The Report does not challenge or debate the principles that underpin the proposals. The goals of combating terrorism, reducing crime and illegal working, reducing fraud and strengthening national security are accepted *a priori* as legitimate responsibilities of government.

The Report *concludes* that the establishment of a secure national identity system has the potential to create significant, though limited, benefits for society. However, the proposals currently being considered by Parliament are neither safe nor appropriate. There was an overwhelming view expressed by stakeholders involved in this Report that the proposals are *too complex*, *technically unsafe*, *overly prescriptive* and *lack a foundation of public trust and confidence*. The current proposals miss key opportunities to establish a secure, trusted and cost-effective identity system and the Report therefore considers alternative models for an identity card scheme that may achieve the goals of the legislation more effectively. The concept of a national identity system is supportable, but the current proposals are not feasible.

An appropriate identity system for the United Kingdom would be one based on a foundation of public trust and user demand rather than one based on enforcement through criminal and civil penalties. The goal of public trust would be made possible, in part, through the use of reliable and secure technologies.

The remainder of this summary outlines the key areas of concern with the proposals as they stand. Each point is discussed in more detail in the main report.

Purposes of the system

The current proposals seek to address multiple, divergent goals, yet the evidence from other national schemes indicates that identity systems perform best when established for clear and focused purposes. The goal of "prevention or detention of crime", for example, involves a potentially huge number of applications and functions that may not be appropriate for an identity system that also seeks to achieve a goal of public services delivery.

Equally, many of the public interest objectives of the Bill would be more effectively achieved by other means. For example, preventing identity theft may be better addressed by giving individuals greater control over the disclosure of their own personal information, while prevention of terrorism may be more effectively managed through strengthened border patrols and increased presence at borders, or allocating adequate resources for conventional police intelligence work.

The technological environment

The technology envisioned for this scheme is, to a large extent, untested and unreliable. No scheme on this scale has been undertaken anywhere in the world. Smaller and less ambitious systems have encountered substantial technological and operational problems that are likely to be amplified in a large-scale, national system. The use of biometrics gives rise to particular concern because this technology has never been used at such a scale.

The proposed system unnecessarily introduces, at a national level, a new tier of technological and organisational infrastructure that will carry associated risks of failure. A fully integrated national system of this complexity and importance will be technologically precarious and could itself become a target for attacks by terrorists or others.

Cost

Any system that supports critical security functions must be robust and resilient to malicious attacks. Because of its size and complexity, the identity system would require security measures at a scale that will result in substantially higher implementation and operational costs than has been estimated. The proposed use of the system for a variety of purposes, and access to it from a large number of private and public sector organisations will require unprecedented attention to security.

Private sector costs relating to the verification of individuals may account for a sum equal to or greater than the headline cost figure suggested by the government. Staff must be trained to use biometric systems, and in larger organisations must be on hand at all times to verify customers and new employees. New facilities may have to be built to accommodate applicants who feel sensitive about having their biometrics taken in public areas.

The government has substantially underestimated the cost of biometric readers. Because of physical irregularity or mental impairment, a significant number of people are unable to provide a stable biometric unless expensive equipment is used.

The cost of registration of applicants appears to have been underestimated. The Bill makes provision for the disclosure and processing of more than fifty sources of identification. This element, coupled with the capture of biometrics and the investigation of the biographical history of applicants, may result in registration alone costing more than the projected overall cost of the identity system.

The direct cost to people applying to be registered on the system is also likely to be higher than anticipated. Biometric registration may have to be repeated every five years for much of the population. As people age, their biometrics change and become less reliable. As a consequence, these people are more likely to face problems with the use of the identity card system and may require more frequent updates of their biometric information stored on the system. Approximately 17 per cent of the population are aged over 65 and will fall into this growing class, as will such people as the visually

handicapped and those with mental impairment. The implications for reliability, cost and trust in the proposed identity system are significant.

One possible solution to these problems is the endemic use of multiple biometrics. However, this would add significantly to the cost of the system.

The legal environment

In its current form, the Identity Cards Bill appears to be unsafe in law. A number of elements potentially compromise Article 8 (privacy) and Article 14 (discrimination) of the European Convention on Human Rights.

Because of the difficulty that some individuals may face in registering or verifying their biometrics there is a potential conflict with national laws such as the Disability Discrimination Act and the Race Relations Act.

The proposals appear to be in direct conflict with the Data Protection Act. Many of these conflicts arise from the creation of a national identity register, which will contain a substantial amount of personal data, some of which would be highly sensitive. The amount of information contained in the register, the purposes for which it can be used, the breadth of organisations that will have access to the Register and the oversight arrangements proposed are contentious aspects.

The Bill also creates a possible conflict with the right of freedom of movement throughout the EU for EU citizens. It is arguable that the Identity Cards Bill may discourage non-UK EU workers from coming to the UK to work and so may infringe EU principles on the freedom of movement of workers. Furthermore, EU Directive 68/360 governing the rights and conditions of entry and residence for workers may make it unlawful for the government to require non-UK EU citizens to obtain a UK identity card as a condition of residence.

Liability and responsibility for maintaining accuracy of data on the Register, conducting identity checks and ensuring the integrity of the overall operation of the scheme has not been resolved. The legislation places requirements on individuals and organisations that are substantial and wide-ranging, and yet no indication has been given relating to how liability would be established, who would assess that liability, or who would police it.

Oversight

The oversight arrangements set out in the Bill appear to be inadequate in several key respects. An Identity Cards Commissioner as envisioned by the legislation may be an insufficient mechanism to adequately promote public trust. The Commissioner will not be able to act on individual complaints and cannot assess the practical aspects of the scheme. The Commissioner is excluded from assessing the use of criminal and civil penalties related to the scheme, information being provided to security agencies and is not empowered to review his own functions or powers. Moreover, the Commissioner

will report to the Home Secretary, rather than Parliament, and thus may lose the appearance of full independence from government.[1]

The current population of oversight bodies in the UK is complex, inefficient and frequently in conflict. Commissioners responsible for various aspects of privacy and surveillance, for example, rarely cooperate with each other. Reform of the oversight process rather than the addition of more oversight agencies might be the most effective way forward.

International obligations

The Government has consistently asserted that that biometrics proposals, both in the new UK passport format and in the identity cards legislation, is a harmonising measure required by international obligations, and is thus no different to the plans and intentions of the UK's international partners. There is no evidence to support this assertion.

We conclude that the Government is unnecessarily binding the identity card scheme to internationally recognised requirements on passport documents. By doing so, the Government has failed to correctly interpret international standards, generating unnecessary costs, using untested technologies and going well beyond the measures adopted in any other country that seeks to meet international obligations.

Alternative scenarios

One alternative to the proposed scheme would be to permit a wider range of practical applications for day-to-day dealings with businesses. This scenario would make use of purpose-specific identity technologies that would give consumers a more secure and simple means of accessing commercial organisations in an electronic environment such as the Internet. By offering direct consumer benefits as well as government services, such systems could assist in securing public support for the scheme.

In considering performance of more limited identity schemes in other countries, and the possible applications and limitations of technologies available now or in the near future, it is likely that the benefits to individuals and business from the UK scheme are extremely limited.

This report concludes that the proposals currently being considered by Parliament do not represent the most appropriate, secure, cost effective or practical identity system for the United Kingdom. The system outlined by the legislation appears unlikely therefore to achieve its stated objectives.

All identity systems carry consequential dangers as well as potential benefits. Depending on the model used, identity systems may create a range of new and unforeseen problems. These include the failure of systems, unforeseen financial costs, increased security threats and unacceptable imposition on citizens. The success of a national identity system depends on a sensitive, cautious and cooperative approach

[1] Liberty briefing on the Identity Cards Bill, http://www.liberty-human-rights.org.uk/privacy/id-card-bill-key-points.pdf.

involving all key stakeholder groups including an independent and rolling risk assessment and a regular review of management practices. We are not confident that these conditions have been satisfied in the development of the Identity Cards Bill. The risk of failure in the current proposals is therefore magnified to the point where the scheme should be regarded as a potential danger to the public interest and to the legal rights of individuals.

Overview of the legislative proposals

The Identity Cards Bill outlines an identity system that has eight components: the *National Identification Register*, a *national identity registration number*, the collection of a range of Biometrics such as fingerprints, the *national identity card*, provision for *administrative convergence* in the private and public sectors, establishment o*f legal obligations* to disclose personal data, *cross notification requirements*, and the creation of *new crimes and* penalties to enforce compliance with the legislation.

The Bill sets out criteria for the establishment of the system based on "Public Interest". Clause 1(4) of the Bill defines public interest as being "in the interests of national security", "for the purposes of the prevention or detection of crime", "for the purposes of the enforcement of immigration controls", "for the purposes of the enforcement of prohibitions on unauthorised working or employment" and "for the purpose of securing the efficient and effective provision of public services."

The proposals entail substantial collection and accumulation of personal information. Clause 1 and Schedule 1 of the Bill sets out more than fifty categories of information required for the register (subject to change by regulation). Along with the standard identifiers such as name, birth coordinates, current and previous addresses and residential status, the register is also mandated to contain such data as biometric details, full chronology of residential location in the UK and overseas, a record of all dealings between the individual and the Register and a full audit trail of activity on the Register.

The government has estimated that the cost of the scheme over ten years will be £5.5 billion, although there is some confusion over the relationship between this figure and the cost of providing enhanced biometrics on passports and over the likely arrangements for dealing with passport application and enrolment costs. The current proposal is that cost of the scheme will be covered through direct contribution from ID card applicants. An "enhanced" biometric passport, which includes entry on the national register, will, according to current official projections, cost about £85. Identity registration without a passport will on current estimates cost between £35 and £40, with an additional charge for the card itself. There will be a charge for the renewal or replacement of cards.

Clause 15 (3) of the Bill specifically prohibits any provision (within the Identity Cards Bill) requiring people to carry the card at all times. This clause also rules out compulsion to submit a card to receive a benefit or any public service. However, following approval of an order, c. 6 (1) empowers the Secretary of State to order anybody or everybody to register for a card. Although the government has speculated that this clause may not be brought into force for some years, there is no time period established in the Bill. Parliament could approve the order to do so at any time it wishes.

The card system will be buttressed by a substantial array of new state powers and criminal penalties. The Bill creates a score of new offences including refusal to obey an order from the Secretary of State (6(4)), failure to notify authorities about a lost, stolen, damaged or defective card (13(1)), failure to renew a card (9(2)), failure to submit to fingerprinting (9(4)(b)), failure to provide information demanded by the government

(9(4)(d)), failure to attend an interview at a specified place and time (9(4)(a)) and failure to notify the Secretary of State of any change in personal circumstances (including change of address) (12(1)). Failure to obey an order to register or providing false information will also constitute an offence. Penalties range from £1,000 fine to two years imprisonment. A penalty of up to £2,500 can be levied for failure to attend an appointment for a biometric scan. This fine can be repeated for every subsequent failure to attend.

The government proposes to eliminate this risk of forgery and multiple identities by establishing a "clean" database of identities. Entry onto the database will require multiple biometric capture, biographical footprint checking and a range of primary documentation. The Home Office believes that the database will contain no multiple identities because a "one to many" check will be used before a person is enrolled.

Biometrics would be taken upon application for a card and for entry on the National Identification Register, and would be verified thereafter for major "events" such as obtaining a driving license, passport, bank account, benefits or employment.

Background and chronology

On November 29th 2004, following a two and a half year gestation, the Government introduced and published its Identity Cards Bill.[2] This legislation was debated (in Second Reading) in the Commons on 20th December, and was then considered in Committee in mid January. The legislation reached Third Reading on 10th February 2005 when it passed by 224 votes to 64. The Second Reading debate in the House of Lords is scheduled for 21st March. The Bill is similar in many respects to the Draft Identity Cards Bill[3] that the Government published in April 2004 following the public consultation[4] and the Home Affairs Committee hearings.[5]

Overview of the scheme

The Identity Cards Bill is something of a misnomer in that the card element is only one part of a much larger integrated scheme. The proposal is multi-faceted and far-reaching, and in its current form will involve substantial use of personal information within a complex legal and technological environment.

The Bill outlines an identity system that has eight components.

The National Identification Register. This element is the information hub of the system. Clause 1 of the Bill imposes an obligation on the Secretary of State to establish a central population register containing a wide range of details of every UK citizen and resident aged from 16 years and 3 months.

[2] Identity Cards Bill (as amended by Standing Committee B), http://www.homeoffice.gov.uk/comrace/identitycards/.
[3] Draft Identity Cards Bill, http://www.homeoffice.gov.uk/comrace/identitycards/publications.html.
[4] Legislation on identity Cards: a consultation. Home Office, April 2004, http://www.homeoffice.gov.uk/comrace/identitycards/publications.html.
[5] Home Affairs Committee, Fourth Report, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm.

The code. Clause 2 (6) requires that every individual must be given a unique number, to be known as the National Identity Registration Number (NIRN). This number will become the "key" for government and private sector organisations to access information on the register and, in certain circumstances, to share that information.

Biometrics. Clause 5 (5) requires individuals to submit to fingerprinting and "other" means of physical identification. This is likely to include electronic facial recognition, signature and iris recognition.

The card. Clause 8 establishes the actual identity card, generated from and containing part of the information in the Register.

Legal obligations. Clause 15 establishes a requirement to produce the card in order to obtain public services.

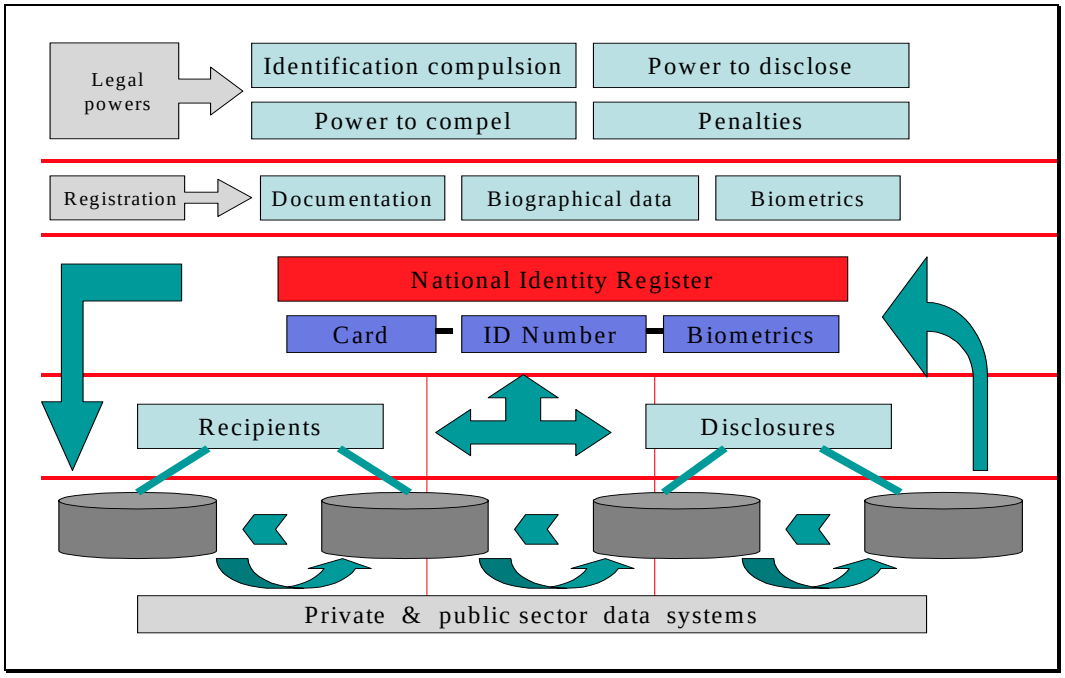
Administrative convergence. The number and the card register will be used by a variety of agencies and organisations both for access and disclosures, and in the future as a possible administrative base. 1 (5) permits the bringing together of all registration numbers (National Insurance, NHS number etc) used by a person.

Cross notification. Agencies will be required to notify each other of changes to a person's details. Clause 19 authorises the Secretary of State to disclose details from the register to other agencies without the consent of the individual.

New crimes and penalties. The Bill establishes a large number of new crimes and offences to ensure that people comply with the ID requirements.

These elements are set out clearly in clause 5 of the Regulatory Impact Assessment[6] for the Bill.

[6] Identity Cards Bill, Regulatory Impact Assessment, Home Office. November 2004, http://www.homeoffice.gov.uk/docs3/ria_251104.pdf.



Overview of the scheme's objectives

The Bill sets out a number of purposes for the Card and the Register. Some are more open-ended than others. For example, the scheme is described as "a convenient method for such individuals to prove registrable facts about themselves to others". The Bill also establishes that the card scheme will allow "the provision of a secure and reliable method for registrable facts about such individuals to be ascertained or verified wherever that is necessary in the public interest."

"Public Interest" encompasses a number of dimensions. Clause 1(4) of the Bill defines it as being "in the interests of national security", "for the purposes of the prevention or detection of crime", "for the purposes of the enforcement of immigration controls", "for the purposes of the enforcement of prohibitions on unauthorised working or employment" and "for the purpose of securing the efficient and effective provision of public services."

On the face of it, this definition would imply that the card and the register would be necessary to seek employment,[7] to gain access to health,[8] benefits and other services, and that it would be used by police, security and immigration officers in the execution of their functions. However the words "for the purposes of the prevention or detection of crime" could possibly be connected to financial control and money laundering regulations to provide a means by which the ID system can be used for a much wider range of purposes. The could include operating a bank account, using professional

[7] 'Need a job? Get a card - arresting ID pitch to business', John Lettice, The Register, http://www.theregister.co.uk/2004/12/03/business_immigrant_checks/.
[8] 'U.K. to Put Biometric Readers in all Hospitals, Blears Says', Bloomberg. September 28, 2004, http://quote.bloomberg.com/apps/news?pid=10000102&sid=adIU._FV1Wnw&refer=ukU.K.

services[9] such as a solicitor or accountant, applying for a permit or license, internal travel, buying property, stocks or shares, applying for credit or using large amounts of cash.

It has been proposed that the card and register may ultimately be used to verify entitlement to most if not all public services[10] while the Bill and the Regulatory Impact Assessment paves the way for widespread use by the private sector. The Assessment states that the government will "work closely with private sector organisations to ensure that the [ID card] scheme develops along lines which will meet their business requirements". This could mean that links and transactions within private sector records are likely to appear alongside the government-held registrable facts associated with an individual.

The Home Office recently stated: "We are proposing to make online checks against the register the norm, except in those low risk/low value cases where a visual check is judged to be sufficient."[11] Responding to a question of whether libraries and video rental shops might require the card the Home Secretary told the Home Affairs Committee: "Wherever someone is required to prove their identity and those operating that particular service have registered so they can use a (biometric) reader then that would be fine."[12]

Personal information contained in the Register and on the Card

The Government has asserted that the creation of the ID system will result in the collection of less, not more, personal information than currently exists. In April, for example, the Home Secretary told BBC1's Breakfast programme: "There will be no more information, in fact a lot less, and much less accessibility than there are for shopping cards at the moment". The Home Secretary repeated this claim during a speech[13] in November, resulting in a robust response[14] from the retail sector.

The government's claim is contentious in that it appears to confuse data on the identity card (i.e. a chip embedded in a piece of plastic) with the national Registry, which is where almost all the personal information will be held. (The Bill, however, does not specify what information should be contained in or on the card itself, and leaves this to regulation).

However, clause 1 and Schedule 1 of the Bill sets out more than fifty categories of information that may be required for the register (subject to change by regulation). Along with the standard identifiers such as name, birth coordinates, current and

[9] 'New client? ID card please', Accountancy Age, December 2, 2004, http://www.accountancyage.com/news/1138822.
[10] 'ID card database to support a public service delivery agenda', Out-law.com, December 6, 2004, http://www.out-law.com/php/page.php?page_id=idcarddatabaseto1102340874&area=news.
[11] 'Talks consider use of ID cards for business', James Watson, Computing, December 1, 2004, http://www.vnunet.com/news/1159786.
[12] House of Commons, Home Affairs Committee, Minutes of evidence, May 4, 2004, http://www.parliament.the-stationery-office.co.uk/pa/cm200304/cmselect/cmhaff/uc130-vii/uc13002.htm.
[13] Rt. Hon David Blunkett, Speech to the IPPR, November 17, 2004, http://www.homeoffice.gov.uk/docs3/identitycards_041118speech.htm.
[14] 'Blunkett concern on loyalty cards', BBC News online, November 17, 2004, http://news.bbc.co.uk/1/hi/uk_politics/4018939.stm.

previous addresses and residential status, the register is also mandated to contain such data as biometric details, full chronology of residential location in the UK and overseas, a record of all dealings between the individual and the Register and a full audit trail of access and disclosure activity on the Register.

Access to the information on the national register

Clause 19 of the Bill permits the disclosure of information from the register without the individual's consent to (among other agencies) police organisations, the security services, Inland Revenue, the Department for Work & Pensions, the Serious Organised Crime Agency and Customs & Excise.

Under clause 19 (3) of the Bill information from the register can be handed to or accessed by police for purposes of prevention or detection of crime. This provides substantial scope to use the information. Police may, for example, apply to link fingerprint information on the register to "crime scene" evidence. They must however establish that they have taken reasonable steps to seek the information from other sources.

19 (4) provides for the creation of access and disclosure for "other purposes" specified by Order.

Overall cost of the scheme

The government estimated in 2002 that the scheme would cost somewhere in the order of £3.1 billion. When in 2004 the Home Affairs Committee asked the Home Secretary to clarify the exact amount he refused, citing commercial secrecy. By the time the final Bill was published in November 2004 the government acknowledged that the cost[15] of the scheme over ten years would be £5.5 billion, though the specific breakdown of this figure is somewhat unclear. Industry specialists have warned[16] that the complexity and uncertainty of the scheme's architecture and technology could create a higher cost.

Clause 37 also allows the Secretary of State (with the permission of the Treasury) to pass regulations to apply additional charges for a range of circumstances such as disclosure of information and modification of information on the register.

Recovery of cost

The current proposal is that the scheme will be paid for through direct contribution by ID card applicants. An "enhanced" biometric passport, which includes entry on the national register, will cost around £85. An ID card without a passport will on current estimates cost[17] between £35 and £40. There will be a charge for the renewal or replacement of cards.

[15] 'Home Office admits cost of ID cards will be double estimate', Jean Eaglesham and Maija Pesola, Financial Times, November 30, 2004, http://news.ft.com/cms/s/fbc6527a-4276-11d9-8e3c-00000e2511c8.html

[16] 'ID card costs soar as supplier slams technology', Nick Huber, Computer Weekly, November 4, 2004, http://www.computerweekly.com/Article134763.htm.

[17] 'ID card scheme unveiled by Queen', BBC News Online, November 23, 2004, http://news.bbc.co.uk/1/hi/uk_politics/4034699.stm.

Voluntary and compulsory elements of the scheme

The Home Office has been clear that its intention has always been to create a compulsory regime, but until recently this crucial point has suffered some confusion. Government ministers have almost unanimously ruled out the option for legal compulsion to carry a card, and indeed clause 15 (3) of the Bill specifically prohibits any provision (within the Identity Cards Bill) requiring people to carry the card at all times. This clause also rules out compulsion to submit a card to receive a benefit or any public service. However, this clause does not provide protection to anyone who has been ordered to register for a card under the "compulsion" clause of the Bill. Following approval of an order, 6 (1) empowers the Secretary of State to order anybody or everybody to register for a card. This might include benefits recipients, new employees, people wanting to open a bank account, people of a particular ethnicity, people who have been in contact with law enforcement or, indeed, the entire population. Although the government has speculated that this clause may not be brought into force for some years, there is no time period established in the Bill. Parliament could approve the order to do so at any time it wishes.

At the commencement of the first consultation phase the government's stated definition of "compulsory" was expressed as: "not required to be carried by each individual at all times". Now the official position is that the card will eventually become universal and compulsory. That is, it will become compulsory to be entered onto the National Identification Register. Clause 2 (4) of the Bill allows the Secretary of State to enter a person onto the National Identity Register without that person's consent. Clause 5 allows the Secretary of State to propose "designated documents" that will require entry onto the Register. This power may apply, for example, when a person applies for or renews a passport or when a foreign national seeks a residence permit. Passport holders will automatically be entered onto the identification register. For those people who do not have a passport 6 (1) will allow the government to require people to be registered.

The proposal for a compulsory stage has met a mixed response. In its final report[18] on the Draft Identity Cards Bill the Home Affairs Committee warned: "The move to compulsion is a step of such importance that it should only be taken after the scrutiny afforded by primary legislation: the proposed "super-affirmative procedure" is not adequate." The Committee urged the government to consider compulsion only through the introduction of fresh legislation. This recommendation was rejected by the government. In fact, the Home Secretary pre-empted even the limited mandate of Parliament by issuing a statement in which he announced: "I will now bring forward legislation to bring in a compulsory, national ID card scheme."[19]

[18] Home Affairs Committee, Fourth Report, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm.

[19] 'Home Secretary Sets Out next Steps on ID Cards', Home Office press release, Reference: 331/2004 -: October 24, 2004, http://www.homeoffice.gov.uk/n_story.asp?item_id=1124.

Age restrictions within the legislation

The government has addressed the matter of issue of cards for children from the age of 5. In its consultation[20] paper it identified 36 possible uses of cards in such circumstances as entry to "12 Certificate" films and ownership of a pet.

The Bill establishes the minimum age for card registration at 16 years and three months. However, 2(7) of the Bill permits the Secretary of State by Order to lower the minimum age. This option may be pursued. The government's consultation paper states: "For an entitlement card scheme to be an effective proof of age card, it would need to be available to young people over the full range of age restrictions that apply to various goods and services".

Children's rights groups have expressed concern[21] that provisions in the Identity Cards Bill may allow a link with data held in the forthcoming national children's database permitted by the Children's Act. The Children's Act has been criticised[22] by the Parliament's Joint Committee on Human Rights[23] over its potential breach of the right to privacy.

Penalties for non-compliance with the legislation

It is probable that registration for a card will be required for anyone who wishes to work, use the banking or health system, travel internationally or receive benefits. As Mr Blunkett advised Parliament:[24]

> "The issuing of a card does not force anyone to use it, although in terms of drivers or passport users, or if services - whether public or private - required some proof of identity before expenditure was laid out, without proof of identity and therefore entitlement to do it I doubt whether non-use of it would last very long."

It is important to keep in mind that the card will be buttressed by a substantial array of new state powers and criminal penalties. The Bill creates a score of new offences including refusal to obey an order from the Secretary of State (6(4)), failure to notify authorities about a lost, stolen, damaged or defective card (13(1)), failure to renew a card (9(2)), failure to submit to fingerprinting (9(4)(b)), failure to provide information demanded by the government (9(4)(d)), failure to attend an interview at a specified place and time (9(4)(a)) and failure to notify the Secretary of State of any change in personal circumstances (including change of address) (12(1)). Failure to obey an order to register or providing false information will also constitute an offence. Penalties range from £1,000 fine to two years imprisonment. A penalty of up to £2,500 can be levied for

[20] Legislation on identity cards: a consultation, Home Office, http://www.homeoffice.gov.uk/comrace/identitycards/publications.html.
[21] Action on Childrens Rights, http://www.arch-ed.org/chldrnbill.htm.
[22] 'Children Bill repeats ID Card database problems', Out-law.com, September 28 2004, http://www.out-law.com/php/page.php?page_id=childrenbillrepeat1096381311&area=news
[23] Joint Committee On Human Rights - Nineteenth Report, http://www.publications.parliament.uk/pa/jt200304/jtselect/jtrights/161/16102.htm.
[24] House of Commons, Hansard, July 3, 2002, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo020703/debtext/20703-07.htm

failure to attend an appointment for a scan of fingerprints and iris. This fine can be repeated for every subsequent failure to attend.

Enforcement of the penalties

Many of the offences set out in the Bill are civil penalties. Defendants can object to the penalty by writing to the Home Office, but the Secretary of State has the right to increase the penalty if they choose to do so (34(3)). People charged in this way can also appeal to the courts (35(1)).

International environment and obligations

To date, the discussion on the relationship between the proposed Identity System and Britain's international obligations have been confusing. On the one hand, the Government is calling for the creation of a 'gold standard' for identity using techniques and technologies that are unprecedented. On the other hand the Government asserts that the legislation is merely a harmonising measure, meeting international obligations, and is thus no different to the plans and intentions of the UK's international partners.

In this section we will look at the nature of the international requirements for standardised identity documents. We will also address developments in other countries.

We conclude that the Government is unnecessarily binding the identity card scheme to the internationally agreed requirements on passport documents. By doing so, the Government has failed to correctly interpret international standards, generating unnecessary costs, using untested technologies and going well beyond the measures adopted in any other country that seeks to meet international obligations. The Government is making unnecessary choices on important international issues in order to meet domestic policies. There are more effective and less complex ways to meet international standards and obligations.

Background to the international context

It is indeed true that many countries are moving towards enhanced identity infrastructures, and much of this activity is attributed to rising concerns regarding terrorism. Countries that have repeatedly held national debates on ID cards and rejected the principle are now reconsidering earlier stances. But a direct response to terrorism is rarely a primary driver in these debates.

Many Governments are attempting to create a sense in the public mind that biometric identity documents are inevitable. They argue that the world is moving in this direction, that the technology is available and ready, and that states are compelled by international obligations to adopt the technology. Few of these initiatives have been proposed in response to terrorism, but are instead initiatives that have been long-standing and previously achieved little momentum. Political and financial momentum was subsequently generated after terrorism became a predominant concern.

This situation is best seen in the United Kingdom through the explanations for why an Identity Scheme is both desirable and financially viable. In public statements, the Government has focused on changes to the technical standards of travel documents, notably passports. These international travel documents are increasingly burdened with additional functionality so they can fuse with the role of identity cards. According to Home Office Minister Beverley Hughes,

> "I welcome the publication of the UK Passport Service's Corporate and Business plans today. The work carried out over the next five years by the UKPS, in partnership with other Government departments and agencies, will be crucial to the fight against identity

> fraud, as we build the base for the compulsory national Identity Card scheme.
>
> "Identity crime is a growing threat both here and abroad, and facilitates illegal immigration, benefit fraud, illegal working, and terrorist activity. It is only by thinking ahead and starting this work now that we will tackle this menace, and ensure that the UK is in a position to face up to the technological and law-enforcement challenges of the future."[25]

On the introduction of the draft Bill in April 2004, the Home Secretary announced that because passports were necessarily going to be biometrics-enhanced, ID cards were inevitable.

> "UK passports are going to be introducing biometrics whether people like it or not, because that's the way the world is going. ... Within three years we will be in a position to start everyone having a biometric passport issued and along with it a biometric card. People will not be able to have multiple identities."[26]

At the Labour conference in the fall of 2004, the Home Secretary presented how, once the Government could link the passport to an extended set of social protections, the costs of the passport would help pay for the ID card.

> "[W]e will legislate this winter to upgrade our secure passport system, to create a new, clean database on which we will understand and know who is in or country, who is entitled to work, to services, to the something for something society which we value. As people renew their passports, they will receive their new identity card. The cost of biometrics and the card will be added to the total of passports."[27]

When the Identity Cards bill was announced in the Queen's Speech, the Home Secretary linked the ID card to the new passport, and extended the cost argument, drawing links to U.S. and EU policies.

> "And why the necessity of doing it at all now? Well fairly obviously on a very personal level what is it good for in terms for us? If we are going to have to pay $100 a throw to get a biometric visa for clearance to travel to and from the US and there are 4 of us in the family, it's a lot easier to use a biometric ID card, linked to our new biometric passport then it is to have to pay over and over again in order to be cleared to be able to get to the US, and that will certainly become the case in other parts of the world as well. It's helpful for us, in terms of being able to establish common travel arrangements in Europe. Not necessary inside but certainly coterminous with the Schengen travel area, in order to be able to do that, alongside our colleagues in France,

[25] 'UK Passport Service 2004-2009 business plan highlights biometric IDs', March 31, 2004, PublicTechnology.net http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=820.
[26] 'Blunkett pushes for ID card law 'in 18 months'', Andrew Sparrow, Daily Telegraph, April 26, 2004.
[27] 'UK ID cards to be issued with first biometric passports', John Lettice, The Register, October 11, 2004.

> Germany and Spain who are now developing the issue of biometrics for travel inside and outside the European Union."[28]

This line of reasoning was summarised by the Prime Minister, responding to a question from the leader of the Liberal Democrats on the practical costs and challenges to the proposed scheme.

> "The point that I would make is that what has changed my mind on identity cards is that we now have the technology and, indeed, will effectively be obliged to use it for passports, which represents the bulk of the cost—£70 out of the £85 is for the passport, which we will have to introduce in any event. It makes sense in my judgment, when we have this biometric technology and when it really can make a difference on some of these issues—this is a common consensus certainly among the police and enforcement services—that we make it clear that ID cards will be introduced."[29]

Following the introduction of the Identity Cards legislation, the Home Secretary asserted, in an article for the Times, that

> "This drive towards secure identity is, of course, happening all over the world. Under current plans, for example, from next autumn British tourists who need a new passport will have to get a biometric one to visit the US or get a biometric visa. We will - rightly - have to bear the costs of introducing the new technology to enhance our passports anyway. We should take the opportunity of that investment to secure wider benefits such as those I set out here."[30]

This line of reasoning concludes that biometric ID cards are inevitable. The Government has linked the Identity Card to international standards and obligations on the passport, whilst extending the mandate of the passport into a much larger programme including the management of domestic policy.

With this as the background to the international context, the remainder of this section will explain the nature of these international obligations, other international initiatives on identity, and how other countries are dealing with these same pressures, initiatives, and technologies.

Passport Standards: ICAO, the EU, and the U.S.

Background

For a number of years the international community has co-operated on increasing the security standards on passports. The UN-level agency responsible for these standards is the International Civil Aviation Organization (ICAO). In the late 1990s the ICAO undertook research on the potential uses of biometrics and other forms of digitisation of

[28] Home Secretary 'Identity Cards Speech' to the Institute for Public Policy Research, November 17, 2004, http://www.homeoffice.gov.uk/docs3/identitycards_041118speech.htm.
[29] House of Commons, Hansard, December 15, 2004, Column 1664.
[30] 'ID cards defend the ultimate civil liberty', Charles Clarke, The Times, December 20, 2004.

passport information, but in the years that followed not much progress had been made in this quest.

The U.S. Government enlivened this process with the *USA-PATRIOT Act*. The *USA-PATRIOT Act*, passed by the U.S. Congress following the events of September 2001 included the requirement that the President certify within two years a biometric technology standard for use in identifying aliens seeking admission into the U.S. The schedule for its implementation was accelerated by another piece of legislation, the *Enhanced Border Security and Visa Entry Reform Act 2002*. Section 303 and 307 of this second law included seeking international co-operation with this standard.

> "By October 26, 2004, in order for a country to remain eligible for participation in the visa waiver program its government must certify that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and which incorporate biometric and authentication identifiers that satisfy the standards of the International Civil Aviation Organization (ICAO)."[31]

This Act created pressure on the Visa Waiver Countries[32] to institute new passports that include biometrics, and also generated momentum for the activities of the ICAO to come up with the standard.

ICAO Requirements

Moving the issue of biometric passports to the ICAO pushed the biometrics policy well beyond the Visa Waiver Program countries. The ICAO is the international standard-setter for passports, and since 1995, had been researching biometric passports. Since then, the performance of some biometric technologies had improved sufficiently to make facial recognition, fingerprints and iris scans contenders for implementation in passports standards.

The technical working group assessing these technologies includes representation from Australia, Canada, Czech Republic, France, Germany, India, Japan, New Zealand, Netherlands, Russian Federation, Sweden, United Kingdom and United States. The primary purposes of biometric use, according to the ICAO, is to allow for *verification* ("confirming identity by comparing identity details of the person claiming to be a specific living individual against details previously recorded about that individual") and *identification* ("determining likely identity by comparing identity details of the presenting person against details previously recorded on a number of living individuals"). Additional potential benefits include advanced passenger information to ports of entry and electronic tracking of passport use.

In their review of biometric technologies, the ICAO assessed compatibility according to seven criteria, including

[31] Enhanced Border Security and Visa Entry Reform Act of 2002 - ALDAC No. 1, Telegram from the Secretary of State to all Diplomatic and Consular Posts, on Executive Order 12958, March 14, 2003, http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html.

[32] Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Switzerland, Sweden, United Kingdom.

- compatibility with enrollment requirements
- compatibility with MRTD[33] renewal requirements
- compatibility with MRTD machine-assisted identity verification requirements
- redundancy
- global public perception
- storage requirements
- performance

The ICAO then assessed the available technologies and separated them into three groups, based on their overall ability to meet the comprehensive set of requirements, and found that

> Group 1: Face achieves the highest compatibility rating (greater than 85%);
> Group 2: Finger(s) and eye(s) emerge with a second-level compatibility rating (near 65%); and
> Group 3: Signature, hand and voice emerge with a third-level compatibility rating (less than 50%).

By 2003, facial recognition emerged as the primary candidate.[34] Intellectual Property issues prevented iris scans from being accepted; and it was felt that facial recognition is more socially acceptable. The ICAO felt that a single standard biometric technology used by all nations would ensure interoperability. This biometric implementation would only require the inclusion of a digital photograph embedded on a chip within the passport.

Surprisingly, shortly afterward, the ICAO mildly shifted its position. At a meeting in early 2003, its working group stated that

> "ICAO TAG-MRTD/NTWG[35] recognises that Member States currently and will continue to utilise the facial image as the primary identifier for MRTDs and as such endorses the use of standardised digitally-stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine readable travel documents.
>
> ICAO TAG-MRTD/NTWG further recognises that in addition to the use of a digitally stored facial image, Member States can use standardized digitally-stored fingerprint and/or iris images as additional globally interoperable biometrics in support of machine assisted verification and/or identification."[36]

[33] Machine readable travel documents.
[34] International Civil Aviation Organization, Biometrics Deployment of Machine Readable Travel Documents ICAO TAG MRTD/NTWG Technical Report: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation Using Machine Readable Travel Documents, Montreal, ICAO, 2003.
[35] Technical Advisory Group on Machine Readable Travel Documents and New Technology Working Group.
[36] ICAO, Report of the Technical Advisory Group on Machine Readable Travel Documents, Fourteenth Meeting, Montreal, 6-9 May 2003.

The ICAO was recognising that "some States may conclude it desirable to deploy two biometrics on the same document."[37] In attempting to accommodate flexibility for the varying demands of the member states of the ICAO working groups, the ICAO had subverted its primary goal of interoperability. The inclusion by a country of additional biometrics on its passport does not aid the travel of citizens from this country because only their home country will be able to make use of that biometric. For example, the inclusion of iris data in UK passports will not aid travel to the United States, because the U.S. does not record or verify iris scans. The inclusion of any additional biometrics is unnecessary for added international travel security, as the additional biometric can only be of use to the British Government for possible domestic uses.

The ICAO's new position has given rise to two conditions. First, despite its goal of interoperability, the current international standard is flexible in the use of biometrics provided that all passports include the mandatory digital photograph. Second, the ICAO standards are mute on the point of whether there needs to be a back-end database that stores all biometrics of citizens' passports, and whether countries may collect these biometrics from visitors. If Britain includes iris scans in its passports, which is not in any way required for travel to the U.S., there is nothing that would prevent the U.S., or any other country, from collecting and storing the totality of information on British tourists.

The ICAO does not require the development of databases of biometric information for the issuance of national passports and verification of foreign passports. In fact, the ICAO is aware that there are contentious legal issues involved with the infrastructure for these passports, including potential conflict between the goals of centralising citizens' biometrics and protecting privacy laws, and collision with 'cultural practices'. According to ICAO documents,

> "At States own borders, for passports issued to their own citizens, whether to extract the biometric from the traveller's passport, or from a database containing the biometric template assigned to that traveller when their passport was issued (note some States are legislatively inhibited from storing biometric templates and in this case have no choice other than to use the image or template stored in the travel document)."

The ICAO thus states that,

> "ideally, the biometric template or templates should be stored on the travel document along with the image, so that travellers' identities can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable."[38]

The ICAO goes on to confirm that while central databases can facilitate additional security confirmation checks, they are not necessary. In response, the European

[37] ICAO, Machine Readable Travel Documents: Introduction, http://www.icao.int/mrtd/biometrics/intro.cfm.
[38] ICAO, Biometrics Deployment of Machine Readable Travel Documents: Technical Report, ICAO TAG MRTD/NTWG, May 21, 2004.

Commission admitted that this issue required further attention and research to "examine the impact of the establishment of such a European Register on the fundamental rights of European citizens, and in particular their right to data protection."[39]

In response to the ICAO's statement, an open letter issued to the ICAO by civil society organisations from the around the world observed,

> "It may be interesting to see if national governments recall this option, or if they rather change their national laws to allow for centralized storage, as allowed in other ICAO documents. Creative compliance may be a tool of both the state and non-state actors."[40]

The call by Governments for national biometric databases, the creation of databases on foreign travellers, and the development of biometrics beyond a digital photograph, are not in accordance with international obligations.

EU Specifications

The UK Government is by no means alone in its attempts to create biometric databases. The European Union has also taken steps in this direction with proposals that will involve the collection of fingerprints of all UK residents when they travel within the EU.

Despite earlier statements by the European Commission on the need for research on the relationship between a biometric database and data protection rules, the Council of the European Union has established a policy requiring all 400 million EU biometric passports to include fingerprints, each to be stored in an EU register.

The Council of the European Union decided in autumn 2004 to standardise all EU passports through the drafting of regulation. The European Parliament began consideration of a standardised biometric passport shortly afterwards. In October 2004, in a closed meeting, the Justice and Home Affairs Council decided to include mandatory fingerprinting for all EU citizens in the draft regulation. The Council then pressed the European Parliament into hastening the policy through the Parliament in December 2004, without considering in any detail the decisions made by the Justice and Home Affairs Council. The Parliament was informed by the Council that refusal to accept the demands would result in the Council calling for an 'Urgency Procedure' that would ensure the passage of the regulation. Additionally, if the Parliament had refused, the Council threatened to delay the introduction of the co-decision procedure for immigration and asylum issues to April 1 instead of the scheduled date of January 1.[41]

The legality of this course of action is open to question. However, throughout the entire process, the Council had argued that it was compelled to include biometrics into the

[39] Commission of the European Communities, Proposal for a Council Regulation on Standards for Security Features and Biometrics in EE Citizens' Passports, Brussels, The European Commission, 2004, http://register.consilium.eu.int/pdf/en/04/st06/st06406-re01.en04.pdf.
[40] Privacy International and others, An Open Letter to the ICAO, March 30, 2004, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-43421.
[41] Privacy International and others, An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents, November 30, 2004, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-85336.

passports because of U.S. requirements. Again the central argument continues to apply: the inclusion of fingerprints in the EU passport system will not assist the U.S. authorities, nor is it a requirement from the U.S. authorities. Rather this policy serves a EU-domestic policy to generate a registry of fingerprints of all EU citizens and residents.

It is important to note that the United Kingdom is not bound by the EU specifications.

U.S. border regulations

At this juncture it is useful to review the U.S. requirements once again. The *USA-PATRIOT Act* only requires that the President, within two years, must certify a biometric technology standard for use in identifying aliens seeking admission into the U.S. The policy was modified by the *Enhanced Border Security and Visa Entry Reform Act 2002*, requiring that all visa-waiver program countries implement, by October 2004, biometric passport programmes that satisfy the ICAO standards.

If countries did not comply with the deadline they would be excluded from the Visa-waiver program, with a costly consequence. As the deadline approached, however, it was becoming clear that no countries in the program were ready to issue biometric passports. The Department of State and the Department of Homeland Security recognised that this could create a potential hazard as hundreds of thousands of visitors to the U.S. would have to apply for a visa, creating chaos at U.S. consulates and embassies. The Secretaries of State and Homeland Security appealed to the U.S. Congress for a two-year delay to the deadline, citing 'privacy issues' and the technological challenges encountered by these other countries. The Secretaries warned that potential visitors to the U.S. would 'vote with their feet' and go elsewhere.[42]

Congress responded unfavourably to this request, and only granted a one-year extension. Countries now have until October 2005 to implement new passport regimes that include a biometric. Further postponement will be difficult to achieve. It seems unlikely that many countries will be ready for this deadline, particularly if these Governments insist on including additional biometrics that involve more complicated registration processes and additional technologies and costs.

In order to comply with the ICAO standard, the U.S. is implementing a biometric passport of its own.[43] The U.S., however, in compliance with the ICAO standard is only requiring a digital photograph **on a chip in the passport** and does not appear to be moving towards a database solution.

Meanwhile, the U.S. is photographing and fingerprinting all visitors under the US-VISIT program. All personal details that are recorded are kept for 75 years and used by various departments in the Federal, State, and tribal governments. It is important to note, unlike in the EU and the UK, the U.S. has decided **against** fingerprinting and iris-scanning its own citizens.

[42] Letter to the Chairman of the Committee on the Judiciary, House of Representatives, from the Secretary of Homeland Security and the Secretary of State, March 17, 2004.
[43] U.S. Department of State, Abstract of Concept of Operations for the Integration of Contactless Chip in the U.S. Passport, April 2004.

Identity Systems in other countries

A number of countries are moving towards including biometrics in identity cards, passports, and government databases.

Malaysia,[44] Singapore and Thailand are establishing similar card systems. China[45] is moving rapidly in this direction with the development of a compulsory ID database and card system but abandoned the biometric element after it concluded that the technology was unworkable with large populations.[46] The U.S. military in Iraq is developing a similar card and biometric system to control[47] access to Fallujah, while the UNHCR[48] has deployed an iris biometric system to control refugee traffic across the Pakistan-Afghan border. The UAE[49] also uses an iris system for border control. No European country has such a comprehensive card system as that proposed for the UK.

The Home Affairs Committee observed:

> "Most members of the European Union have voluntary or compulsory identity cards. Apart from the United Kingdom the only members without any form of identity card scheme are Ireland, Denmark, Latvia and Lithuania. Most EU countries have a national register, or issue citizens at birth a personal number for use in a wide range of circumstances, such as paying tax, opening a bank account or claiming benefits. Many cards have a biometric, in the sense that they incorporate a fingerprint, and some are compulsory to carry and produce on request. No country yet has a biometric system of the sort proposed for the United Kingdom, but a number are introducing smart-cards and considering options for more sophisticated biometrics."[50]

However, with the exception of Malaysia, Singapore, Hong Kong and Cyprus, no Common law country in the world has ever accepted the idea of a peacetime ID card. The Australian[51] and New Zealand[52] public have rejected similar proposals outright. Following widespread criticism,[53] Canada abandoned its proposed biometric ID card

---

[44] Vericardsys Website information, http://www.vericardsys.com/MyKad.htm.
[45] 'China starts to launch second-generation ID cards', People's Daily, March 30, 2004, http://english.peopledaily.com.cn/200403/30/eng20040330_138863.shtml.
[46] 'Fingerprints Missing From Chinese National ID Card', Card Technology, September 11, 2003, http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030911CTDN261.xml.
[47] 'Marine Corps deploys Fallujah biometric ID scheme', John Lettice, The Register, December 9, 2004 http://www.theregister.co.uk/2004/12/09/fallujah_biometric_id/.
[48] 'UNHCR passes 200,000 mark in returnee iris testing', UNHCR press release, October 10, 2003, http://www.un.org.pk/unhcr/press/Oct_10_03.htm.
[49] 'Iridian Launches Expellees Tracking and Border Control System in UAE', Biometric Tech News, March 19, 2003, http://www.biometritech.com/enews/031903d.htm.
[50] Home Affairs Committee, Fourth Report, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm.
[51] Roger Clarke, Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme, 1987, http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html.
[52] Smart Cards as National Identification Cards, School of Computing & IT, University of Wolverhampton, 1998, http://www.scit.wlv.ac.uk/~c9479633/cp3349/smrtid.html.
[53] 'ID card plan to top $7 billion', Louise Elliott, Canadian Press, October 6, 2003, http://www.canoe.ca/CNEWS/Canada/2003/10/06/218966-cp.html.

system in early 2004, opting to focus its efforts on enhanced border security. National ID card proposals have consistently been rejected by the United States Congress.

The situation regarding biometric passports is becoming more complicated. Denmark has implemented biometric passports, but the biometric information is kept on the chip in the passport and not in a central register. The biometric is limited to a digital photograph. The Swiss have acted similarly. The Greek Data Protection Authority prevented the Government from implementing biometric checks at the borders, forcing the Government to abandon its plans for a biometric border system for the Olympics.[54]

On the other hand, a number of countries are mimicking the UK. Recently the French Government announced its intentions to include further biometrics on its ID card, due to "international obligations" from the ICAO to include fingerprints, and in reference to the new acceptance of ID cards in the UK since the 'law' of December 2004.[55] The Philippines and Thai Governments are modelling their proposed ID cards on the UK scheme, with centralised databases of multiple biometrics tracking a wide range of uses. Germany, on the other hand, is considering a similar approach, but was recently warned against it on technological grounds. The German Government had considered the inclusion of additional digital biometrics, but the Federal Parliament's Office of Technology Assessment advised against complex systems involving centralised databases, warning of "a gigantic laboratory test", and varying costs depending on the scheme selected. Depending on different scenarios and document features, the report says, the cost could range from EUR 22 million to EUR 700 million for implementation and from EUR 4.5 million to EUR 600 million for annual maintenance for passports and ID cards.[56]

United States and Drivers Licenses

In February 2005 the U.S. House of Representatives approved H.R. 418, the REAL ID Act. It has not been approved by the Senate at the time of writing this report, nor is its passage likely to be easy. The legislation has encountered significant opposition from politicians and groups at all points in the political spectrum.

One of the bill's relevant aims is to establish and rapidly implement regulations both for State drivers' license and for identification document security standards. The bill first requires states to deny drivers' licenses to undocumented immigrants. This step is seen as moving the driver's license into the realm of a national ID card.

The first step in laying the foundations requires that federal agencies refuse any drivers' license that does not meet minimum document requirements and issuance standards, including verification of immigration status. As a result, temporary residents in the U.S. will only get a driver's license that is valid until their authorised period of stay expires. For all other non-citizens, licenses will be valid for only one year.

According to the American Immigration Lawyers Association,

[54] 'Biometric checks illegal in Greece, says Data Protection Authority', eGovernment News, November 11, 2003, http://europa.eu.int/idabc/en/document/1775/337.
[55] Ministere de l'Interieure de la Securite Interieure et des Libertes Locales, Le Programme INES, January 31, 2005.
[56] 'Introduction of biometric ID cards and passports to cost up to EUR 700m in Germany', eGovernment News, November 18, 2004, http://europa.eu.int/idabc/en/document/3495/336.

> "Preventing immigrants from obtaining driver's licenses undermines national security by pushing people into the shadows and fueling the black market for fraudulent identification documents. Moreover, it undermines the law enforcement utility of Department of Motor Vehicle databases by limiting rather than expanding the data on individuals residing in a particular state. Perhaps more to the point, it is clear from the 9/11 and Terrorist Travel staff report that the proposed restrictions would not have prevented a single hijacker from obtaining a driver's license or boarding a plane. (...) The terrorists did not need U.S.-issued driver's licenses to board the planes on September 11; they had foreign passports that allowed them to board airplanes. Use of foreign passports to board airplanes would still be permitted under this provision."[57]

The Act also requires that States sign up to the interstate compact for sharing licensing information.

The database that is generated under this regime will also be shared with Mexico and Canada. The bill specifies information to be held in the database; including name, date of birth, gender, digital photograph, signature, and address.

The law also repeals current law and allows the Secretary of Homeland Security to "prescribe one or more design formats" for the licenses. The White House announced its support for the bill, as it will "strengthen the ability of the United States to protect against terrorist entry into and activities within the United States."[58]

The bill now goes to the Senate for review, where many predict a difficult path ahead. The policies in this bill were previously rejected by the Senate when they were included within the Intelligence Reform Act 2004, in response to the recommendations of the 9/11 Commission.

Even at its worst, however, this bill would only give the Federal Government the same powers that the Government here already has over the information held in the DVLA. The general response to the REAL ID bill in the U.S. is one of widespread concern, and there are already a number of pressing court cases on the matter. Americans generally are opposed to ID cards and have rejected all proposals to implement such a system.

The Common Travel Area & the Ireland dimension

In the event that the UK identity card proposals pass into law, there is a perception that the existence of the Common Travel Area of the UK & Ireland will necessitate the establishment of an Irish identity card, otherwise the Common Travel Area would present a fundamental security loophole in the ID card proposals. This view is not supported by evidence.

---

[57] American Immigration Lawyers Association, The REAL ID Act of 2005: Summary and Selected Analysis of Provisions, January 27, 2005, http://www.aila.org/contentViewer.aspx?bc=10,911,5516,8191.

[58] Executive Office of the President, Statement of Administration Policy: HR 418 – REAL ID Act of 2005, Office of Management and Budget, February 9, 2005.

Under the conditions of the Common Travel Area, citizens of each country may travel freely within the Area to seek employment or for any other reason without being subjected to immigration controls Border authorities may, however, require the presentation of passports or some other form of identification.

These rights (within the UK) are enshrined in the 1949 Ireland Act, which stipulates that Irish citizens living in Britain can enjoy full freedom of movement between the two countries, and should enjoy the same benefits as British citizens. The legislation ensures that they are not to be treated as foreign nationals. The government has not signalled any intention to repeal these provisions.

Speaking in the House of Commons, Ulster Unionist Party Leader, David Trimble, asserted:

> "If the proposal reaches its final stage of being a compulsory identity card system, it will be necessary to have persuaded the Irish Republic to introduce an almost identical system. A common or shared database will probably be needed for it to operate."[59]

In a holding answer to a related question put by David Lidington MP, Citizenship & Immigration Minister Des Browne stated:

> "The principle of the Common Travel Area will be unchanged by the introduction of identity cards. All third country nationals who have permission to stay in the UK for more than three months, irrespective of their point of entry, will be required to enrol on the register at the three-month point."[60]

This position was confirmed by Home Minister Beverly Hughes, who in answer to a question from Sarah Teather MP said "The Government's proposals for identity cards do not compromise the principle of the Common Travel Area".[61]

The principle of the Common Travel Area may well be unaffected by the identity card proposals, but a number of practical issues are likely to emerge if the Common Travel Area is to be maintained with Irish membership. The human rights and law reform group JUSTICE has observed:

> "The Government needs to address whether the Common Travel Area can continue as a viable concept under the ID card proposals. The problems are technological as well as legal and ideological; reliance on the use of new equipment, who is responsible for this and whether they wish to be responsible are all questions that need to be considered to make the transition a smooth one."

[59] House of Commons, Hansard, December 20, 2004 : Column 1992, http://www.publications.parliament.uk/pa/cm200405/cmhansrd/cm041220/debtext/41220-31.htm.
[60] Hansard, Written answers, January 10, 2005, Column 305W, http://www.parliament.the-stationery-office.co.uk/pa/cm200405/cmhansrd/cm050110/text/50110w83.htm.
[61] Hansard, Written answers, January 26, 2004, Column 214W, http://www.publications.parliament.uk/pa/cm200304/cmhansrd/vo040126/text/40126w51.htm.

JUSTICE raised a number of important questions about the practicality of travel under the current arrangements if a UK identity system was to commence. These are:

(a) To what extent would the Republic be able to continue to be part of a joint immigration area with the UK if that country relied on passport cards that contained electronic information that can only be read by specially installed machines?

(b) Would the UK government want to install these machines in Irish ports and airports, and would the Irish want them?

(c) Would the British people be content with the fact that details on their cards could be read outside the UK, above and beyond the biometrics currently envisaged by the International Civil Aviation Authority (ICAA) and endorsed by the EU?

The Irish Department of Justice has also expressed concern about the fate of the Common Travel Area, postulating that an identity card system may need to be established for Ireland.

Provided that the appropriate technology is in place throughout the Area, we see no reason why this step should be taken. Alternative documentation can still be used within the Area, as it is now, and those Irish nationals residing in the UK for more than three months will be able to apply for a UK identity card, as would the nationals of any other country.

Key objectives of the UK Scheme

National security, organised crime and terrorism

This objective has been subject to claim and counter-claim. On July 3rd 2002, in response[62] to a question by Chris Mullin MP, David Blunkett said "I accept that it is important that we do not pretend that an entitlement card would be an overwhelming factor in combating international terrorism". Later, in answer to a question from Sir Teddy Taylor MP, he said he would not rule out the possibility of "their substantial contribution to countering terrorism".

The Government's considered position is that an ID card will help in the fight against terrorism. However the essential facts are disputed. David Blunkett has told parliament that the security services have advised him that 35 per cent of terrorists use false identification, However Interpol general secretary Ron Noble told[63] the House of Lords Home Affairs Committee that all terrorist incidents involve a false passport. He was unable to present evidence to support this claim.

The published evidence tends to refute the more extreme claims. In 2004 Privacy International published the findings[64] of the only research ever conducted on the relationship between identity cards and terrorism. It found that there was no evidence to support the claim that identity cards can combat terrorist threats.

The report stated:

> "The presence of an identity card is not recognised by analysts as a meaningful or significant component in anti-terrorism strategies.
>
> The detailed analysis of information in the public domain in this study has produced no evidence to establish a connection between identity cards and successful anti-terrorism measures. Terrorists have traditionally moved across borders using tourist visas (such as those who were involved in the US terrorist attacks), or they are domicile and are equipped with legitimate identification cards (such as those who carried out the Madrid bombings).
>
> Of the 25 countries that have been most adversely affected by terrorism since 1986, eighty per cent have national identity cards, one third of which incorporate biometrics. This research was unable to uncover any instance where the presence of an identity card system in those countries was seen as a significant deterrent to terrorist activity.

[62] House of Commons, Hansard debates, July 3, 2002, Column 231, http://www.publications.parliament.uk/cgi-bin/ukparl_hl?DB=ukparl&URL=/pa/cm200102/cmhansrd/vo020703/debtext/20703-05.htm.
[63] 'All terror attacks use false passports, claims Interpol chief', John Lettice, The Register, December 2, 2004, http://www.theregister.co.uk/2004/12/02/noble_wows_lords/.
[64] Privacy International, Mistaken Identity: exploring the relationship between national identity cards and the prevention of terrorism, April 2004, http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf.

> At a theoretical level, a national identity card as outlined by the UK government could only assist anti-terrorism efforts if it was used by a terrorist who was eligible and willing to register for one, if the person was using their true identity, and if intelligence data could be connected to that identity. Only a small fraction of the ninety million crossings into the UK each year are supported by comprehensive security and identity checks."

Crucially, the Bill also contains a fundamental condition that nullifies most of its efforts to support counter-terrorism. David Blunkett has told the Home Affairs Committee that in order to prevent the creation of "ID card martyrs"[65] the government would not make it a criminal offence to refuse to be registered for a card. Instead, refuseniks would be liable for a civil penalty. In view of some entrenched hostility to the scheme, perhaps this approach makes tactical – and politically essential - common sense. However, some critics have pointed out that wealthy people[66] or those backed by criminal organisations can avoid an ID card or registration simply by paying the recurring £2,500 fine. This fine could effectively become a tax on criminals and terrorists operating in the UK.

Of equal significance is the admission by the Home Office that visitors to the UK who are entitled to a stay of three months or less will not be required to apply for a card.

The government appears to be incrementally backing away from its original assertion that the card system would be a tool to directly prevent terrorism. In a recent press briefing, Home Office minister Des Browne said[67] "It (the ID system) does not stop it but it helps you police it and interdict it".

Identity fraud

The government has heavily promoted the need to combat the problem of identity theft, consistently citing its estimate[68] of £1.3 billion per year lost because of the activity of identity fraudsters.

While identity theft is indeed a crime that can have a devastating impact on the victim, this estimate has been called into question. A 2004 conference[69] organised by the Law Society heard that the figure was derived from a "best guess". When the data is more closely analysed, the conclusions are less certain. Summarising the presentation by Roger Smith, Director of JUSTICE, the Law Society wrote:

> "It (the Cabinet Office report) asserts that £1.3 billion is lost due to identity fraud. However, when you analyse the data closely, it dissolves. Customs is worth £250 million loss on the basis of total

[65] Home Affairs Committee, May 4, 2004, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/4050405.htm.
[66] 'There's only one way ID cards won't be abused', Sam Leith, Daily Telegraph, December 3, 2004, http://www.telegraph.co.uk/opinion/main.jhtml?xml=/opinion/2004/12/03/do0303.xml.
[67] 'ID cards: this is not a big brother database', Andy McCue, Silicon.com, December 1, 2004, http://management.silicon.com/government/0,39024677,39126226,00.htm.
[68] Cabinet office, Identity Fraud: a study, July 2002, http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf.
[69] Law Society conference "Identity Cards: benefit or burden", London, March 22, 2004. http://www.lawsociety.org.uk/influencinglaw/policyinresponse/view=article.law?DOCUMENTID=166478.

> MTIC fraud between £1.7million - £2.6 billion with a midpoint of £2.15 billion, we can assume that identity fraud is 10% of this figure."

Additionally, credit card fraud is frequently confused with identity theft, and estimates of the two activities frequently intersect.

Still, at first sight it appears logical to argue that a national identity system will help combat identity theft. There is, however, a substantial body of evidence to show that the establishment of centralised identity can increase the incidence of identity theft.

The clearest example of this relationship exists in the United States, where the Social Security Number[70] has become an identity hub and a central reference point to index and link identity. Obtaining a person's SSN provides a single interface with that person's dealings with a vast number of private and public bodies. Hence the level of identity theft in the U.S. is extremely high.

This situation applies equally in Australia,[71] where the introduction of an extensive Tax File Number has also increased the incidence of identity theft beyond the levels experienced in the UK.

The key factor behind identity theft is the widespread availability of a central number, linked to a range of personal information. Consumer groups in the U.S. have recently criticised the Senate Banking Committee for failing to take action to reverse this trend. The Consumers Union argues[72] that identity theft will continue to rise until the relationship between the SSN and the publication of personal details in the finance sector can be reduced.

In the United States, Blue Cross and Blue Shield recently decided to discard the inclusion of Social Security numbers to help prevent identity theft. Between April 1 and the end of the year, all of the insurance company's members will be given new ID numbers and new ID cards containing those numbers.[73]

Prevention and detection of crime

Although Law and Order is a key motivation for the establishment of ID cards in numerous countries, their usefulness to police has been marginal.

Assertions that identity cards would be a useful too for policing have received little support or substantive backing by academic or law enforcement bodies. During debates in the mid-1990's over the proposed introduction of an identity card the Association of Chief Police Officers (ACPO) said that while it is in favour of a voluntary system, its members would be reluctant to administer a compulsory card that might erode relations with the public.

---

[70] 'Proposed California Bill Bans Distribution of Social Security Numbers', Information Week, December 6, 2004, http://informationweek.com/story/showArticle.jhtml?articleID=54800697.
[71] Speech by Karen Curtis, Federal Privacy Commissioner, to the 2nd International Policing Conference, Adelaide, 3rd November, 2004 http://www.privacy.gov.au/news/speeches/sp5_04p.html.
[72] Consumers Union statement, September 23, 2003, http://www.consumersunion.org/pub/core_financial_services/000407.html.
[73] 'Blue Cross to drop Social Security numbers from ID cards', The Business Journal, March 8, 2005.

According to police in most economically developed countries, the major problem in combating crime is not lack of identification procedures, but difficulties in the gathering of evidence and the pursuit of a prosecution. Indeed, few police or criminologists have been able to advance any evidence whatever that the existence of a card would actually reduce the incidence of crime, or the success of prosecution. In a 1993 report, ACPO suggested that street crime, burglaries and crimes by bogus officials could be diminished through the use of an ID card, though this was in conflict with its position that the card should be voluntary.

Support along these lines for the introduction of cards is also predicated on the assumption that they will establish a means of improving public order by making people aware that they are being in some way observed. Sometimes, cards are proposed as a means of reducing the opportunity of crime. In 1989, the UK government moved to introduce machine readable ID cards to combat problems of violence and hooliganism at football grounds. The general idea was that cards would authorise the bearer to enter certain grounds and certain locations, but not others. They could also be cancelled if the bearer was involved in any trouble at a ground or related area. The idea was scrapped after a report by the Lord Chief Justice claimed that such a scheme could increase the danger of disorder and loss of life in the event of a catastrophe at a ground.

One unintended repercussion of ID card systems is that they can entrench wide-scale criminal false identity. By providing a one stop form of identity, criminals can easily use cards in several identities. Even the highest integrity bank cards are available as blanks in such countries as Singapore for several pounds. Within two months of the new Commonwealth Bank high security hologram cards being issued in Australia, near perfect forgeries were already in circulation.

This conundrum has been debated in Australia, the UK and the Netherlands. It relies on the simple logic that the higher an ID cards value, the more it will be used. The more an ID card is used, the greater the value placed on it, and consequently, the higher is its value to criminal elements.

There appears to be a powerful retributive thread running along the law and order argument. Some people are frustrated by what they see as the failure of the justice system to deal with offenders, and the ID card is seen, at the very least, as having an irritant value.

It is impossible to provide a comparative assessment that would link the existence of a national identity card with the overall level of crime in each country. It is, however, possible to establish certain inferences by assessing crime trends across Europe.

Table 1: Crime Recorded by Police in EU Countries, 1995 - 1999[74]

Country	Recorded Crime	Drug - Trafficking	Homicides	Terrorist Incidents[75]	ID Cards
	% change	% change	Avg 97-99, /100,000	1968-2005	NC: not compulsory C: compulsory
Eire	- 21	+139	1.35	26	No Cards
England[76]	- 10	- 6	1.45	165 uk[77]	No Cards
Scotland	- 8	+ 9	2.10	uk	No Cards
Denmark	- 8	- 56	1.20	28	No Cards
Luxembourg	- 5	+ 23	0.83	5	ID NC
Germany	- 5	+ 33	1.22	458	ID C
France	- 3	+ 29	1.63	1027	ID NC
Finland	- 2	+ 29	2.55	1	ID NC
Spain	+ 1	- 12	2.60	1218	ID C
Austria	+ 1	+ 40	0.84	64	ID NC
Sweden	+ 2	- 32	1.94	40	ID NC
Netherlands	+ 2	+ 119	1.66	77	ID NC
Italy	+ 5	+ 18	1.56	405	ID NC
Portugal	+11	- 9	1.39	51	ID NC
Greece	+14	+ 128	1.69	593	ID C
Belgium	+18	+ 45	1.75	119	ID C

These figures do not establish a relationship between cards and levels of crime, but they do indicate that there is no safe way to assess whether a card system will influence crime trends. It is certainly the case, according to these figures, that crime trends in countries without a national ID card tend to be in the downward direction.

Benefit fraud

The proposals will in all likelihood have a substantial impact on the use of false identities by benefits claimants. This element of benefit fraud, however, represents only a small percentage of the overall fraud problem. David Blunkett advised Parliament[78] "benefit fraud is only a tiny part of the problem in the benefit system". The majority of fraud on the benefits system is through under-reporting of income, or non-reporting of financial and family circumstances. Benefits agencies worldwide agree that false

[74] International comparisons of criminal justice; 1999 spreadsheet RDS website issue 6/01 Gordon Barclay et al., May 2001, source: www.homeoffice.gov.uk/rds/.
[75] Incidents from MIPT Terrorism Knowledge Base, source: www.tkb.org/Home.jsp.
[76] England and Wales.
[77] N. Ireland had 618 incidents.
[78] House of Commons, Hansard debates, July 3, 2002, Column 230, http://www.publications.parliament.uk/cgi-bin/ukparl_hl?DB=ukparl&URL=/pa/cm200102/cmhansrd/vo020703/debtext/20703-05.htm.

identity is not a key issue. The Australian Department for Social Security estimated[79] that benefit overpayment by way of false identity accounts for 0.6 per cent of overpayments, whereas non-reporting of income variation accounts for 61 per cent.

In evidence[80] to the Home Affairs Committee, the Parliamentary Under-Secretary at the Department of Work and Pensions, Chris Pond MP, confirmed that false identity represented a tiny fraction of the benefit fraud problem. He said his Department advised that of the estimated £2 billion total annual benefit fraud, £50 million came from people not being who they said they were when making a claim. There is a possible deterrent effect established by an ID system, though this has not been quantified.

It is possible that the cost to government of establishing a new ID infrastructure for benefits would amount to more than the annual loss through false identity.

[79] Privacy International, Identity Cards: frequently asked questions, 1996, http://www.privacy.org/pi/activities/idcard/idcard_faq.html.

[80] House of Commons, Minutes of evidence, Home Affairs Committee, April 27, 2004. http://www.parliament.the-stationery-office.co.uk/pa/cm200304/cmselect/cmhaff/uc130-vi/uc13002.htm.

The legal environment

The Identity Cards Bill raises a number of issues and potential conflicts relating to a variety of existing laws. The most important of these are:

- A number of elements of the Bill potentially compromise Article 8 (privacy) and Article 14 (discrimination) of the European Convention on Human Rights.

- The Bill also creates a possible conflict with the right of freedom of movement throughout the EU for EU citizens. It is arguable that the Identity Cards Bill may discourage non-UK EU workers from coming to the UK to work and so may infringe EU principles on the freedom of movement of workers. Furthermore, EU Directive 68/360 governing the rights and conditions of entry and residence for workers may make it unlawful for the government to require non-UK EU citizens to obtain a UK identity card as a condition of residence.

- Because of the difficulty that some individuals may face in registering or verifying their biometrics there is a potential conflict with UK laws such as the Disability Discrimination Act and the Race Relations Act.

- The proposals appear to be in direct conflict with the Data Protection Act. Many of these conflicts arise from the creation of a national identity register, which will contain a substantial amount of personal data, some of which would be highly sensitive. The amount of information contained in the register, the purposes for which it can be used, the breadth of organisations that will have access to the Register and the oversight arrangements proposed are contentious aspects.

- Liability and responsibility for maintaining accuracy of data on the Register, conducting identity checks and ensuring the integrity of the overall operation of the scheme has not been resolved. The legislation places requirements on individuals and organisations that are substantial and wide-ranging, and yet no indication has been given relating to how liability would be established, who would assess that liability, or who would police it.

The European Convention on Human Rights

The fifth report[81] of the Parliament's Joint Committee on Human Rights set out "serious concerns" relating to more than a dozen key areas of the ID legislation. These include:

- The extent of the personal information which will be included within the "registrable facts" held on the Register, and whether all of the information held serves a legitimate aim, and is proportionate to that aim, as required by Article 8 (paragraphs 10 –15);

[81] Joint Committee on Human Rights, Identity Cards Bill, Fifth Report of session 2004-2005, House of Commons & House of Lords, http://www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/35/3502.htm.

- The potential for personal information to be recorded on the Register without the knowledge or consent of the individual concerned, under clause 2(4),which allows the inclusion on the Register of information "otherwise available " to the Home Office (paragraph 17);

- The potential for the system of "designated documents " to render registration and ID cards effectively compulsory for certain groups of people who hold these documents, and the resultant potential for arbitrary or disproportionate interference with Article 8,and for discrimination in breach of Article 14 (paragraphs 18 –21);

- The potential for a "phased in " system of compulsory registration and ID cards to lead to interference with Article 8 rights which is not justified by any legitimate aim, and may discriminate against those groups subject to compulsion, contrary to Article 14 (paragraphs 22 –25);

- Under a compulsory scheme, the extent of personal information which may be disclosed from the Register to a service provider as a condition of access to public services under clause 17,potentially in breach of Article 8,and the lack of safeguards against unnecessary disclosure to service providers under clause 17
- (paragraphs 26 –29);

- The potential, under a compulsory scheme, for both public and private persons to make contracts or services conditional on production of an ID card, or access to information on the Register, without sufficient safeguards under clause 18,and the risk of breach of Article 8 (paragraphs 30 –33);

- Provision for extensive data sharing from both the public and private sectors in order to confirm information on the Register, or information which the Home Office wishes to enter on the Register, under clause 11 (paragraphs 34 –36);

- Provision for extensive disclosure of personal information on the Register to public bodies for a wide range of purposes under clauses 19 –21, and for unlimited extension of these powers of disclosure by way of regulations under clause 22, without sufficient safeguards, risking breach of the Article 8.2 requirements that an interference with private life be in accordance with law, that it pursues a legitimate aim, and is proportionate to that aim (paragraphs 37 – 43).

This report does not assess or amplify these concerns, but does endorse the need for further investigation of the issues raised by the Joint Committee.

EU Free Movement Principles and Directive 2004/38/EC

The Government's Identity Card Bill would appear to require the mandatory registration on the National Identity Register of all EU citizens resident in the UK for more than

three months.[82] This requirement arguably conflicts with EU freedom of movement principles and, in particular, with the recently enacted EU Directive on the Free Movement of Persons, Directive 2004/38/EC (the Directive). The Directive's provisions suggest that EU citizens should not and cannot be compelled to register with the National Identity Register and obtain an identity card, at least not on the conditions set forth in the proposed Bill.

The free movement of persons within the EU remains one of the four pillars of the EU's Internal Market. Under the free movement principle, EU citizens retain a fundamental right to freedom of movement and residence within the EU, as conferred directly by Article 39 of the EC Treaty, subordinate legislation and related case law. The precise rights of entry and residence now are governed by a complex body of EU legislation. Under legislation that preceded the new Directive, EU citizens could enter another Member State "on production of a valid identity card or passport" and stay in that Member State for up to three months without the need to comply with any formalities, such as obtaining a residence card. Workers, self-employed persons and their families were entitled to a five-year residence permit that could be renewed automatically.

Then, in 2001, the European Commission issued proposals that ultimately resulted in the enactment of Directive 2004/38/EC. The Directive's principal aim is "to simplify and strengthen the right of free movement and residence of all Union citizens" by codifying existing directives into a single legislative act. The Directive creates a new right of permanent residence and sets forth the limits that can be placed on these rights by Member States on public policy, public security or public health grounds.

The UK Government has until 30 April 2006 to implement the Directive and, prior to implementing the Directive, is precluded from enacting conflicting legislation. As noted by the European Court of Justice in Case C-129/96 *Inter-Environment Wallonie ASBL v Région Wallonie*, "it is during the transposition period that the Member States must take the measures necessary to ensure that the result prescribed by [a] directive is achieved at the end of that period" and to refrain "from adopting measures liable seriously to compromise the results prescribed".

The Proposed Identity Cards Scheme is Arguably Incompatible with Directive 2004/28/EC. The Directive requires Member States to allow EU citizens "to enter their territory with a valid identity card or passport" (Article 5) and to reside there for up to three months "without any conditions or any formalities other than the requirement to hold a valid identity card or passport" (Article 6). EU citizens, therefore, have the express right to stay in the UK for up to three months without any conditions or formalities. Requiring them to acquire a UK identity card during that period of time would qualify as a condition or formality. The Government appears to have accepted this and has stated that for "legal reasons, it is not feasible to require EU nationals to register until they have been in the UK for three months and intend to stay longer."[83]

---

[82] "Registration certificates and residence permits for foreign nationals would be issued, taking account of EU standards, but to the same level of security as the UK identity cards and as part of a single overall system of recording and verifying the identity of all legal residents". Cm 6359, Identity Cards: The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130, p 4.

[83] Cm 6359, Identity Cards: The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130, p 10.

Article 7, in turn, confers on all EU citizens the right to reside in another EU Member State for more than three months, if the citizen falls into one of the following categories of persons: workers and self-employed persons, students and those with sufficient resources to support themselves without becoming a burden on the relevant Member State's social welfare system.[84] Article 8 describes the administrative formalities that a Member State may apply to such EU citizens -- namely, the host Member State may require the EU citizen to "register with the relevant authorities" (Article 8(1)). Article 8(2) goes on to clarify that a "registration certificate shall be issued immediately [by the Member State], stating the name and address of the person registering and the date of registration." The "registration certificate" is, however, all that the Directive requires.

A more comprehensive assessment is set out in Appendix 3 of this report.

Potential conflict with other UK laws

The Disability Discrimination Act

In the section on biometrics, this report identified potential problems for blind and visually impaired users of iris recognition systems. While this disadvantage will most likely extend to a broader range of disabilities, we will concentrate here on issues relating to potential discrimination affecting visually handicapped people.

This research raises concerns about consequences of the Bill, particularly:

- The recording on the national Identity Register of biometric data, as set out in 1 (5)(d) of the Bill;

- The collection from an individual of biometric data, as set out in 5 (5)(b);

- The conditions set out in Section 6 and in 12 (4)(b) requiring an individual to submit to biometric identification;

- The powers set out in s.6 requiring the surrender of biometrics to gain access to benefits and services;

- The penalties specified in 6 (4) and 12 (1) for failure to obey a directive of the Secretary of State and to notify the government of change of personal circumstances. The latter on the face of the legislation may encompass changes to biometric conditions;

- The Offences specified in Section 30 relating to provision of false information.

The Bill does not contain detailed information regarding the collection or maintenance of biometric data. We understand that details of the proposed system for collection of biometric data will be established in Regulations.

[84] Family members (whether or not EU citizens) have a corresponding right of residence if they are accompanying or joining the EU citizen.

Against the backdrop provided by the evidence above, the report raises a number of concerns about specific provisions in the Bill.

Eligibility to enroll in the National Identity Register. Section 5 of the Bill requires the production by the applicant of "prescribed information", as determined by the Secretary of State. The Secretary of State will have the power to require unspecified and unlimited additional data. This may impose significant additional requirements on blind and visually impaired people who are unable to successfully register their iris. It may be necessary to explore whether the extent of such personal data and identifying information should be specified and limits placed on what may be required.

Compulsion. S.6(1) gives the Secretary of State the power to compel people to register and to attend appointments at a designated place and time. S.6(4) and s.6(6) provide for severe penalties for failing to attend or for defying such an order (up to £2,500 for each breach). There is a concern that blind or visually impaired people may be ordered to attend meetings more often than fully sighted people in order to verify their identity. Many of these people need to make special arrangements for travel. Others may have difficulty negotiating unfamiliar geographic areas to attend a designated location. Safeguards and limitations should be in place to protect blind and visually impaired people from ongoing impositions and requirements placed on them by a Document Authority.

Collection of biometric data. The collection from an individual of biometric data is set out in 5(5)(b). The Bill provides no detailed information on the manner of this collection, nor does it set out the minimum standards for the technology used. It is possible that blind and visually impaired people are more likely to encounter difficulty in using the biometric technology, and thus a requirement should be in place on the face of the Bill to ensure the protection of their privacy and dignity.

Inability to register an iris. The Bill sets out requirements for the surrender of biometrics on the order of the Secretary of State, and establishes penalties for defying such an order. This provision raises a number of questions of practicality. How does a blind or visually impaired person establish to the satisfaction of a Document Authority that he or she is physically incapable of being registered, rather than being obstructive? What evidence or documentation should be required to establish the relevant circumstances? What arrangements are to be put in place to deal with such situations? It can be argued that these conditions should be set out in the Bill rather than being left to the Regulations.

Notification of change of personal circumstances. Penalties are specified in 6 (4) and 12 (1) for failure to obey a directive of the Secretary of State and to notify the government of change of personal circumstances. The latter - on the face of the Bill - may encompass changes to personal biometric conditions. It would appear, for example, that the 200,000 or more people per year who undergo cataract procedures would be required to notify the government and (possibly) then be required to re-enrol. Many blind or visually impaired people who undergo medical treatment would be unsure of a change to their iris biometric. Others with deteriorating eye conditions may feel they

should notify the government routinely to avoid a £1,000 penalty. This would, perhaps in law, be viewed as an unfair and unacceptable burden.

Provision of services. S.15 of the Bill sets out a requirement for the production of identity cards and other "registrable facts" (including biometric data) for the provision of benefits and services. The Bill makes no provision, nor sets out any safeguard or limitation, for people who are unable to provide a usable biometric. It is important to recognise, on the basis of the data set out earlier in this report, that significant numbers of blind and visually impaired people may not be able to be verified against their enrolled iris.

Provision of false information. The Offences created in Section 30 relating to provision of false information give rise to concern. The Bill states that imprisonment may result from providing such information when a person (a) knows or believes the information to be false; or (b) is reckless as to whether or not it is false. A person with a changing or deteriorating eye condition, or a person who is preparing for medical treatment, might be accused of fulfilling these conditions. This risk becomes particularly substantial at the point of re-enrolment or verification, when an iris may not match the biometric recorded on the National Identity Register. The Bill, in the view of blind and visually impaired people we have consulted, should be explicit on these points and provide appropriate safeguards.

Potential for indirect racial discrimination

The potential for indirect racial discrimination under the identity cards regime has also been flagged as a potential issue of concern. The Government has acknowledged that the "draft legislation and the administration of the scheme is bound by the Race Relations Act 1976, as amended by the Race Relations (Amendment) Act 2000".[85] Section 1A of the Race Relations Act 1976 describes indirect discrimination as a measure which is of equal application regardless of race or ethnic or national origins but puts or would put persons of the same race or ethnic or national origins "at a particular disadvantage when compared with other persons." Indirect discrimination is permissible but only if it is "a proportionate means of achieving a legitimate aim".

The Government argues that the "identity cards scheme itself is non-discriminatory as it is intended to cover everyone in the United Kingdom for longer than a specified period".[86] However, this statement fails to address adequately the period before identity cards become compulsory for all citizens. The Government will need to ensure that any phased rollout of the identity card scheme, such as requiring an asylum seeker to obtain an identity card before an existing UK citizen, complies with the principle of proportionality.

The Data Protection Act

The Data Protection Act (DPA) provides a range of safeguards over the use of personal data and would be relevant to the creation of a national identity system. The Information

[85] Identity Cards Bill: Race Equality Impact Assessment, para.13.
[86] Ibid.

Commissioner has expressed concerns that the scheme, as set out in the Bill, could jeopardise some elements of data protection.

The Act contains eight Data Protection Principles (DPP's) that establish rights and safeguards relating to the collection, processing, access, disclosure, storage and security of personal information. These are all central to the design and operation of an identity card system.

The Identity Cards Bill raises many questions about compatibility with existing Data Protection legislation. The remaining lack of clarity of purpose and the wide-ranging scope for the Secretary of State to amend the various elements of the legislation by Order, mean that the elements of transparency and certainty sought by the First Data Protection Principle may not be provided. The lack of clarity has a knock on effect for satisfying the rest of the principles – if the purpose is not clear it is difficult to assess whether information is relevant or excessive. The Bill also proposes turning the principle that it is the data controller's duty to ensure the accuracy of their data on its head by laying this onus on the individuals themselves. Furthermore, though not clearly stated, it is implicit that the information fed into the National Identity Register will be kept indefinitely.

The Bill in many ways seeks to obviate the requirements of the DPA, taking the whole ID card outside the data protection regime: 'The Government's commitment to make the scheme consistent with the data protection legislation can be summarized as outline proposals to exempt the scheme from five of the eight data protection principles through the use of statutory powers'[87]

There are three main elements to the First Data Protection Principle: processing must be legitimate, fair and lawful. The very enactment of the enabling legislation will ensure that any processing will be legitimate. There may be questions however, surrounding the other two elements of fairness to individuals and lawfulness. Although the Bill does list more clearly the purposes for which the ID card and Register will be used than in earlier proposals, the provisions within the Bill for wide ranging powers of the Secretary of State to make amendments to the legislation by Order without sufficient consideration by Parliament or public debate mean that the existing purposes and consequent disclosures may become less clear over time. Any Fair Processing Notices provided by either the Home Office or participating public bodies will become inadequate.

Although the Register forms a substantial part of the Bill its existence is not acknowledged in the title of the Bill. The problems in the development and maintenance of such a database are well known with difficulties including the identification of the appropriate technology and the ongoing operation of such large-scale systems. The Data Protection Act requires any personal information held in a database to be accurate, up to date, relevant, adequate and not excessive for the stated purposes; standards which provide sufficient challenges to data controllers. However, should compulsion for the whole nation become fact, the scope of the Register, the amount of information to be

[87] Memorandum submitted by the Editors of 'Data Protection and Privacy Practice' to the Select Committee on Home Affairs

held and the necessary complexity of the infrastructure will present additional problems in terms of compliance with the Data Protection Act.

The Bill states that the Register is to be a convenient method for individuals to prove registrable facts about themselves to others and to allow those facts to be ascertained by others where it is in the public interest. Only one of those 'registrable' facts is a person's identity. Identity per se is listed in cl. 1(6) of the Bill as being a person's full name, other names by which they have been known, place and date of birth and identifying physical characteristics. The Bill lists another 15 classes of information that may be included on the Register. It is difficult to see how the requirement for all this information can satisfy the 3rd Data Protection Principle by being relevant, adequate and not excessive for the proposed purposes. A person will be required to provide their present main address, alternative addresses and previous addresses; a great deal of historical information will be collected that will not contribute to a person's 'identity'.

The information held on the Register will be disclosable without the consent of the individual to the Security Services, Chief Police Officers, Inland Revenue and Customs& Excise, any prescribed government department and any other person specified by Order by the Secretary of State. Again the potentially wide audience to whom this large and powerful amount of information might be disclosed will go the fairness and transparency features of the 1st Data Protection Principle and the specificity requirement of the 2nd principle.

The issue of ID cards to those applying for the issue or renewal of certain documents such as driving licences and passports will not only contribute to the lack of clarity as to purposes but will also undermine the idea that the compulsion to hold an ID card will be the subject of scrutiny in Parliament before it is extended to the wider populace. When an individual is asked to present an ID card based on one of these documents it is very likely that not all information will be relevant on every occasion. The risk is that excessive information will be disclosed and possibly retained even where it is not necessary for the particular circumstances in which the card was presented and the 3rd Principle will again be breached.

If the argument for a National Register is accepted, then the actual practical aspects of administration, maintenance and compliance with the information quality data protection principles (3rd, 4th, 5th) present very serious concerns.

A more comprehensive assessment is set out in Appendix 4 of this report.

Liability issues

The Identity Cards Bill sets forth a number of civil and criminal offences relating to the use of identity cards and the information contained on the National Identity Register. Notably, it will be an offence under Section 12 to fail to notify within the prescribed period any change of circumstances, such as a change of address. Under Section 11, the Secretary of State is empowered to require a third party to provide information about an individual for the purposes of verifying the information on the Register. Section 11(5), in particular, offers a non-exhaustive list of the persons who may be covered by this requirement, including government departments and Ministers of the Crown. However,

it is clearly intended that the order to provide information could be imposed on anyone, such as "local government or the private sector".[88]

Nothing in Section 11 appears to limit the scope of such an order of the Secretary of State; in particular, it is not clear whether such an order could override duties of confidentiality, legal professional privilege, doctor-patient privilege and related duties. The net effect of the above is to create a Register which contains information relating to persons, that may have been gathered in contravention of duties owed to that person in circumstances where the person was unaware that the information was being gathered, and that the person affected has no means of knowing what information is being gathered or whether it is accurate and correct.

In addition, the Bill does not address whether the individual must consent to the provision of the information or whether the individual should be informed that an order issued by the Secretary of State has been made or complied with. Schedule 1 specifies that information that may be recorded in the Register includes "particulars of every occasion on which information contained in the individual's entry has been provided to a person". This implies that information can be entered on the Register without the individual's knowledge or consent. Yet, without such prophylactic measures, the likelihood of inaccurate or false information becoming entered onto the Register remains high.

Significantly, it remains unclear to what extent, if any, private parties supplying information to the Register may be exposed to liability for providing information about individuals that is in fact inaccurate or incorrect. Given that public bodies will be relying on the Register to make determinations that will have a significant impact on the lives of the persons concerned, such as decisions related to benefits and public services entitlements where the potential harm caused by inaccuracies appearing on the Register remains high, the issue of potential liability for private parties remains an important one.

On a related note, Section 11(6)[89] makes clear that any third party, including potentially non-public entities, submitting information to the Register may owe a duty to the person ordering the provision of the information, namely the Secretary of State. It is unclear to what extent such a third party may be liable for incorrect information that it provides to the Register and where that inaccuracy leads to an adverse consequence, such as preventing or hindering the identification of a security risk. This issue also requires additional clarification.

---

[88] Explanatory Notes to the Identity Cards Bill, para. 77.

[89] Section 11(6) of the draft UK legislation states:

The power of the Secretary of State to make an order specifying a person as a person on whom a requirement may be imposed under this section includes power to provide:

(a) that his duty to provide the information that he is required to provide is owed to the person imposing it; and

(b) that the duty is enforceable in civil proceedings:

(i) for an injunction;

(ii) for specific performance of a statutory duty under section 45 of the Court of Session Act 1988 (c.36); or

(iii)for any other appropriate remedy or relief.

Biometrics

Prosecutions for dealing with or creating false ID cards and high-level identity documents have been pursued in many countries, including Britain,[90] Hong Kong,[91] Pakistan,[92] Ireland,[93] Malaysia,[94] Yemen,[95] Czech Republic,[96] Venezuela,[97] India,[98] Italy,[99] and Sri Lanka[100] where the forgeries were supplied to suicide bombers. This year the Israeli government estimated that "hundreds of thousands" of fake ID cards are in the hands of its population.[101]

In many cases the false identity was secured merely by bribing an official or by providing counterfeit documentation at the point of registration. The government proposes to eliminate this risk by establishing a "clean" database of identities. Entry onto the database will require multiple biometric captures, biographical footprint checking and a range of primary documentation. The Home Office has explained that the database will contain no multiple identities because a "one to many" check will be used before a person is enrolled.

A biometric is a measure of identity based on a body part or a behaviour of an individual. The most well known biometrics are fingerprints, iris scans, DNA and signatures. The position taken by the UK government is that some biometrics are extremely secure and reliable forms of ID, and it has promoted the use of fingerprints and iris scans to establish one's identity or, at least, one's uniqueness. The theory behind this approach is that a biometric is less likely to be spoofed or forged than might a simple photo identity card.

In the UK identity proposals, biometrics would be taken upon application for a card and for entry on the National Identification Register, and would be used thereafter for major "events" such as obtaining a driving license, passport, bank account, benefits or employment. The eye and fingers of the applicant would be scanned, and then compared both with the biometric on the identity card (which contains the biometrics in electronic form), and against a national database (which also contains the biometrics).

---

[90] 'Passport scam uncovered', BBC News Online, December 3, 1999, http://news.bbc.co.uk/1/hi/uk/548559.stm.
[91] 'Six months' jail for forged ID cards', The Standard, November 11, 2004, http://www.thestandard.com.hk/news_detail_frame.cfm?articleid=52102&intcatid=42
[92] 'No passports for old NIC holders: Faisal', The News international, Pakistan, http://www.jang.com.pk/thenews/oct2003-daily/29-10-2003/main/main13.htm.
[93] Parliament of Ireland, April 1, 2003, http://www.irlgov.ie/debates-03/1Apr/Sect10.htm.
[94] http://www.mmail.com.my/Current_News/MM/Friday/National/20041210100244/Article/index_html
[95] 'Yemen confirms Cole suspects' trial', BBC News Online, December 6, 2000, http://news.bbc.co.uk/2/hi/middle_east/1058085.stm.
[96] Ministry for the Interior of the Czech Republic, Report on the Security Situation in the Czech Republic in 2000, http://www.mvcr.cz/dokumenty/bezp_si00/angl/crime2.html.
[97] 'Some thoughts on identification', Asuntos Legales, http://www.analitica.com/archivo/vam1996.06/asleg1us.htm.
[98] 'Hill Kaka - A military or a political failure', Kashmir Sentinel, http://www.kashmirsentinel.com/june2003/18.html
[99] 'Italian police uncover massive Red Brigades weapons cache', China Daily, December 21, 2001, http://www.chinadaily.com.cn/en/doc/2003-12/21/content_292183.htm.
[100] 'Anticipatory bail application of former Dept. of Registration of persons Commissioner refused', Sarath Malalasekera, Daily News, August 10, 2004, http://www.dailynews.lk/2004/08/10/new24.html.
[101] 'Sheetrit promises new smart ID card tender before 2005', Globes online, September 7, 2004, http://www.globes.co.il/DocsEn/did=834696.htm.

However, any claim of infallibility is incorrect. All biometrics have successfully been spoofed or attacked by researchers. Substantial work has been undertaken to establish the technique of forging or counterfeiting fingerprints[102] while researchers in Germany have established[103] that iris recognition is vulnerable to simple forgery.[104]

A 2002 report of the United States General Accounting Office "Using biometrics for border security" states:

> Biometric technologies are maturing but are still not widespread or pervasive because of performance issues, including accuracy, the lack of applications-dependent evaluations, their potential susceptibility to deception, the lack of standards, and questions of users' acceptance.[105]

It also warns against making assumptions about the ability of the technology to perform across large populations:

> "The performance of facial, fingerprint, and iris recognition is unknown for systems as large as a biometric visa system…"

There are two distinct problems that can result from failure to adequately register with a biometric device. The first is described as the *Failure to Enrol Rate* (FTER). This occurs when a person's biometric is either unrecognisable, or when it is not of a sufficiently high standard for the machine to make a judgment. The second crucial indicator is the *False Non-Match Rate* (FNMR) that occurs when a subsequent reading does not properly match the properly enrolled biometric relating to that individual.

The first problem would result in a person not being enrolled in an identity system. The second can result in denial of access to services. While iris recognition appears to perform better than other biometrics in both these figures, there are still substantial problems, and these are likely to disproportionately affect, for example, visually disabled people.

Usability, accessibility, and acceptance of biometrics

Usability, accessibility and acceptance of the technology by the citizen are key concerns with the implementation of biometrics.

Usability: currently available equipment is difficult to operate, particularly by people who are not used to interacting with high-tech equipment, and by those who are not using the technology frequently. Some of the problems could be overcome through a program of usability testing and re-design to provide better user instructions and feedback. Some problems, however, cannot be addressed through re-design and are likely to persist. Correct positioning of the body, and presenting the eye in focus to an

[102] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino, Impact of Artificial "Gummy" Fingers on Fingerprint Systems, May 15, 2002, http://www.cryptome.org/gummy.htm
[103] 'Body Check', Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, CT Magazine, November 2002, http://www.heise.de/ct/english/02/11/114/.
[104] Liveness Detection in Biometric Systems, http://www.biometricsinfo.org/whitepaper1.htm.
[105] U.S. General Accounting Office, Using Biometrics for Border Security, Washington D.C., November 2002 http://www.gao.gov/new.items/d03174.pdf.

iris scanner, is difficult for many users. This will present problems to people with certain eye conditions, and to many people who are not using the systems regularly. With regular use, usage time can be around 12 seconds per user per identification, but for infrequent users, usage times increase substantially, and each failure to verify will slow the process down further, and/or demand additional resources for checking identity by other means.

Accessibility: A small percentage of people (which would nevertheless amount to tens of thousands for an ID card) are unable to enrol fingerprints or iris images. The quality of both characteristics is known to decline with age (fingerprints wear down, some eye conditions increasing with age cloud the iris), and operation of equipment becomes difficult with some conditions related to ageing (e.g. arthritis and tremor can impair ability to place fingerprints, positioning and focussing of the eye with deteriorating eyesight, and drooping of eyelids can cover so much of the iris that an image cannot be computed). There has been no scientific study to determine the stability of biometric characteristics over time. Apart from ageing, fingerprints may become unrecognisable because of cuts or burns, extreme weight gain or loss. Pregnancy and medication can affect the recognition of irises.

The vast majority of biometric trials have been in the "frequent traveller" context, using volunteers who are predominantly white male professionals in the age group between 20-55 years old. The recent UK Passport Service trial funded by the Home Office had a representative sub-sample of the whole population, but the results from this trial have not been published to date.

Face recognition has a lower failure-to-enrol rate (if removal of veils for enrolment and verification is compulsory), but has in past trials shown false rejection rates of around 10% (i.e. every 10th user with a proper ID card would not be recognised and would be subjected to a further test). For the Smartgate face recognition system in Sydney airport (the security check for Quantas crew), an average processing time of 14 seconds, and a false rejection rate of 2% is reported. It is to be noted, however, that this performance is achieved with regular (daily) users, who were given special training, and building measures to control lighting, and live updating of the templates (i.e. the image taken to verify is used to keep the reference image up to date). These measures are not only expensive, but updating of images cannot be contemplated for the ID card, since the security risks of doing this in a distributed system (i.e. biometric equipment at various border control points a citizen might pass through) are unacceptable.

Acceptance: Many people have concerns about interacting with the technology. Contact sensors (e.g. those used for fingerprint recognition) raise hygiene concerns. Iris recognition raises concerns about potential damage to the eye in longer term use, and whether the iris image could be used for health diagnostics. Whilst from a scientific point of view, these concerns are without basis (touching a FP sensor is no different from touching a door handle, taking photographs of the eye should neither irritate nor damage it), the existence of those concerns need to be addressed. Other concerns (often based on scenes from Hollywood movies such as James Bond or Minority Report) are expressed about physical safety (criminals might cut off fingers or rip out eyeballs to overcome biometric scanners). The other key category of concern is related to hidden

identification and tracking of individuals. For the biometrics proposed for the ID card, this applies particularly to face recognition.

Fingerprinting

There are two key points concerning fingerprinting that are likely to compromise the government's objectives. The first is that the proposed system is not "universal". A significant number of people will not be able to use it. The GAO report concluded that the fingerprints of about 2 to 5 percent of people cannot be captured "because the fingerprints are dirty or have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals".

These findings are supported by the biometrics industry. BarclayCard has conceded that trials with fingerprint biometrics proved them too unreliable as a means of verifying identity. People who had recently used hand cream created serious problems for the fingerprint readers, as did people with particularly hard or calloused skin, such as chefs, gardeners and labourers.

The GAO report raises other concerns that challenge the universality proposition for biometrics. It advises that comparative biometric testing has shown that "certain ethnic and demographic groups (elderly populations, manual laborers, and some Asian populations) have fingerprints that are more difficult to capture than others."

Error rates in fingerprinting are both significant, and poorly understood. According to a recent review[106] of available systems, only a handful of products achieved an equal error rate of under 3%, and the performance of most was much worse. Furthermore, it would be hazardous and risky for governments to lock their core infrastructure into a single proprietary product while both attack and defence are evolving rapidly.

According to one expert, our understanding of fingerprints "is dangerously flawed and risks causing miscarriages of justice".[107] Amongst the numerous cases of mistaken identification through fingerprinting, that of Brandon Mayfield is indicative of the many problems in assessment and interpretation of fingerprint data.

Following the Madrid Bombings of March 11, 2004, Spanish National Police managed to lift a fingerprint from an unexploded bomb. Three highly skilled FBI fingerprint experts declared that Oregon lawyer Brandon Mayfield's fingerprint was a match to the crime scene sample. U.S. officials described the match as "absolutely incontrovertible" and a "bingo match". As a former U.S. soldier, Mayfield's fingerprint was on the national fingerprint system. Mayfield was imprisoned for two weeks. The fingerprint, however, was not his. According to one law professor,

> "The Mayfield misidentification also reveals the danger that extraneous knowledge might influence experts' evaluations. If any of those FBI fingerprint examiners who confidently declared the match already knew that Mayfield was himself a convert to Islam who had

[106] Fingerprint Verification Competition 2004, Open Category Results: Average results over all databases, Preliminary results, http://bias.csr.unibo.it/fvc2004/results.asp.
[107] 'The Achilles' Heel of Fingerprints', J.L. Mnookin, Washington Post, May 29, 2004.

> once represented a convicted Taliban sympathizer in a child custody dispute, this knowledge may have subconsciously primed them to "see" the match. ... No matter how accurate fingerprint identification turns out to be, it cannot be as perfect as they claim."[108]

When Mayfield's personal information was combined with the crime scene evidence, the FBI was convinced of his culpability. Yet according to a recent panel of experts, they were wrong.[109] As the collection of biometric information increases, and as it moves from law enforcement to civilian applications, the error rate may significantly increase.

Iris recognition and blind and visually impaired people

Iris recognition is a relatively new identification technique. In the decade since the iris identification algorithms were patented, nearly all technical reports and trials have been conducted at a general level. It appears that no trials have been undertaken with specific reference to blind or visually impaired users. When such people are unable to use a system for whatever reason, they are referred to within the biometrics industry as the "outlier" population (the members of which are colloquially known by the industry as "goats").[110] They are frequently excluded from research trials. The reported levels of accuracy and acceptability of iris recognition therefore tend to be based on analysis of those who are physically able to use the technology rather than representing a cross-section of the community.

A distinction should be made between the "outlier" population – those who physically cannot use the technology – as opposed to the population who would find the technology difficult to use or who would produce inconsistent data. The latter group may be larger than the outlier population. Not all blind and visually impaired people will be unable to use iris recognition technology. Indeed it is quite possible that most people will interface with iris recognition, though perhaps with varying degrees of difficulty. Such situations will be covered later in this report.

Research findings and medical literature indicate significant potential problems for blind and visually impaired people when using iris recognition systems.

A 2002 technology assessment report by the U.S. General Accounting Office (GAO) highlighted a number of problems with the accuracy of iris recognition.[111] While acknowledging that the mathematics of the technique appeared sound, the enrolment and verification elements of iris recognition were far from perfect. The Failure To Enrol Rate was around half a percent, while the False Non Match Rate ranged from 1.9 to 6 percent. This means that around 1:200 of the research population could not enrol, while a further 1:18 to 1:50 could not match their enrolled iris.

[108] Ibid.
[109] 'FBI Faulted in Arrest of Ore. Lawyer', B. Harden, Washington Post, November 16, 2004.
[110] See references to this term, for example, in http://www.speechtechmag.com/issues/3_3/cover/442-1.html
[111] U.S. General Accounting Office, Using Biometrics for Border Security, Washington DC, 2002, http://www.gao.gov/new.items/d03174.pdf.

It is unclear how much of this failure was due to the inability of visually impaired people to interface with the technology, however the report does acknowledge that iris technology can be hindered by poor eyesight. It also states that people without glasses have a lower FNMR than people wearing glasses. Importantly, the report – one of the most substantial yet published – warns:

> People with glaucoma or cataracts may not be reliably identified by iris recognition systems.[112]

Biometrics researchers – and the industry itself - generally acknowledge the limitations of iris technology for blind and visually impaired people. A report published in the FBI Law Enforcement Journal observed:

> Although the theory requires additional research, some evidence suggests that patterns in the eye may change over time because of illness or injury. Therefore, eye identification systems may not work for blind people or individuals with eye damage.[113]

This view is reflected in various studies and reports. One industry report states:

> Subjects who are blind or who have cataracts can also pose a challenge to iris recognition as there is difficulty in reading the iris.[114]

A report for the European Commission observes:

> The iris recognition systems had public acceptability problems in the past because of the use of an infrared beam. The recent systems register the iris image at a distance from the user but users are still sceptical of this technology. Blind people or people with severely damaged eyes (diabetics) will not be able to use this biometric method.[115]

A study by the UK National Physical Laboratory reported that:

> (iris recognition) tests revealed difficulty in enrolling a blind person's iris because the system required both eyes to be enrolled.[116]

While the European Telecommunications Standards Institute (ETSI) acknowledges:

> Iris recognition may fail in the case of a blind eye.[117]

---

[112] ibid p.73.
[113] Stephen Coleman, Biometrics: solving cases of mistaken identity and more. Source: FBI Law Enforcement Bulletin v.69 no.6 (June 2000), p. 9-16, ISSN: 0014-5688 Number: BSSI00019069, http://www.nesbary.com/class/621w02/articles/coleman.htm.
[114] Penny Khaw, Iris recognition technology for improved authentication, SANS Institute, 2002 http://www.sans.org/rr/papers/6/132.pdf.
[115] European Commission, Final Report - Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication Including an Appraisal of the Areas Where They are Most Applicable, April 1997, http://66.102.9.104/search?q=cache:gbLP6j2f8KMJ:ini.cs.tu-berlin.de/~schoener/sem-biometry/polemi97_eu_report_biometrics.doc+%22iris+recognition%22+%22blind+people%22&hl=en&ie=UTF-8.
[116] Tony Mansfield, Gavin Kelly, David Chandler, and Jane Kane, CESG Contract X92A/4009309 Biometric Product Testing Final Report, Draft 0.6, Middlesex: National Physical Laboratory.

The biometrics industry appears reluctant to publicly discuss the prevalence of the outlier problem. However, in an industry presentation, Iridian Technologies has stated that the outlier population for iris recognition is "less than two per cent".[118] This may represent up to a million people in the UK.

This is a substantially larger outlier population that has been previously acknowledged. In its public statements, industry often cites the incidence of Aniridia, in which a person has no iris. Studies have shown Anaridia to occur in about 1:60,000 births. This prevalence would translate to almost 1,000 UK residents.[119]

This however is only one of many populations that may be unable to register with an iris recognition system. One medical report examining iris changes following cataract surgery concluded:

> Cataract procedures are able to change iris texture in such a way that iris pattern recognition is no longer feasible or the probability of false rejected subjects is increased. Patients who are subjected to intraocular procedures may be advised to re-enrol in biometric iris systems which use this particular algorithm so as to have a new template in the database.[120]

More than 200,000 cataract operations are performed each year in the UK. The objective of the NHS "Action on Cataracts programme", initiated in 1998, is to increase the number of cataract procedures carried out in the UK to 250,000 per year.[121]

The Nystagmus population is also likely to be at a disadvantage when using iris recognition technology. The inventor of the iris algorithms, Dr John Daugman, has acknowledged:

> Persons with pronounced nystagmus (tremor of the eyes) may have difficulty in presenting a stable image; however, some iris cameras now use stroboscopic (flashed infrared) illumination with very fast camera integration times, on the order of milliseconds, so tremor becomes unimportant for image capture.[122]

Whether the estimated 60,000 or so people with Nystagmus in the UK will be able to use iris biometric systems will depend entirely on whether the government is prepared to ensure that appropriate iris camera equipment is made generally available, both in the enrolment phase and for all points of verification of the iris.

Daugman has also identified a larger problem facing blind and visually impaired people:

---

[117] ETSI EG 202 116 V1.2.1 (2002-09) Design for All, Human Factors (HF) - Guidelines for ICT products and services, http://docbox.etsi.org/EC_Files/EC_Files/eg_202116v010201p.pdf.
[118] Industry presentation by Iris Australia & Iridium, http://www.sensory7.com/presentations/DSD.ppt.
[119] emedicine.com, http://www.emedicine.com/OPH/topic43.htm
[120] Roberto Roizenblatt et al., Iris recognition as a biometric method after cataract surgery, *BioMedical Engineering OnLine* 2004, 3:2.
[121] Cited in EuroTimes, published by the European Association of Cataract and refractive surgeons, http://www.escrs.org/eurotimes/archive/nov_dec2000/ukopthamologists.asp.
[122] John Daugman, Iris Recognition, available at http://www.icdri.org/biometrics/iris_biometrics.htm.

> Blind persons may have difficulty in getting themselves aligned with the iris camera at arm's length, because some such systems rely on visual feedback via a mirror or LCD display to guide the user into alignment with the camera.[123]

Daugman describes the existence of sophisticated iris cameras that "are mounted on automatic pan and tilt platforms that actively home in on an eye, including autozoom and autofocus". Again, the need for such technology at a universal level must be recognised from the outset by government if integrity of iris readings is to be maximised throughout the population.

Industry selectively acknowledges such difficulties. One Australian iris technology company reports:

> There is a very small outlier population that cannot use Iris Recognition. These are mainly people who have had cataracts or have experienced extreme trauma and scarring to both eyes.[124]

The company does not mention problems relating to visual prosthesis, nystagmus or total blindness.

There are however many circumstances where enrolment with an iris system is possible, but difficult. The iris division of the U.S. based LG Electronics optimistically observes:

> While blind people can be difficult to enrol, there are instances where blind people have used iris recognition successfully.[125]

There appear to be substantial practical difficulties facing people who have even minor eye conditions or visual aids. The UK trials of iris recognition have been suspended because of such problems.[126] One IT industry publication reported:

> (O)n Thursday (6 May), MPs testing the iris-recognition technology were told that up to 7% of scans could still fail, due to anomalies such as watery eyes, long eyelashes or hard contact lenses.[127]

Multiple biometrics

The Home Office has stated that it intends dealing with iris recognition failures by instituting a second or third biometric – fingerprints or facial recognition. The GAO report makes the point that the False Non Match Rate for fingerprinting can be extremely high – up to 36 percent. The failure of facial recognition can be even greater.

---

[123] Ibid.
[124] Argus technology website http://www.argus-solutions.com/about_overview.htm
[125] Website information http://www.lgiris.com/iris/index.html
[126] Hard contact lenses cause the recognition system to fail because their diameter is less than the diameter of the iris. Light reflection off the surface of glasses or contacts can cause an unacceptable FTER or FNMR. The iris code is, in effect, trinary: Each bit could be either 0, 1 or read as "couldn't measure this bit with sufficient confidence". With partial occlusion (long eyelashes etc) the number of uncertain bits exceeds a threshold and the measurement must be attempted again.. With eye damage, depending on the system threshold used, measurement may be impossible and must be stopped. If the threshold is set too low there will be too many false matches.
[127] 'Technical glitches do not bode well for ID cards, experts warn', Computer Weekly, May 7, 2004.

If we assume that this overall failure rate is representative in the population of blind and visually impaired people, there will still be a large number of people who are consistently rejected by the system after considerable effort. Such a situation, at both a legal and a societal level, would be unacceptable.

We believe that the above data clearly establishes that there is a strong likelihood that iris recognition will create substantial difficulties and potential denial of services to blind and visually impaired people. With this background in mind, the specific elements of the draft legislation will now be addressed.

This data presents challenges to the implementation of a national identity system that employs iris recognition. At a level of principle and practicality any legislation should ensure:

- That visually impaired people will not be denied access to services because they are physically unable to register for an Identity Card;

- That visually impaired people will not encounter discrimination in the use of identity systems;

- That visually impaired people will not encounter hardship or difficulty when registering for a card.

- That the legal requirements imposed on individuals set out in the Bill do not place blind and visually impaired people at greater risk of prosecution than would be the case for fully sighted people.

The research cited above raises concerns that aspects of the Identity Cards Bill may bring about a violation of standards, right and safeguards set out in instruments such as the *Disability Discrimination Act* 1995 & the *Code of Practice of Rights of Access to Goods, Facilities, Services and Premises*. These and other provisions seek to ensure that organisations provide that their procedures and infrastructure do not create disadvantage to people with a disability.

The possible use of iris scanning is one of the principal concerns with the Identity Cards Bill. There exists a threat that this technique may inherently discriminate against people with visual impairment.

The available literature indicates that blind and partially sighted people may be unable to use such systems, may generate unstable or unusable biometric data, or may suffer disproportionate disadvantage in using such systems. The research indicates that because of a deteriorating or unstable sight condition many blind or partially sighted people will either not be able to provide Iris Recognition data on enrolment or will subsequently provide an altered reading during routine checks or renewal. The Bill provides for the imposition of a variety of penalties and offences that may unfairly apply to blind and visually impaired people who in good faith use iris systems, but are unable to provide data that is accurate or consistent.

The environment of public trust

The creation of public trust in a national identity system depends on a sensitive, cautious and cooperative approach involving all key stakeholder groups. Public trust thrives in an environment of transparency and within a framework of legal rights. Importantly, trust is also achieved when an identity system is reliable and stable, and operates in conditions that provide genuine value and benefit to the individual. We are not confident that these conditions have been satisfied in the development of the Identity Cards Bill.

Public opinion should be separated from public trust. Opinion polls consistently demonstrate public support for the concept of an identity card, and yet the detail of those polls indicates that people have little trust in the core elements of the proposed scheme. Nor, according to the polls, is the overwhelming majority of the population convinced of the benefit of the identity card. Few are prepared to pay the sum proposed by the government.

A review of polling data suggests that the headline support figure for an identity card translates more accurately into support for the *goals* of an identity card – counter-terrorism, fraud reduction, illegal working and law enforcement objectives. While this level of response is not unusual in polling on public interest policies, it is especially relevant to the success of the identity card. Long-term public cooperation is essential to the success of a policy of this complexity and importance.

Public opinion

Currently, support in principle for a national identity card is substantial. Opinion polls commissioned both by organisations supporting the proposals (e.g. Detica) and by groups opposing them (e.g. Privacy International) have uniformly highlighted a headline support figure of around eighty percent of the population. Polling results in most categories are remarkably consistent.

An April 2004 Detica/MORI poll[128] provides some insight into public expectations of the government's proposals. A third of the population surveyed tended to support a card because they believe it will prevent illegal immigration. This was by far the most popular motivation, followed by 21% who perceived it as an aid to law enforcement, and 16% who felt it would be an aid in the fight against terrorism.

Proposals to charge people directly for a card appear to be the key trigger for public concern. A recent poll (from Reform/ICM)[129] indicated that 81% of UK adults support government ID plans. However, this headline support was reduced to 67% once the costs of the scheme were mentioned (with 31% of those surveyed not wanting to pay anything towards a card, and another 30% only willing to pay up to £10 – much less than the government is planning to charge).

[128] Detica/MORI poll, http://www.mori.com/polls/2004/detica.shtml.
[129] Reform/ICM poll, http://www.reform.co.uk/filestore/pdf/041203%20id%20cards%20tables.pdf.

Public support appears more complex when other polling figures are examined closely. The April 2004 Detica/MORI poll found that two-thirds of those surveyed knew "little or nothing" about the ID scheme. There is some evidence that other countries that have introduced proposals for ID cards have found that public opinion has turned sharply against card schemes once their full details and implications become clear. In Australia, initial support of 90% for an "Australia card" turned within months to opposition of 70% as details of the legislation were analysed by media commentators.

As the UK proposals move through Parliament and towards actual implementation, they are likely to receive far more specific attention from the media and the public. Even at this stage, the Reform/ICM poll found that a smaller majority (58%) was happy with the scheme's key feature of a centralised database of fingerprints and iris scans. This is roughly consistent with an earlier Privacy International/YouGov poll[130] that found a support of 61% for the database. The ICM survey found opposition of 54% to £1,000 fines for failing to notify the government of a change of address, and an even split over whether increasing the number of police officers would be a better use of public funds. A similar level of opposition to address requirements was also found by the Privacy International/YouGov poll in May, with 47% opposed (24% strongly) to notification requirements.

Public trust in the ability of government may also be a contentious issue. The MORI poll found almost 60% of those surveyed had little or no confidence in the Government's ability to introduce a national ID system smoothly.

Public expectations and perceptions

The LSE's research indicates that three components of the identity proposals are likely to become prominent in public attitudes. These are (a) the biometrics element of the scheme, (b) the privacy and security of personal information, and (c) the balance between the financial cost of the system as its value to the individual.

The expectations and presumptions that drive public opinion are clearly more significant than the headline support figures themselves. These underlying attitudes have been assessed through research into focus group outcomes. Annex Two provides details of a study into the views of people with regard to biometrics. The results indicate that science fiction movies are a key driver of opinion and perception, that security is a keyword for those who support the technology, while surveillance and control are key negatives for those who are concerned about the technology.

These results indicate that much has yet to be done to provide a solid foundation of knowledge and awareness of these advanced technologies. Until then, public support is likely to be fickle.

[130] Privacy International/YouGov poll, http://www.privacyinternational.org/issues/idcard/uk/idpollanalysis.pdf

Design principles and options

Much of the controversy, challenges, and threats arising from the Government's identity proposals are due to the technological design itself. While it is true that many of the technological details remain undetermined and are to be established at a later date in secondary legislation, some of the larger decisions regarding the architecture of the scheme are already decided, and are encoded within the bill.

There are many ways to design even the simplest technologies. The course of history has been dramatically shaped by small decisions regarding a technology. Whether it was the intention of the designer, early applications and market opportunities, the social norms at the time, or a myriad of other factors, small decisions have transformed the way our society works. This is the transformative potential of technology as both an enabler and as part of the infrastructure of society.

With Government projects as important as a national identity system, technological choices are crucial. Relatively simple choices, such as which department or ministry is responsible for the design of a government infrastructure, may shape future policy decisions radically, and may even determine entire courses of action. For example, in the U.S. the choice of which arm of the military would be responsible for the nuclear infrastructure dictated much of the Cold War policy because of the use of Air Force missile silos rather than Army installations that were mobile. Similarly, when a ministry of energy is responsible for research into nuclear power, the power generators that result differ significantly from those designed by a defence ministry.

When the Home Office is the proponent and selector of an infrastructure as vast as an identity system, the choices made in the basic design of the system will reflect the interests and expertise of the Home Office. This is particularly important in the design of an ID card, particularly as its design goals include not only combating crime, but also enabling e-government, enhancing trust in commerce, and providing the 'gold standard' for identity in Britain. The Home Office's design choices are in stark contrast to the system being developed in France, emerging from the Ministry for the Civil Service, State Reform and Spatial Planning. The ID Card Bill for the UK proposes a massive complex centralised system with an audit trail that focuses on identification, while the French system proposes a simpler decentralised and user-oriented system that focuses on confidence-building.

In other sections in the report we addressed issues on international environment and public opinion. This section identifies the core differences between the scheme proposed here compared to other countries. We also look to public opinion as a guiding principle in the design of the system, trying to build an infrastructure that would work from existing trust relations and local identity requirements. The audit trail is the greatest challenge to the proposed UK system, complicating the architecture unnecessarily, placing the bill and the ID system on legally problematic grounds, and ignoring the existing identification structures in British society.

The Challenges Arising from the Government's Model

Despite claims of harmonisation and creating a system that is consistent with international obligations and practice, the Government contradicts these claims by designing a system of unprecedented complexity. As the Home Secretary stated in his first speech on the introduction of the Identity Card Bill, (it) is a mistake in believing that what we are putting forward is a replica of anything else that actually exists across Europe and the world".[131] Technological and legal challenges emerge from these important differences.

Three salient features distinguish the Home Office scheme from other identity card systems planned or deployed elsewhere in the world.

- the accumulation of a lifetime "audit trail" of the occasions when a person's identity has been verified and information from the database disclosed;
- the construction of a central database containing biometrics for an entire population, to be used for broad purposes, with the intention of eliminating the possibility that each individual could be enrolled more than once;
- the insistence on a single standard identity in order to generate trust, replacing or reframing British social and economic relationships.

These novel aspects raise important questions of compliance with Article 8 of the European Convention of Human Rights, which allows for state infringements of privacy only to an extent which is *necessary in a democratic society* and *proportionate* to permitted justifications which include a "pressing social need" and national security.

Along these lines, the UK Parliament's Joint Committee on Human Rights recently published a report that seriously questions the compatibility of the ID Cards Bill with the European Convention on Human Rights. The Committee states that

> "For interferences with Article 8 rights to be legitimate … it must be shown that they interfere with privacy rights to the minimum degree necessary, and that their aim could not be achieved by less intrusive means …"

From our research and interviews with computer security experts, the currently envisioned national ID card does *not* meet this test.

If there are reasonable technological alternatives to the Home Office's scheme which can accomplish the objectives permitted by ECHR Article 8 in a way which causes less infringement to the privacy rights of the individual, then compliance with ECHR requires these technological alternatives to be adopted.

[131] Home Secretary Speech to the IPPR, November 17 2004, http://www.homeoffice.gov.uk/docs3/identitycards_041118speech.htm.

Audit trails and the arising legal questions

The Identity Cards Bill defines a category of data to be held in the Register database that has come to be known as the "audit trail".[132] It consists of a record detailing occasions when an individual's identity is checked, and consequent disclosures of information. It is the last definition in the text of the legislation, but it is of the first importance in evaluating the design of the system and the impact on civil liberties .

The Parliamentary Joint Committee on Human Rights report on the Bill states that the ECHR infringement caused by the audit trail is **particularly** significant since it

> ...will include a record of the occasions on which his or her entry on the Register has been accessed by others (clause 1(5)(h)), for example, in the use of public services, or by prospective employers, or as part of criminal investigations (regardless of whether these result in prosecutions or convictions). Thus the information held on the Register may amount to a detailed account of their private life.[133]

On the face of the Bill, access to the audit trail is limited to Agencies concerned with serious crime and national security, however the JCHR notes that:

> it is a particular concern that the order-making power in clause 22 would allow the Secretary of State to make further provision for disclosure of this material, without the need for additional primary legislation.[134]

Moreover, the Regulatory Impact Assessment published by the Home Office states that:

> The verification service will be available not just to the authorities responsible for maintaining immigration controls but to providers of public services and private sector organisations.
>
> Key ID card checks would be performed online to minimise the usefulness of high quality forged cards and to provide an audit trail. Following consultation with key user groups, there is a clear requirement for most verification checks to be made on-line. Ongoing specification work is taking account of the need for the verification service to have the necessary capacity to support this.[135]

The Home Office envisions a "single, standard verification service, operating online to achieve full security, (with a) full audit trail of card use".[136] Consequently, the audit trail could contain an entry for each instance of online verification to the central database,

---

[132] Sch.1(9)….(a) particulars of every occasion on which information contained in the individual's entry has been provided to a person; (b) particulars of every person to whom such information has been provided on such an occasion; (c) other particulars, in relation to each such occasion, of the provision of the information.
[133] JCHR, 5th Report, January 26, 2005, para.13 http://www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/35/35.pdf.
[134] Ibid para.42.
[135] http://www.homeoffice.gov.uk/docs3/ria_251104.pdf
[136] Home Office presentation to Intellect, December 16, 2004, Slide 20, http://www.homeoffice.gov.uk/docs4/Intellect_HO_FINAL.pdf.

building up an increasingly dense set of transaction events, across the public and private sectors, so that the trail could become a general means of tracking and profiling the behaviour and activities of individuals in society, showing where/when/why any checks took place.

The privacy implications were briefly explored in Commons Standing Committee:[137]

> Mr. Richard Allan: ...Another point that it might be helpful to have clarified is the scope of the audit trail… Will they form a whole-life record? That is the key question. Are we saying that from the moment somebody gets an identity card, which is going to be fairly swiftly if the Government have their way, the audit trail will be kept for whole of life? If at no point will it be deleted as historic data, the data that can be disclosed under clause 20(4) will be potentially intrusive and comprehensive. The public ought to be aware of the extent to which those data will be kept and the circumstances under which they may be disclosed.
>
> Mr. Humphrey Malins: …for how long the audit trail will continue. Will it continue to my death, perhaps 50 years later? By then, what information about me will have been built up on the Register? Virtually all my business and domestic activities, and my travel, will be on there for people to access. Is there a cut-off point, after a certain number of years, when this information will be deleted?...
>
> Mr. Des Browne[138]: ... in relation to an individual's civil liberties, I would much rather that such information was preserved. I can see arguments why deletion of that information would give a false impression of the way in which an individual's information had been accessed. Once it was deleted and lost, the fact that information had been abortively accessed on a number of occasions would be lost, and that might be just the sort of thing that a commissioner would want to comment on. For clear and understandable reasons, I am not prepared to set out now the parameters for when that information should be stored or deleted. That will develop over time, and it will be a matter for the commissioner.

The Identity Cards Bill (clause 26) provides for the Intelligence Services Commissioner to keep under review the Agencies' acquisition, storage and use of information from the Register, and for any associated complaints to be dealt with by the Investigatory Powers Tribunal, but neither appears to be explicitly empowered to access any portion of audit trails relating to Agencies' usage (i.e. a clause analogous to Cause 24(4)). In fact, the Bill does not require a comprehensive audit trail of access by intelligence and serious crime agencies, or by any other parties. Clause 3 and Sch.1(9) only provides that an audit trail may be recorded. The analysis below presumes these provisions are

[137] Identity Cards Bill Standing Committee, Hansard, January 27, 2005, http://www.publications.parliament.uk/pa/cm200405/cmstand/b/st050127/am/50127s02.htm.
[138] http://www.publications.parliament.uk/pa/cm200405/cmstand/b/st050127/am/50127s04.htm.

unintended omissions from the Bill as drafted, which will be rectified in later legislative stages.

The audit trail and the Data Protection Act 1998

Under the Data Protection Act 1998, individuals have a general right of access to personal data held about them. The Information Commissioner has commented in relation to apparent restrictions on this right of "subject access" in the Draft Bill, that in the current Bill,

> "there is no longer any attempt to restrict an individual's right of access under the Data Protection Act 1998 to certain 'audit' or 'data trail' information."[139]

The Home Office has even attributed their decision to create such extensive data trails to "representations from the information commissioner".[140] If true, this amounts to an own-goal for the national regulator of information privacy, because the consequence of creating a dense and perhaps ubiquitous audit trail are a much worse outcome for privacy than the potential abuses against which it is purported to act as a safeguard.

Access of any part of an individual's entry in the Register (including access to the audit trail) should itself generate a corresponding new entry in the audit trail. Therefore the entries in the audit trail will logically comprise two types of event:

- **consented or aware** : a person presenting their card for online verification, to authorise use of some public or private service, and concomitant disclosure of information from the Register. This includes occasions when an individual exercises their right of subject access to information held in the Register, and disclosure of that information to the data subject.
- **non-consented or unaware** : access to the Register without the individual's awareness and/or specific consent, for example to ascertain identity by means of matching with a live biometric obtained after arrest by the police, or checks by a public or private organisation empowered to do so without notifying the individual.

It is critically important to note that audit trail events of the first kind reveal information about the individual's activities, behaviour and movements, whereas the preponderance of audit trail events of the second kind record the activities and behaviour of organisations conducting checks on the Register.

Disclosure under a Subject Access Request

Under DPA 1998, disclosure of information to an individual asserting their subject access right is exempted to the extent it would be:

---

[139] The Identity Cards Bill - the Information Commissioner's Perspective, http://www.informationcommissioner.gov.uk/cms/DocumentUploads/The%20Identity%20Cards%20Bill%20Dec%2004.pdf

[140] Stephen Harrison's speech to the Law Society, reported in the Guardian 23rd March 2004, 'Government will Track ID card use', http://www.guardian.co.uk/guardianpolitics/story/0,,1175638,00.html.

- s.28 – required for the purpose of safeguarding national security
- s.29 – likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature.

Exemption for national security

The validity of an exemption claimed under s.28 is adjudicated by the Information Tribunal (National Security Appeals), and was tested in a 2001 case involving Norman Baker MP.[141] The Security Service claimed that under the Neither-Confirm-Nor-Deny (NCND) doctrine, a blanket ban on any disclosure of their records was justified. The Tribunal rejected the validity of the certificate imposing a blanket ban, because it held that there were conceivable circumstances under which disclosure might not breach the NCND doctrine.

Whether the exemption is claimed under a blanket or a case-by-case Ministerial certificate, under DPA 1998 it is certain that information disclosed to individuals about their audit trail will be redacted of any and all events pertaining to access by the intelligence and security Agencies. A fortiori, in relation to national security purposes, the right of subject access is irrelevant to providing redress against abuses harming the individual**.**

Exemption for prevention and detection of crime

If the trail contained records of access to the Register for reasons which would engage the exemption allowed by DPA s.29, then the audit trail disclosed to the individual could be redacted of access events pertaining to such reasons. Thus the disclosed trail would not indicate Register access by serious crime agencies, or other users empowered under clause 22, to the extent that exempted "prejudice" would likely be caused. A fortiori, in relation to the exempted purposes of DPA s.29, the right of subject access is irrelevant to providing redress against abuses harming the individual**.**

Differentiating between two types of audit trail events

As shown in the analysis above, the right of Data Protection subject access to the audit trail would not reveal information about access to the Register by security, intelligence and in many cases law enforcement agencies (assuming that the audit trail will contain information about access by any of these agencies – which as noted previously is not explicitly required by the Bill as drafted).

The rationale for the existence of the audit trail is ostensibly to provide the individual with a means to seek redress in cases of abuse (so far as permitted by subject access exemptions), and the Commissioners and Tribunals with evidence to detect, investigate and substantiate instance of abuse and complaints, in the interests of the individual. The trail might also serve a secondary function as a means of surveillance, to ascertain the whereabouts and activities of an individual, perhaps over an entire lifetime.

[141] *Norman Baker MP v. Secretary of State for the Home Department*, Decision by the Information Tribunal, http://www.dca.gov.uk/foi/bakerfin.pdf.

From the point of view of protection of the individual, the audit trail of Register access events, of which they are not aware or for which their consent is not required, should be maintained for a sufficient period to allow redress of abuse, but there is no such compelling reason in the interest of the individual to retain a trail of consented/aware access events indefinitely.

The design implications of fixing this problem are relatively simple. There is no technological reason why an individual should not exercise their right of subject access to their audit trail by periodically "downloading" a copy to a personal computer from an online portal to the Register provided for this purpose. The evidential integrity of this audit trail data could be guaranteed by certifying it with a digital signature affixed by the Register, (in accordance with the Electronic Communications Act 2000). There is then no necessity to require the Register to maintain an original copy of the data, and it could be deleted if the individual wishes. Of course the Register would create a new audit trail from that time going forward, until again downloaded and deleted. Any subsequent claim and investigation of abuse could rely on audit data in the individual's custody (and if necessary cross-checked with decentralised secondary records held by public or private organisations empowered to make use of the Register).

It may be argued that it would be useful for the Register to keep a copy of the trail in case the behaviour/whereabouts/activities of the individual subsequently needed to be investigated for some official purpose. But such retention would need to be justifiable under the provisions of the Data Protection Act and ECHR Article 8 tests of necessity and proportionality.

It may also be argued that the idea of downloading and then erasing trails of the consented/aware events will only be of interest to an technophile elite, but the design and operation principles established through primary legislation should be durable, and it is only in the past decade that most people have had access to personal computers and the Internet.

There is therefore overall a strong case for differentiating between audit trails events pertaining to Register access and identity verification of which the user is aware or to which they have consented, and other types of event. It is **not** in the interests of the individual for a comprehensive trail to be retained indefinitely - the cumulative threat to privacy will at some point outweigh the risk of ancient abuse claims incapable of pursuit. Furthermore the Investigatory Powers Tribunal imposes a one year time-limit on their acceptance of complaints, which would apply equally in relation to complaints about the conduct of Agencies in relation to the ID scheme.

At any rate, the residue of trails left after deletion of consented/aware events (at the individual's discretion) would logically be those occasions when the Register was checked without the knowledge or permission of the individual. The former category constitutes a dossier of life events and behaviour about the individual and is therefore highly privacy-invasive, but the latter are predominantly information about the behaviour of organisations using and accessing the Register. There is thus a compelling rationale to distinguish and clearly separate requirements and policies for the recording of these two types of events in any audit trail.

There are strong technical and legal analogies with the debate over the mandatory retention of telecommunications traffic data (cf. Anti-Terrorism Crime and Security Act 2001 Part.11), but with these differences:

- audit trails are strictly superfluous to the function of the Register, rather than arising through ordinary business processes;
- the data are created and retained centrally by a government-operated online authentication service, rather than scattered in different private-sector (ISP and telephone company) records systems. (ECHR Article 8 therefore fully applies);
- the debate in Standing Committee strongly suggests government currently intends no finite limit on retention, and deletion will be the exception not the rule;
- the trails are very strongly authenticated to the individual, and thus more privacy invasive than other forms of retained data (e.g. traffic data).

The way to cut the Gordian knot that abuse cannot be redressed unless an audit trail exists, is that there should be a retention period fixed by statute (perhaps one year – in line with the remit of the IPT) after which all audit trails should be deleted. A long or indefinite retention period will over time become the main privacy threat to the individual, one that outweighs the risk of a potential inability to pursue redress, but this does not seem to have been widely appreciated so far in public debate.

Design Considerations and Legislative Implications of Audit Trails

- In order to deal with privacy issues arising from access to the central register, the audit trail should record all occasions when access or verification takes place without the consent or awareness of the individual;
- The Investigatory Powers Tribunal and Intelligence Services Commissioner would benefit from direct access to the complete audit trail, including those portions recording access events within their purview authorised under clause 23(5);
- We may distinguish the trail of access and verification events of which the user is aware or to which they have consented from other types of event, and require deletion after a period fixed by statute, or sooner at the individual's request;
- It is technologically feasible to require the provision of online Data Protection subject access to trails, at the discretion of the individual and certified as valid with an official digital signature from the Register. The ID card itself can be used as the means to authenticate subject access online;
- To enable such a system to operate within the confines of British law, through the design of the system we can ensure that Commissioners and Tribunals can accept trails in user possession, certified by an official digital signature, as valid evidence in any complaint or investigation of abuse, and we can ensure that unauthorised parties cannot accumulate and retain copies of audit trails through periodic and incremental lawful access to the Register, beyond the fixed statutory period allowed for retention in the Register.

The central biometric database with broad purposes

Another challenge to the proposed ID card and Register scheme remains that, in order to have a biometric system that is proof against duplicate enrolment of individuals, it would appear to be necessary to be able to check each enrolment against a central database of biometrics already enrolled. This would involve a central database with over 60 million records containing personal information such as fingerprints, iris-scans and other biometrics.

A centralised database solution necessarily gives rise to enormous additional privacy challenges. An alternative scheme would involve the storing of biometrics on a 'smartcard', a card containing a digital processing chip with storage capacity. It is likely that the card envisioned by the Home Office is already going to be a smartcard, and if the ID Card is designed in accordance with the passport standards from the ICAO, then the biometrics will already be on the chip. The difference, however, is that the biometrics in the UK Identity Card scheme will include a database holding copies of the biometrics. There is an enormous difference in the implications for the human right to privacy between this type of system, and one where a biometric is only stored locally in a smartcard, as recognised in opinions of the EU Article 29 Working Party on Data Protection.[142]

The Home Office has maintained that a crucial advantage of the proposed scheme is the provision of a unique and inescapable identity for each individual and avoidance of the possibility of multiple enrolments (which might be used for unlawful purposes).

But a system based on smartcard-stored biometrics would undoubtedly be much less costly in design and operation, because identity would be verified by a biometric reader matching against the template stored on the card, rather than online against a central database of biometrics. If attributes and facts securely stored and periodically refreshed on the smartcard were for some reason insufficient, there could still be a central Register of facts, but they need not contain biometrics. Offline biometric-reader terminals would be far less expensive because no online communication capability would be necessary, and no communication costs would be incurred each time the card was read.

Nor is it the case that online verification to a central database would be any more secure than offline verification against a biometric stored in the card. The authenticity of the biometric stored in the card could be checked by a cryptographic digital signature, which only government would hold the key to create, preventing fraudulent cards being created with a valid biometric.

It may be suggested that checking against a central database is more secure because data held centrally would be "fresher" than data held in a smartcard, or errors/omissions/malfeasance might occur resulting in differences between data held on the cards and a central database. However the database could and should rely on

[142] Article 29 Working Party, Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS), the European Commission, August 11, 2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp96_en.pdf and Article 29 Working Party, Working document on biometrics, August 1, 2003, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf.

cryptographic techniques[143] to ensure that any loss of integrity would be instantly detectable. Similarly, cryptography will be used to protect the communications data path between a biometric reader and the database in an online checking scenario. The cryptography and its implementation will have to be trusted for communication with and protection of a central biometric database. If one trusts the cryptography for online, why not for offline?

Would online checking help against very sophisticated insider attacks involving tampering with the database cryptography? The answer is no – these threats imply complete compromise to the integrity of the system. Any putative additional security value for online verification is illusory.

Also, offline verification provides a far more resilient system overall. A single, centralised online authentication service carries an inherent risk of systemic loss of service. A system based on biometric readers that match against templates stored on the card do not carry this additional and catastrophic risk of a single point of failure, and would permit most transactions to continue.

In summary a central biometric database system with online verification is much more costly, much riskier in operation, and for example is extremely vulnerable to distributed denial-of-service (DDoS) attacks on its authentication servers. Its sole advantage seems to be the possibility of preventing individuals enrolling with multiple identities.

The government has stated in support of the proposed scheme that one-third of terrorist incidents involve multiple or false identities. But it would be logically fallacious to infer that a system with unique non-duplicated identities could necessarily reduce the incidence of terrorism. Terrorists could continue to employ those modalities where they have operated under their real identities.

Little benefit fraud involves false or multiple identities, ranging from 1% to 3% . The vast majority involves misrepresentation of circumstances (undeclared income, housing benefit ineligibility etc.). To bear down on benefit fraud, cross-departmental data-matching could be used to detect false statements of circumstances, and this would be effective because inter-related claims must be connected through related identities. What has prevented this to date is a profusion of incompatible legacy systems that are unable to co-operate in data-matching cost effectively and reliably. Identification and identity management systems are only a small part of solving this problem.

More generally, the position in common law has traditionally been that use of an alias or pseudonym is lawfully provided if there is no fraudulent intent. Nevertheless, it is reasonable to ask if there is a risk that introducing an identity system in which multiple enrolment and a plurality of official identities was theoretically possible, could lead to an explosion in exploiting such a “loophole” for illegal purposes.

However, such concerns can be obviated by adopting some simple principles of cryptographic technical design, which are now being developed by IT vendors as

[143] Including, but not limited to, such as chained hash functions.

"Federated Identity"[144] systems, at least one of which has been endorsed by the French government[145] for precisely such purposes.

Design Considerations and Legislative Implications of Central Database

- In order to deal with the privacy and complexity issues arising from the central database model, we may prohibit biometric information from being stored in the Register;
- If there is an insistence upon the storing of biometrics on a central database, then for security purposes these may be recorded only if they employ privacy protection mechanisms which prevent identification unless for purposes specific to the function of that database;
- To ensure consistency, personal data can be redefined to include information derived from the scheme which is reasonably likely to be identifiable by any combination of parties;
- It is technologically feasible that identity claims may be made by means of cryptographic security tokens derived from the Registrable Facts, which contain the minimum personal data necessary to fulfil the intended purpose;
- To ensure consistency across government departments, we can require each public or private-sector service wishing to issue cryptographic security tokens derived from personal data in the scheme to provide a Privacy Impact Assessment to the Identity Scheme Commissioner and Information Commissioner, demonstrating how the design minimises infringement to privacy, in compliance with DPA 1998 and the Human Rights Act, for certification by both Commissioners.

Centralised Single Identity and British Social and Economic practice

When asked why they are in favour of ID cards, many of our focus group participants responded that they already carry around many forms of ID. There are two assumptions from their responses:

1. We have many forms of identification.
2. An ID Card would reduce the number of cards that we carry.

Here we look at these two assumptions in some detail. First, we confirm that indeed there are many ways of identifying yourself to the various public sector and private sector entities. Second, we note that the ID card as proposed by the Government could be used as a unique identifier to all of these entities. But we conclude that the ID card will transform all of these relationships that we held previously. In particular, the Government's proposed ID card is poorly designed for our daily lives. Finally, the ID card can never replace all of these forms of identification.

[144] For more information see: Liberty Identity Web Services Framework (ID-WSF) Supports SAML Version 2.0, February 11, 2005, http://xml.coverpages.org/ni2005-02-11-b.html and Federation of Identities in a Web Services World, A joint whitepaper from IBM Corporation and Microsoft Corporation, http://www-128.ibm.com/developerworks/webservices/library/ws-fedworld/.

[145] The French E-Government Strategic Plan (PSAE) 2004-2007, pp.15 http://www.adae.gouv.fr/IMG/rtf/Le_plan_strategique-GB.rtf.

Currently, individuals can gain access to government and private-sector services through the disclosure of personal information and through presenting some form of ID or authentication when required. But generally these relationships currently take place without disclosing a universal ID number. The forms of identification that we present to these entities either show proof of entitlement, or they provide use of service-specific account details. The advantage of the existing situation is not just that it is privacy-protecting. Rather, the greatest advantage of the existing systems is that each is purpose built and necessarily proportionate in their demands for personal information. They are relationships that have formed over time. People have become accustomed to disclosing this level of information and the entities are accustomed to managing this information.

Consider the situation of a student travelling on public transportation. The student may have received a student-ID card issued by the transportation firm, which is not granted to all people under 25, but merely to those who are students. The proposed ID-card could not be used in such a situation. Moreover, a rail-season ticket purchased by this student is often bound to the personal identifier on the student's travel-ID card. This is not necessarily bound to the student's school identification number, and it is certainly not bound to the student's bank account, NHS information, or other identifiers. It is an identifier issued by the transportation firm, independent of all of these other identifiers. The card expires in accordance with the policy of the transportation firm. For the student, she is assured that the card, when stolen, can only be used for transportation purposes. The student also knows that the transportation firm is only collecting the necessary amount of information on her to issue her the card and to provide transportation.

To appreciate the unlinked nature of today's identifiers, consider the following popular identification methods:

Birth names	User identifiers with service providers (account numbers)
Credit and debit cards	Calling cards
Loyalty Tokens	Employee Badges
Sports club membership cards	National insurance number
NHS number	Passport and passport number
Driver license and number	On-line usernames

As these examples illustrate, individuals today are represented by an abundance of identifiers that are *designed* to be relied on only by one or a few service providers *only in specific contexts*. An Internet Service Provider does not record our NHS number (and has no knowledge or concern whether we have been issued such an identifier, nor any means of linking to such a number). Sport club membership cards are not linked with our employee information, and are identifiers issued in accordance with club membership policies and requirements. As a matter of design, the identifiers held by the sports club are in essence useless to any other entity other than the sports club. It is also fair to say that in a number of these relationships, records are not even in a

computerised form. The personal data that is collected for the issuance of an identifier is not even verified, nor is it required to be.[146]

Local identifiers enable service providers to *identify* individuals within their specific transaction contexts, to create accounts for them, and to effectively deal with fraudsters. At the same time, local identifiers have the important benefit of limiting the capabilities of service providers to create profiles of an individual's activities with other parties. A pub owner does not need to know our name, birth date or birthplace but merely whether we are of the legal age to consume alcoholic beverages. Previously a relationship of trust would be established between the publican and the clientele; or a form of identity would be verified to ensure that the individual's birth year is prior to the threshold year. Our prior means of identification involved natural segmentation that ensures that *identity thieves* can only do damage with specific providers where they have gained information on users of those providers.

The transformation and reduction of local relationships

The envisioned national ID card would replace today's local non-electronic identifiers by *universal* identifiers that are processed fully electronically. This migration would *remove* the natural segmentation of traditional activities. In the case of a pub, if additional information was disclosed, say through a national ID card, malicious staff could steal this information, or this information can be abused in other ways. As a consequence, the damage that identity thieves can cause would no longer be confined to narrow domains, nor would identity thieves be impaired any longer by the inherent slowdowns of today's non-electronic identification infrastructure. Furthermore, service providers and other parties would be able to electronically *profile* individuals *across multiple activities* on the basis of the universal electronic identifiers that would inescapably be disclosed when individuals interact with service providers.

Ironically, the currently envisioned ID card architecture therefore has severe implications for the security and autonomy of service providers. When the same universal electronic identifiers are relied on by a number of autonomous service providers in different domains, the security and privacy threats for the service providers no longer come only from eavesdroppers and other traditional outsiders. A rogue system administrator, a hacker, a virus, or an identity thief with insider status would be able to cause massive damage to service providers, could electronically monitor the identities and visiting times of all clients of service providers, and could impersonate and falsely deny access to the clients of service providers.

In sum, the national ID system as currently envisioned by government poses threats to the privacy of UK citizens as well as to the autonomy and security of service providers. While the card may well be acceptable for the internal needs of businesses that engage in employee-related identity management within their own branches, the privacy and security risks of adopting the card as a national ID card for citizens would be high.

[146] As an example, although we register our next of kin for emergency purposes under many circumstances, it is not the responsibility of a sports club to verify that this person is in fact kin, nor to verify if the contact details that we have given are accurate, by checking against a national registry.

A constructive way forward

Indeed, far less intrusive means exist for achieving the publicly stated objectives of the UK national ID card. Over the course of the past two decades, the cryptographic research community has developed an array of entirely practical privacy-preserving technologies that can readily be used to design a better national ID card. The system would not need to be centralised, could build on existing societal relationships, to better ensure for security and privacy.

Technologies such as digital credentials, privacy-friendly blacklist screening, minimal disclosure proofs, zero-knowledge proofs, secret sharing, and private information retrieval can be used as building blocks to design a national ID card that would simultaneously address the security needs of government and the legitimate privacy and security needs of individuals and service providers. The resulting ID card would minimise the scope for identity theft and insider attacks. A Federated solution would also better model and suit existing relationships, whilst ensuring for proportionate data practices.

These solutions are well known to the private sector, but are rarely sought out when Government endeavour to develop national identification systems. The reasons for Government reluctance to consider these technologies are many. One reason includes the poor design principles behind national ID cards, always perceived as large projects that enable only the full flow of information, rather than the proportionate flow of information. Another significant reason may be because these alternative authentication systems empower individuals to control the amount of information that is disclosed.

If the Government wishes to improve identification in general throughout British society, it needs to consider all the relationships involving the citizen. Rather the Government is proposing a system that will supersede all other relationships and current identification techniques. This is acceptable as long as the National ID is designed to allow proportionality and adaptability to local conditions. The current policy does not do this, even though the technology does exist.

Notably, proper use of privacy-preserving techniques would allow individuals to be represented in their interactions with service providers by local electronic identifiers that service providers can electronically link up to any legacy identity-related information they hold on individuals. These local electronic identifiers within themselves are untraceable and unlinkable, and so today's segmentation of activity domains would be fully preserved. At the same time, certification authorities could securely embed into all of an individual's local identifiers a unique "master identifier." This embedded master identifier would remain unconditionally hidden when individual authenticate themselves in different activity domains, but its presence can be leveraged by service providers for security and data sharing purposes – without causing any privacy problems.

Designing such systems is possible, but the proposed scheme aims only to increase the links to and from, and enable the full flow of information across, sectors and other boundaries.

In Federated Identity systems, there are pluralities of Credential Providers (public and private sector) who issue cryptographic security tokens for representing identity in some limited domain, or linked set of domains. The credentials can be designed to be permit records of transactions to be either linkable or unlinkable, or some spectrum of properties between with two. For example, it is possible for identifiers to:

- be bi-directional or unidirectional, so that multiple identities can be traced from one domain to another, but not in the reverse direction;
- for facts ("attribute values") to be asserted and trusted without disclosing a specific identity;
- for separate identities to be selectively united, either under the control of the individual or another party;
- for infringement of rules to be penalised by disclosure of identity if and only if infringement occurs.
-

Also, embedded master identifiers could be blacklisted across multiple segmented activity domains to ensure that fraudsters in one domain can be denied access to services in other domains, while preserving the privacy of honest individuals. Similarly, service providers would be able to securely share identity assertions across unlinkable activity domains by directing these assertions in digitally protected form through the ID cards of their data subjects in a privacy-friendly manner.

There is thus ample scope for designing identity systems for e-government with rules that can be specifically tailored to intentionally isolated domains of health entitlement and patient records, taxation and benefit claims, border-control and travel, and inter-operation with private sector systems. The rules of each system would constitute the procedure for Data Protection compliance, and could allow good governance of data-sharing for legitimate public policy reasons, whilst limiting infringements of privacy to the minimum necessarily required by ECHR Article 8.

Such flexibility does not of itself answer difficult questions about how much data-sharing and non-consented identification is justifiable in a democratic society conformant with human rights. However adopting such a fine-grained system allows the processes of democratic legislation and oversight many more options than a monolithic identity system predicated on a unique and ubiquitously traceable identity for each individual. Monolithic systems have much poorer resilience and scaling, and offer nugatory privacy, security, and reliability protection in comparison to Federated ID.

The practice of illicitly loaning Federated ID credentials to other people is discouraged by the fact that those to whom a credential is loaned can damage the owner's reputation, incur liabilities in that domain and learn personal information.

Nevertheless, biometrics may be necessary for applications requiring a high degree of identification (such as travel and border-control). A local-biometric card scheme could be devised which checked for duplicate IDs in a compartmentalised way.

Simplifying the cryptographic details, the card could present a biometric template encrypted with a different key specific to the NHS, Asylum/Immigration etc., in such a way that duplicate (encrypted) biometric identities could be detected and traced within a

limited domain (e.g. an international border-control system), but ad-hoc data-matching across domains could not occur unless designed and authorised.

Therefore, the oft made observation that the jurisprudence of ECHR plainly allows national identity cards, must be reconsidered when contemplating a system based on a general purpose central biometric database and a monolithic unique identity facilitating arbitrary infringement of Article 8. The impact of all previous identity card systems has been miniscule in comparison to the potential deleterious impact on privacy of the scheme proposed.

Is there a "pressing social need" for a general purpose central biometric database, if the interests of national security, the prevention or detection of crime, the enforcement of immigration controls, prohibitions on unauthorised working or employment, and efficient and effective provision of public services can all be accomplished with Federated Identity systems, and biometrics compartmentalised to specific domains, physically stored only in tamper-resistant devices, and matched with offline biometric readers?

It is illegal, not "sensible", to create a single electronic internal passport just because there is an international imperative to introduce biometrics into border-control systems. It is technologically unremarkable to design an international travel and immigration biometric system, which links to other sector-specific identity systems only to an extent which is foreseeable, explicitly legislated, enforceable, and compliant with European Convention rights.

The French E-Government Strategic Plan

The French Minister for State Reform is overseeing the implementation of a strategic plan to provide services to citizens, the private sector, and the public sector supported by e-government initiatives.[147] The plans emphasises the need for user-friendly and accessible solutions that create a climate of trust.

In their plan to enhance e-government, the French national plan aims for a user-oriented system, allowing for multiple forms of identification. The emphasis is on simplicity and proportionality. The amount of information collected will be minimised to increase the confidence of users. The French Government acknowledges that e-government gives rise to two contradictory requirements:

- simplifying registration and personal data management for the users would entail breaking down the barriers between government departments, making exchanges flow more smoothly without the user being systematically asked repeatedly for documents, for example, which he has already supplied;
- upholding the protection of personal data, which may in fact restrict the interconnections between government departments.

The French Government is clear on how to resolve this conflict.

[147] The French E-Government Strategic Plan (PSAE) 2004-2007, http://www.adae.gouv.fr/IMG/rtf/Le_plan_strategique-GB.rtf.

> Government guidelines are clear: do not authorise uncontrolled generalised exchanges between departments. However, the development of e-government must grant citizens more transparency in the monitoring of their administrative papers and better control of their personal details (confidentiality, right to access and correct data regarding them).[148]

To enable this, the Government intends to provide tools and services "which will enable [citizens and professionals] to exercise their rights more simply and completely." These tools and services include the:

Decentralised Storage of data

The French Government is aware that there are several options available, including centralising all the data of every user, but notes that, "This solution is not implemented in any country, for obvious reasons of individual freedoms and near technical impossibility." The French Government proposes instead that all data will remain decentralised within each department.

Distributed Identifiers

The French strategy acknowledges that the easiest solution would be to call for a unique universal identifier for all citizens, but the French designers have foremost in mind that privacy law was created to prevent a situation such as this. They further note that the Germans consider such an approach to be an unconstitutional practice. The French Government position states,

> It should be remembered that, with regard to e-government, the State must take a stance as guarantor (of individual freedoms, the authenticity and enforceability of dematerialised procedures and actions, the security of actions carried out by public servants, etc.) and the Government wishes to confirm this position clearly both in the formulation of the decisions taken and in their methods of application.

As a result, French authorities do not see the need for anything more than sectoral identifiers to preserve rights. They also admit that a solution such as the national registry in the UK that would include a listing of all relevant identifiers "would probably not go down too well in our country"[149]. Instead the French Government calls for the creation of an 'identity federator':

> the most successful solution consists of creating an identity federator, enabling the user to use the single identifier to access each of the services of his or her choice without either the government databases or the identity federator itself being able to make the link between the different identifiers.

Further proposals include an on-line environment where the user can verify all the usage of her personal information, and give consent if information needs to be shared between

[148] Ibid, page 13.
[149] Ibid, page 15.

departments. At the same time, the French Government wishes to preserve the ability of users to not identify themselves to government departments.

The French Government has chosen to follow a proportionate path to identification and data management. Their systems will, at a technological level, be less complicated, and will be more resilient to attack and failures. The Government sees the benefits of e-government, but understands and resists the temptation to coalesce or link all personal information held by government departments. In order to ensure user trust and adaptability of current and future systems there will therefore be no central registry, no single identifier, nor a centralised list of identifiers.

Conclusion

In the context of a national ID card infrastructure, security and privacy are *not* opposites but, assuming that proper privacy-preserving technologies are deployed, are *mutually reinforcing*. In order to move forward constructively with a national ID card, it is important for government to investigate technological alternatives that hold the promise of *multi-party* security while *preserving* privacy.

Not only will this approach preserve privacy, but it will also protect the existing relationships in society. It will ensure that the rail company knows what it needs to know for granting special prices to students; that sports clubs know the required information for membership purposes; and the NHS has sufficient information to authenticate patients; without unnecessarily binding these relationships with additional needless information. This approach will also diminish the potential for the amassing and sharing of information that is unnecessary and disproportionate.

Appendix One: Comparison with the HAC findings

We have found it useful to assess our findings by comparing each to the conclusions in the report of the Home Affairs Committee. While the HAC report dealt primarily with the draft legislation, nearly all circumstances are identical to those created by the final legislation introduced in November 2004.

Of the 91 conclusions drawn by the HAC, 52 were supported by this report, 27 were conditionally supported and 6 were considered to have no basis that could be determined through research. 6 were not relevant to the study.

H.A.C. report	L.S.E. report
The international context	
1. While we can understand why the Government has proposed a combined passport and identity card, we regret that no analysis has been published of the costs and benefits of a free-standing identity card. (Paragraph 20)	Supported by research. There are strong grounds on the basis of law, practicality and technology to argue the case for keeping the two documents distinct and separate.
2. We consider in detail later in this report the concerns raised in the United Kingdom over the Government's proposals. The international experience clearly indicates that identity cards and population registers operate with public support and without significant problems in many liberal, democratic countries. In a number of these, the holding and even carrying of the card is compulsory and appears to be widely accepted. However, each country has its own social, political and legal culture and history: the nature of each identity scheme and population register reflects those unique elements. We cannot assume that any particular approach can be applied successfully in the UK. Nor can we yet draw on any significant international experience of the use of biometrics on the scale that is proposed in the UK. (Paragraph 38)	Conditionally supported. While there is little public resistance to identity systems in most countries nothing approximating the scale and complexity of the UK scheme has been undertaken elsewhere. There are numerous examples of hostile public responses following proposals to use this scale of personal information in a range of identity and database applications.
Concerns of principle	
3. An identity card scheme of the sort and on the scale proposed by the Government would undoubtedly represent a significant change in the relationship between the state and the individual in this country. International experience does not suggest that objections of principle are overwhelming, although the development of a biometric-based scheme does introduce new elements that have not been tested elsewhere. We do not, however, believe that an identity card scheme should be rejected on constitutional grounds alone. (Paragraph 59)	Conditionally supported. There is general agreement among key stakeholder groups that the proposals represent a fundamental change in the relationship between the individual and the state. Unless appropriate and necessary safeguards and guarantees can be built into the system it is entirely reasonable to consider rejecting the scheme solely on constitutional grounds.
4. The test should be whether the measures needed to install and operate an effective identity card	Conditionally supported. While proportionality is a key consideration in the development of the

system are proportionate to the benefits such a system would bring and to the problems to be tackled and whether such a scheme is the most effective means of doing so. (Paragraph 60)	scheme, such arguments should not override legal rights and guarantees.
Practical concerns	
5. The proposed system is unprecedentedly large and complex. It will contain sensitive personal information on tens of millions of individuals. Any failure will significantly affect the functioning of public and private services and personal and national security. Measures to ensure the integrity of the design, implementation and operation of the system must be built in to every aspect of its development. As we will remark at a number of points throughout this report, the Government's lack of clarity about the scope and practical operation of the scheme, and the nature of the procurement process, does not give us confidence that this will be achieved. (Paragraph 64)	Supported by research. The study agrees with this conclusion in its entirety.
Benefits and weaknesses of the Government's scheme	
6. It is reasonable for the Government to have refined the aims of its scheme after a consultation exercise and development of proposals for its implementation. It has now set out its reasons for introducing identity cards, in its most recent document, *Legislation on Identity Cards: A Consultation*, which accompanied the publication of the draft Bill. (Paragraph 70)	Conditionally supported. The aims of the scheme are broad and non-specific (see section 7 & 8 below). The consultation exercise undertaken by the government was perceived widely to be largely ineffective in facilitating national debate.
7. However, many elements of the design of an identity card scheme, from the national register, to the design of the card and to its operational use, depend greatly on the precise purpose for which it is designed. Although some core functions are consistent and clear, the changing aims of the scheme do not give total confidence that the Government has arrived at a complete set of clear and settled aims for the card. The Government has not yet clarified how it intends to deal with some elements of the original proposals for entitlement cards, such as which services should be linked to the card and whether there should be unique personal numbers across public services. We consider these issues further below, but it is clear that they are central to the functioning of the scheme. (Paragraph 71)	Supported by research.
8. The draft Bill might have been expected to clarify the Government's aims but we do not believe it has done so. It is essential that the Government explain its intentions on issues raised in this report before the Bill is published. (Paragraph 72)	Supported by research.
Illegal working and immigration abuse	
9. Identity cards could make it easier for those seeking work to demonstrate their right to do so, and, by the same token, make it easier for the police to show that a company employing illegal labour had done so knowingly. (Paragraph 79)	Not supported by research. Many individuals, because of a variety of personal or technical circumstances, may be denied the right to work.
10. We believe that identity cards can make a significant contribution to tackling illegal working. However this will need to be as part of wider	Conditionally supported. While a successful outcome will depend on a package of measures, risk assessment has not been undertaken to assess

enforcement measures, including action against culpable employers. We repeat our recommendations that the Government should target employers who deliberately break the law and that the Proceeds of Crime Act should also be used to seize profits made from the employment of illegal labour. We welcome the steps the Government has taken so far, but to be fully effective there must be properly resourced enforcement of existing regulations. (Paragraph 80)	whether illegal working could become entrenched, more invisible or more extensive.
11. The Government must clarify what action will be expected from the employer, including whether presentation of the card by a job applicant is enough or whether an employer would have to check the biometrics or the authenticity of the card. If so, the Government needs to be clear how often this will be required and what access to biometric readers or the National Identity Register will be available to employers or other agencies. (Paragraph 81)	Supported by research.
12. We are concerned that the three-month period for EU nationals, or those claiming to be such, might constitute a significant loophole: it is difficult to see what would stop someone moving from job to job on false papers. The Government must bring forward proposals to deal with this loophole, as well as making a substantial commitment to robust enforcement of laws against illegal working. (Paragraph 82)	Supported by research. At its most extreme point this situation has the potential to substantially undermine key benefits that could flow from the scheme and has an even greater potential to undermine public trust in the system.
13. It is also clear that the integrity of the UK system will be dependent on the integrity of the passport, asylum and visa regimes in other EU countries. In our visit to Germany we were told of a pilot scheme involving biometrics to prevent fraudulent asylum and visa applications. The Minister of State has set out the UK's involvement in similar schemes. As part of the development of the identity card scheme, the Government should report regularly to Parliament on progress being made across the EU to tackle any weaknesses in other EU countries, and, in particular, those countries currently judged to be the least secure. (Paragraph 83)	Supported by research.
14. We conclude that identity cards, by reducing the "pull factor" from work, and public services, could make a contribution to preventing illegal immigration, but only if the scheme is properly enforced and complemented by action on access to public services. (Paragraph 84)	Conditionally supported. A comprehensive risk assessment is required.
Organised crime and terrorism	
15. We understand that the contribution to fighting terrorism would be the ability to disrupt the use of multiple identity, identity fraud and related activities like money-laundering, and illegal migration by terrorists and their networks. While, of course, not all terrorists make use of activities based on false identities, and some will have legitimate national or international identity documents, we believe that effective action on identity would be a real and important contribution to restricting the	Not supported by research. This reasoning appears to have little foundation in evidence. Research should be undertaken before reaching conclusions on these questions.

ease with which terrorists can operate. (Paragraph 94)	
16. We note, however, the real benefits of an identity card in fighting serious crime and terrorism are only likely to be achieved with a compulsory scheme covering all citizens and residents. It will also be dependent on the effective use of the scheme to check identities, an issue we discuss in the next sections. (Paragraph 95)	Not supported by research. This conclusion is, again, assumed without much factual basis. More detailed research is required.
Identity fraud	
17. We believe there is a danger that in many day-to-day situations the presentation alone of an identity card will be assumed to prove the identity of the holder without the card itself or the biometrics being checked, thus making possession of a stolen or forged identity card an easier way to carry out identity fraud than is currently the case. The availability of readers of cards and biometrics, including to the private sector, is therefore a crucial factor. (Paragraph 99)	Conditionally supported. The outcome would depend largely on the extent of biometric spoofing techniques. The widespread availability of biometric readers in an environment of widespread spoofing would magnify the extent of identity theft.
18. We think it would be likely that identity cards would help combat identity fraud, but only as part of a wider package of measures. The Government should be clearer both about how and when it expects the card and biometrics to be checked and about what levels of security are appropriate in different circumstances. (Paragraph 100)	Conditionally supported. See 17 above.
Entitlement to public services	
19. Identity cards would make it easier to establish entitlement to public services. However the Government should take action now to ensure that measures to check identity are developed across public services prior to the introduction of the new card. (Paragraph 107)	Supported by research.
20. The Government should also review entitlements to public services across the board with the aim of rationalising and standardising them, since there does not appear to be a consistent set of principles underlining access to government services. (Paragraph 108)	Conditionally supported. Standardisation of access to public services should not preclude organisations from evolving unique authentication measures suited to their individual circumstances.
21. The existence within the United Kingdom of up to four different systems for checking entitlement to public services will be a possible cause of confusion, particularly where cross-border services are provided. The UK Government should liaise closely with the devolved administrations on these issues, both to avoid confusion and to learn from the experiences of the devolved administrations' own entitlement cards. (Paragraph 112)	Conditionally supported. See 20 above.
Easier access to public services	
22. The Government's current proposals would improve access to public services to the extent to which this depends on identification. It is important to ensure that the convenience to the state of having a comprehensive system of identifying individuals and accessing data about them is accompanied by an increase in convenience to the individual. The benefit must not be entirely, or even predominantly, to the state. (Paragraph 118)	Supported by research.

23. The Government has not developed coherent proposals for using the identity card in other ways to improve access to a wider range of services and information or to promote greater coherence across public services. As a result, citizens are still likely to be required to carry a wide range of cards and documents to use many local and national, public and private services. We believe that this is a missed opportunity. (Paragraph 119)	Supported by research.
Key issues	
24. We note that at the moment there is very little clarity about the level and nature of checks that will be required and carried out, even though this is fundamental to the whole scheme. We recommend that the Government should provide estimates of the proportion of checks that would be biometric and therefore highest security. (Paragraph 125)	Supported by research.
25. It is not clear that Government departments have identified how the operation of their services, or entitlement to them, need to be changed to make best use of an identity card system. (Paragraph 126)	Supported by research.
26. In most cases, identity cards will only be fully effective if complementary enforcement action can be taken. (Paragraph 127)	Supported by research.
27. Finally, more could be done to check identities today and there is a danger that action will be delayed pending the introduction of an identity card. (Paragraph 128)	Conditionally supported. A full risk and opportunity assessment is required.
Public support	
28. It may be that citizens will choose to use identity cards voluntarily on an extensive basis. However, until identity cards are compulsory there should be realistic alternatives to their use in every case. There should also be effective restrictions on inappropriate demands for them. (Paragraph 133)	Supported by research.
The 'voluntary' stage	
29. Given the Government's decision to base identity cards on passports and driving licences, we believe the incremental approach to introduction is justified. We set out our concerns about the implications of this choice in paragraphs 19-20 above. (Paragraph 138)	Conditionally supported. See 1 above.
Vulnerable groups	
30. The effect of the identity card scheme on minorities, such as the elderly, the socially excluded and ethnic groups, is of the utmost importance. The Government should ensure that the scheme imposes no new disadvantages on these groups, and do so before it is implemented. (Paragraph 141)	Supported by research.
The National Identity Register	
31. We do not ourselves have the expertise to make judgements on the technical issues involved in setting up a national identity card system, but we have been struck by witnesses' insistence on the importance of the Government getting the structure right from the beginning and sticking to its decisions. We are concerned that the Government's approach has not taken into account the need to ensure adequate technical debate and public scrutiny	Supported by research.

of the design of the system. (Paragraph 144)	
Architecture of the database	
32. The structure of the database, and how to set it up and manage it, are among the most important choices the Government has to make. We are greatly concerned that the Government's procurement process appears to be taking these key decisions without any external reference or technical assessment, or broader public debate. We recommend the Government publishes details of consultations with any external bodies and also any technical assessments that have been undertaken. (Paragraph 147)	Supported by research.
Access to the database	
33. A balance needs to be struck between, on the one hand, protecting individuals from unnecessary access by public and private bodies to information held on them and, on the other, ensuring that users of the database have the information they need for the scheme to fulfil its purposes. Above all, it is important that the public should know who may be able to see information about them, and what that information is. (Paragraph 151)	Supported by research.
'Function creep'	
34. Whatever the merits or otherwise of such developments [eg. the establishment of a national fingerprint register], their potential should be recognised. It is essential that they do not develop incrementally or by executive action but are subject to full Parliamentary scrutiny. These issues are at least as significant as the decision to make cards compulsory. (Paragraph 158)	Supported by research.
35. In a similar way, identity cards are not planned to be a single card for all public services, but it clearly is possible, and perhaps desirable, for a successful identity card scheme to develop in this direction. But this should be a decision of Parliament, not of the executive. (Paragraph 159)	Supported by research.
Information on the database	
36. The functions of the Register entail establishing an individual's identity in a number of different circumstances. For some of these, such as interaction with local authorities, addresses may be necessary. There is therefore a case for including them in the National Identity Register. But to do so would have significant administrative and operational consequences, since the Register would need to be updated frequently; the extra work could lead to mistakes which would be disastrous if not properly handled. The Government should be more explicit about the case for including addresses and demonstrate that the advantages of doing so outweigh the problems that would be created. The Government should also clarify whether addresses would be only on the Register or whether they would be legible on the surface of the card itself. (Paragraph 163)	Conditionally supported. While there may be a justification for the requirement to provide or store addresses, the case for inclusion of this data on the national register has not been clearly established. Using the national identity registration number to link to other databases may be a more secure and cost effective option.
37. In many parts of Europe, including Sweden and Germany, where there is a requirement to register	Not supported by research. This requirement would create a range of additional security and

addresses, it is a legal requirement for landlords to register their tenants. We recommend that this be adopted if the Government decides to include addresses, since it would help alleviate the problem of frequent changes of address. (Paragraph 164)	administrative issues. Tenants would be required to disclose their identity card to landlords, and in the event of loss or failure of the card, may be denied housing.
38. The nature of the individual number and its relationship to other identifying numbers used by the state are more decisions that are crucial for the design and development of the system. The Government must be clear and open about the issues involved and enable informed parliamentary and public scrutiny of any decisions (Paragraph 167)	Supported by research.
Biometrics	
39. The security and reliability of biometrics are at the heart of the Government's case for their proposals. We note that no comparable system of this size has been introduced anywhere in the world. The system proposed would therefore be breaking new ground. It is essential that, before the system is given final approval, there should be exhaustive testing of the reliability and security of the biometrics chosen, and that the results of those tests should be made available to expert independent scrutiny, perhaps led by the Government's Chief Scientific Adviser. (Paragraph 175)	Supported by research.
Medical information	
40. We agree with the BMA: it would not be either useful or appropriate to keep medical details on the Register. But it would be sensible for the identity card to be the mechanism that enables individuals to access their NHS records. (Paragraph 176)	Conditionally supported. Risk assessment required.
The Citizen Information Project and other Government databases	
41. We doubt that the Citizen Information Project will provide "a strong and trusted legal basis for holding personal contact information" if the information on it has to be confirmed by another, separate identity card Register. There is a very large degree of overlap between the Citizen Information Project and the National Identity Register. The Registrar General mentioned the options of "comprehensive legislation to oversee information matching which in itself was conducted by individual agencies but which improves the quality of individual registers without actually going to the next step of creating a register" and of "common standards for register management in the British government": each of these would be more worthwhile than the Citizen Information Project as it is currently planned. (Paragraph 185)	Not applicable to this study.
42. We are concerned by the proliferation of large-scale databases and card systems, since we have seen little to suggest that they are being approached in a co-ordinated way. While we have not taken detailed evidence on current proposals, other than the Citizen Information Project, we have the impression that each government department is continuing with its own project in the hope that it is not going to be significantly affected by other projects. The format of registration on different	Conditionally supported. While this concept may have merit at a fiscal level, it also goes a considerable way to violating the principle of Functional Separation, which provides privacy protections for individuals as well as creating safeguards to prevent full centralisation and control of personal information.

databases should be coherent and consistent. (Paragraph 186)	
43. We believe that the Government must tackle this proliferation of databases, examining in each case whether the number, identifier or database is needed, what its relationship is to other existing or planned databases, how data will be shared or verified and other relevant issues. For this action to be effective, it must be co-ordinated at the highest levels of the Civil Service. (Paragraph 187)	Conditionally supported. See 42 above.
44. We do not think that there should be a central database with all information available to the Government on it. But an identity card should enable access to all Government databases, so that there would be no need for more than one government-issued card. (Paragraph 188)	Conditionally supported. See 42 above.
Registration and enrolment	
45. The integrity of the enrolment and registration processes are central to both the smooth running of the system and to its security. Without data of investigative or evidential quality, few of the objectives of the scheme can be achieved. Issues the Government must consider include: the number of mobile units to enrol the housebound, the elderly and those in remote locations; how sensitive the equipment is to the environment; the training of personnel; and the need to minimise opportunities for corruption and fraud. More study of these aspects is needed. (Paragraph 193)	Supported by research.
Cards	
46. The type of card to be used is a decision of the same order of importance as the architecture of the database, since it has consequences for issues such as how the card will be used and the number of readers and the infrastructure needed, both of which have significant implications for costs. Some choices, such as the nature of the chip, seem to follow a decision to use the passport as an identity card (and therefore follow ICAO) rather than any independent assessment of what would be most appropriate for an identity card. We are concerned that the Home Office appears to be taking these key decisions without any external reference, technical assessment or public debate. (Paragraph 197)	Supported by research.
47. The Government's figures on how much cards would cost compare them to 10-year passports and driving licences. The Government has not, however, confirmed explicitly how long the validity of identity cards would be. It must do so before the Bill is published. (Paragraph 198)	Conditionally supported. Because of the inclusion of biometric data, the validity period of the cards may vary according to individual circumstance.
Readers and infrastructure	
48. We are deeply concerned that the Government has published so little information about the number, type, distribution and cost of card readers and the infrastructure necessary to support this. This information is not only essential to proper costing of the scheme, but also to an assessment of how effective the scheme will be. (Paragraph 201)	Supported by research.
49. We are also concerned that the Home Office	Supported by research.

may be leaving it to other government departments, local government and the private sector to decide what level of investment to make in card readers and infrastructure. There is an obvious danger that each organisation will opt for a low level of security, relying on others to raise the level of security in the system as a whole. If this happens the value of the identity card system will be significantly undermined. We also expect the Home Office and other Departments to give at least broad estimates of the numbers of readers they expect to need of each type and what level of provision other organisations are expected to make. (Paragraph 202)	
Multiple cards	
50. We support the issue of multiple identity cards to an individual in cases where there is a legitimate need, and welcome the Home Office's expression of flexibility on this issue. (Paragraph 203)	Supported by research.
Security	
51. We believe that an identity card system could be created to a sufficient level of security. We stress, however, that the security of the system depends as much on using the proper procedures with the appropriate level of scrutiny to verify the card in use as it does on the integrity of the card issuing process or the identity register. (Paragraph 207)	Conditionally supported. This conclusion cannot be drawn until agreement has been reached on a specific architecture.
Costings	
52. The Home Office have provided us with details of the assumptions on which their costings have been based, on a confidential basis. We are not convinced that the level of confidentiality applied is justified. Cost information is an essential element in determining the value for money of any project. It is of prime importance where expenditure is funded from the public purse and of particular relevance with regard to public sector IT projects which have a history of poor performance and cost-overruns. We are also concerned that the least robust cost estimates appear to relate to the assumptions with the greatest cost-sensitivity, such as the length of enrolment time, the anticipated number of applications requiring further investigation, the cost of card production and the criteria for subsidised cards. Changes to any one of these factors could cause significant increases to the cost of the programme. (Paragraph 212)	Supported by research.
53. The failure to attach a Regulatory Impact Assessment to the draft Bill, or to provide any detailed information on estimated costs and benefits, significantly weakens the basis for pre-legislative scrutiny and the public consultation exercise. This secrecy is all the more regrettable since the case for an identity card system is founded on whether its benefits are proportionate to the problems it seeks to address: a proper cost-benefit analysis is an indispensable element of this. The excuse of commercial sensitivity should not be used to avoid publishing a full Regulatory Impact	Supported by research.

Assessment with the Bill. (Paragraph 213)	
Procurement	
54. We welcome the Home Office's efforts to overcome their record on IT procurement. We do not believe that it is impossible for them to deliver the project on time, to specification and to cost. (Paragraph 215)	Not supported by research. This conclusion appears to be entirely speculative.
55. But we are concerned about the closed nature of the procurement process which allows little public or technical discussion of the design of the system or the costings involved. We do not believe that issues of commercial confidentiality justify this approach. Any potential gains from competing providers providing innovative design solutions are likely to be more than offset by the unanticipated problems that will arise from designs that have not been subject to technical and peer scrutiny. (Paragraph 216)	Supported by research.
56. Nor do we believe that the Government's OGC Gateway process has yet demonstrated the robust track record on procurement projects that would allow it to be relied upon for a project of this scale. (Paragraph 217)	Supported by research.
57. The Home Office must develop an open procurement policy, on the basis of system and card specifications that are publicly assessed and agreed. The Home Office should also seek to minimise risk, including, as appropriate, by breaking the procurement process down into manageable sections. We have already recommended that the Chief Scientific Officer be invited to oversee the development of the biometric elements of the scheme. We recommend that individuals or groups with similar expertise be invited to advise on the scrutiny of other aspects of the scheme. (Paragraph 218)	Supported by research.
Conclusions	
58. Identity cards should not be ruled out on grounds of principle alone: the question is whether they are proportionate to the aims they are intended to achieve. Identity cards could make a significant impact on a range of problems, and could benefit individuals through enabling easier use of a range of public services. This justifies, in principle, the introduction of the Government's scheme. But the Government's proposals are poorly thought out in key respects: in relation to the card itself, to procurement and to the relationship of the proposals to other aspects of government, including the provision of public services. These issues must be addressed if the proposals are to be taken forward. It is important that the Government clarifies the purposes of the scheme and makes them clear through legislation. (Paragraph 219)	Conditionally supported. See 4 above.
The draft Bill	
59. The draft Bill gives the Government powers to require and register a wide range of information not obviously needed to establish identity. It gives a wide range of organisations access to that	Supported by research.

information and to the audit record of when and by whom the National Identity Register has been accessed, so giving information on key actions of individuals. While the draft Bill undoubtedly enables these actions to be taken in the fight against serious crime or terrorism, it allows for far wider access to the database than this justifies. In particular, given the lack of clarity about the aims of the identity card, to leave so much to secondary legislation is unacceptable. (Paragraph 222)	
60. It is unacceptable that basic questions about the degree of access to the National Identity Register should be left to secondary legislation. The Government must clarify what access will be given to public and private sector bodies, and under what circumstances. Once identity cards are compulsory, there is a significant danger that the concept of consent to disclosure of information will in practice be eroded, unless there are clear statutory safeguards against improper access to the Register. (Paragraph 224)	Supported by research.
61. We note that whilst a range of data might be required to verify an application, it is not necessary for all that data to be retained on the National Identity Register. They could either be returned or, if necessary for audit purposes, held on a separate database. The Bill should be amended to restrict data held on the register to that information required to establish identity once the card has been issued. (Paragraph 229)	Supported by research.
62. The one exception would be information about immigration status. This is so central to the justification for the Bill that it would be useful and convenient to hold this on the central register. (Paragraph 230)	Not applicable to this study.
63. The purposes of the draft Bill as set out in Clause 1 are very broad and the list of registrable facts is longer than those the Home Office has said are necessary to establish identity. Both the purposes of the Bill and the registrable facts should be strictly limited to establishing identity and immigration status, so as to ensure that the provisions of the Data Protection Act cover the operation of the scheme effectively. (Paragraph 231)	Supported by research.
64. It is not yet possible to be more precise about the list of registrable facts, because the aims of the scheme, and hence the requirements for information to be registered, are not sufficiently clear. As the Bill proceeds, the Government must set out its justification better. (Paragraph 232)	Supported by research.
65. Clause 1 should set out the aims of the scheme. A possible formulation might be: "to enable an individual to identify himself in order to gain access to public and private services or when required to identify himself for the purposes of law enforcement". Wording of this sort would establish a test against which the data to be stored and used could be tested. It would also guard against the type	Supported by research.

of function creep in which the state uses the register to identify individuals without amendment by Parliament. (Paragraph 233)	
66. There should be explicit provision in the Bill that all access to the register must be recorded. (Paragraph 234)	Conditionally supported. See Appendix detailing concerns about the audit trail.
67. We support the provisions in Clauses 2(4) and 8(4) that enable registration of failed asylum seekers and other similar cases, but recommend that the Home Office clarify the purposes of these Clauses in the Bill. (Paragraph 235)	Not applicable to this study.
68. Clause 3 provides an acceptable mechanism for amending the information required to be held on the Register, but only if the statutory purposes of the Bill are clarified as we recommend. (Paragraph 237)	Conditionally supported. The desirability of having a national Register of data has not been comprehensively assessed.
69. It is practical to allow some flexibility over precisely which documents are required at registration and that these should be set out in secondary legislation. But the Bill should state that only those documents that are reasonably necessary to establish identity may be required. There should be a right of appeal to the National Identity Scheme Commissioner. (Paragraph 239)	Supported by research.
70. The proposed penalties [for failing to register when required to do so and for failing to provide information] are reasonable given their purposes and existing penalties for similar offences. (Paragraph 244)	Not supported by research. The conditions established through the development of a comprehensive identity card system cannot readily be compared with those of other mechanisms.
71. It is unlikely that if full Parliamentary procedures were followed the Government would, as it fears, be accused of "proceeding by stealth". The move to compulsion is a step of such importance that it should only be taken after the scrutiny afforded by primary legislation: the proposed "super-affirmative procedure" is not adequate. We would, however, support the inclusion in the Bill of powers to enable the Government both to set a target date for the introduction of compulsion and, if necessary, to require agencies and other bodies to prepare for that date.	Supported by research.
72. The Government should consider statutory provisions to ensure the integrity of the registration and enrolment system, as well as specific penalties for breaches of these provisions. (Paragraph 250)	Supported by research.
73. It is reasonable to require individuals to report relevant changes in their circumstances, provided that the range of information they are required to update is not excessive and that they are able to check that the information held on them is accurate. We do not believe that there should be charges for updating information on the Register, since this would be likely to affect adversely the accuracy of the information held. (Paragraph 253)	Conditionally supported. This matter also involves the question of necessity. Further consultation is required to assess whether, for example, only resident and immigration status changes are required to be notified.
74. We find it anomalous that failure to update a driving licence should be a criminal offence, especially when failure to update the National Identity Register will not, and we note that the Home Office does not know how many prosecutions there have been for failing to update a	Supported by research.

driving licence. This offence should be reviewed in the light of the proposed legislation on identity cards. (Paragraph 254)	
75. Clause 11(1) could have significant implications for past and current employers, neighbours, landlords, family members and past spouses, all of whom might be required to assist in the identification of an individual. The Government should clarify the scope and limits of this clause on the face of the Bill. (Paragraph 255)	Supported by research.
76. The practical application of Clauses 11 and 12 to socially excluded groups must be clarified as soon as possible. This should be done in such a way as to ensure that such groups are no further disadvantaged by the operation of the scheme. The Bill should contain legal duties on the Home Secretary to take into account special needs, such as health, in applying these clauses; and to establish a clear legal status in the primary legislation for those of no fixed abode.	Supported by research.
77. We agree with the CRE that the Bill should be accompanied by a full Race Impact Assessment and that there should be a further Assessment at the time of the move to compulsion. (Paragraph 257)	Supported by research.
78. A reasonableness defence to the offences that might follow from Clause 13(1) should be included on the face of the Bill, rather than left to regulations. (Paragraph 258)	Supported by research.
79. The Bill should contain an explicit reaffirmation of the right of individuals to see both the data held on them and the audit trail of who has accessed those data and on what occasions, subject only to the national security and crime exemptions of the Data Protection Act. (Paragraph 259)	Supported by research.
80. It is reasonable that there should be the possibility of restricting releasable information in certain cases. We welcome the Home Office's readiness to consult on the issue. (Paragraph 260)	Conditionally supported. It might be considered that such a decision should be taken in each case by the Identity Cards Commissioner.
81. Earlier in this report, we referred to the different levels of security, from simple visual examination of the card to access to the National Identity Register, which the Home Office expects to be undertaken. Although it would not be possible to specify in detail all the circumstances in which different bodies might have access to the Register, we believe that the principle and tests of reasonableness should be placed on the face of the Bill. (Paragraph 261)	Conditionally supported. While a test of reasonableness is a valid limiting function governing access, a full risk assessment should be undertaken to determine whether specific access circumstances and organisations should be set out on the face of the Bill.
82. The Bill might also allow individuals to limit access to certain data under certain circumstances. For example, a citizen might choose that addresses could not be released to all those who access the Register. (Paragraph 262)	Supported by research.
83. We welcome the provisions of Clause 19 prohibiting any requirement to produce an identity card before the move to compulsion. (Paragraph 264)	Supported by Research.
84. We are not opposed in principle to access to the database and to the audit trail without the consent of	Conditionally supported. See Appendix on audit trails.

the individual concerned. But we are extremely concerned by the breadth of the provisions of Clauses 20 and 23 and particularly by Clause 20(2) which would allow nearly unfettered access to the security and intelligence agencies. At a minimum, disclosures without consent should be limited to cases of national security or the prevention or detection of serious crime. (Paragraph 269)	
85. It is not acceptable to have as broad a Clause as 20(5) simply because the Government is unclear about its objectives. (Paragraph 272)	Supported by research.
86. The Bill should have explicit data-sharing provisions to make clear the relationship between the National Identity Register and other official databases. Some of the proposed databases have no statutory basis—this is unacceptable and needs to be addressed in further legislation. (Paragraph 273)	Supported by research.
87. It is reasonable for the scheme to be operated by an Executive Agency similar to the DVLA or UK Passport Service. But we reject the argument that since their operations are not overseen by a Commissioner, neither should those of an identity card agency. We believe that because the identity card scheme would directly affect the daily lives of millions of people, and routinely involve sensitive and often highly personal information, oversight of its operation is utterly different to that of the DVLA or UK Passport Service. The National Identity Scheme Commissioner should report directly to Parliament. He or she should have powers of oversight covering the operation of the entire scheme, including access by law enforcement agencies and the security and intelligence services. (Paragraph 276)	Supported by research.
88. There are no provisions in Clause 27 to cover aiding and abetting the offences created, or conspiracy to commit them. It is possible that these can be dealt with through existing legislation, but we believe that it would be more sensible to cover them explicitly in the Bill. (Paragraph 277)	Not applicable to this study.
89. We welcome the Home Office's commitment to enabling complaints to be made about the operation of the scheme. The provisions to enable this must be effective, unbureaucratic and practical. (Paragraph 278)	Supported by research.
Overall conclusions	
90. We believe that an identity card scheme could make a significant contribution to achieving the aims set out for it by the Government, particularly tackling crime and terrorism. In principle, an identity card scheme could also play a useful role in improving the co-ordination of and the citizen's access to public services, although the Government has not yet put forward clear proposals to do so. We believe that the Government has made a convincing case for proceeding with the introduction of identity cards. (Paragraph 279)	Conditionally supported. The impact of an identity card on levels of crime and terrorism is largely unknown and conclusions in this area are speculative.
91. However, the introduction of identity cards carries clear risks, both for individuals and for the	Supported by research.

successful implementation of the scheme. We are concerned by the lack of clarity and definition on key elements of the scheme and its future operation and by the lack of openness in the procurement process. The lack of clarity and openness increases the risks of the project substantially. This is not justified and must be addressed if the scheme is to enjoy public confidence and to work and achieve its aims in practice. (Paragraph 280)	

Appendix Two: Biometrics, Public Opinion & the Public Trust

Based on the findings of "*Biometrics and Privacy:* A Study of Behaviours and Attitudes".[150]

Background

There indeed exists a dichotomy between individuals' stated attitudes towards privacy and their actual behaviours. Even while claiming to be concerned with protecting their privacy, individuals consistently sacrifice their privacy for seemingly minimal amounts of benefit. The inverse is also true, as those who say that they do not need privacy, also protect their personal information without thought. For those agents, such as businesses and government agencies, which demand and require information from individuals, understanding this disconnect between attitudes and behaviours is essential. The difficulty is differentiating between stated preferences and the way in which preferences for privacy are determined. This difference will affect individuals' actual demand for privacy.

The introduction of strong forms of authentication, such as biometric identifiers, highlights this problem. Individual perceptions of biometric technologies will be the result of the complex interplay between prior associations and the internal valuations of the costs and benefits. Those in the private and public sectors who hope to use biometrics to identify consumers and citizens need to understand this process in order to influence the demand for privacy.

In this section we analyse how biometrics affects the determinants of the demand for privacy and the implications of these effects for private and public sector implementation. Successful implementation of a biometric identity system is predicated on building trust relationships.

Our results point to two basic types of demand for privacy, *privacy-rational* demand and *privacy-myopic* demand.

Privacy-Rational Demand: The baseline demand for privacy by a longsighted individual. A *rational or longsighted* individual calculates costs and benefits of privacy over the long-term and takes advantage of and is aware of the full range of complex privacy-enhancing technologies. Longsighted demand is relatively inelastic.

Privacy-Myopic Demand: The demand for privacy by a myopic individual. A myopic individual is short-sighted and neither appropriately protects privacy nor understands the full costs and benefits of maintaining/sacrificing privacy. Myopic demand is relatively elastic.

[150] Conducted by the LSE in association with EDS. The authors of the report are Jeegar Kakkad, Ariosto Matus and Derek Wong.

Identifying the demand for privacy requires identifying the price-quantity trade-offs associated with maintaining privacy and the factors that change price. Much of the discussion surrounding information privacy and biometrics focuses on the convenience or benefits gained through sacrificing information privacy.

The Costs of Strong Authentication

Individual behaviour suggests that a small reward is worth the sacrifice of non-intrusive pieces of personal information, the provision of which amounts to a loss in anonymity. If this relationship exists because demand for anonymity is elastic then it should hold as well for biometrics and stronger forms of authentication. An elastic demand for anonymity would suggest that any benefits gained would be valued relatively more than any anonymity lost. If behaviour represents revealed preferences, then consumers are neither worried about being identified nor concerned with the eventual costs of identification.

However, if the low demand for anonymity is due to privacy-myopia then consumers may care about anonymity and privacy, but realise providing information entails a loss of autonomy. Rationally, the connection between being identified with biometric information is easier to establish than with weaker authentication. Thus, greater benefits/conveniences are required to provide smaller amounts of personal information, for example biometric data.

If revealed preferences hold, the effect of biometrics on the demand for privacy is fairly neutral: biometric requirements represent a shift along the demand curve, lowering the *quantity of privacy demanded*, but not affecting the demand for privacy. However, the latter case implies a lower cost to maintaining privacy as the expected cost of identification with biometrics rises relative to the expected cost with weaker forms of authentication.

Advancing technology poses both risks and benefits for consumers. Ever stronger forms of authentication, for example biometric passports, not only strengthen ownership concerns, but also increase the costs of identification due to linking personal information. This latter effect can be seen as reducing the cost in the secondary market of creating usable information sets used, for example, for targeted-marketing purposes. Technology can also increase benefits by increasing the technology available to protect privacy. However, insofar as revealed preferences hold, consumers' limited willingness to use advanced anonymising technologies may not overcome the costs of stronger forms of authentication. Given myopia, increased technology should raise the demand for privacy.

Stronger forms of authentication, like biometric identifiers, increase the demand for privacy by altering individuals' internal valuations of the cost of maintaining privacy. The strength-of-signal and loss of autonomy inherent to biometrics increase the costs of identification. An increase in the stated demand for privacy implies greater amounts of benefits are required to entice a consumer to sacrifice given amounts of privacy or autonomy.

Biometrics reduces the myopia due to bounded rationality and asymmetric information about secondary information markets. Moreover, the gap between privacy-rational demand and privacy-myopic demand explains the observed gap between stated preferences and actual behaviour.

Understanding the Responses

What is the lay public's perception of biometrics? What values are associated with it? What ideas come to mind when someone engages in a discussion about biometrics, privacy, security and identification? What patterns of behaviour can we predict from such social representations? We come up with an explanation of the different attitudes, perceptions, judgments and prejudices that the general public has expressed regarding biometrics.

For this we collected information from three focus groups, each comprised of citizens of the UK, the U.S. or other countries. All participants were between the ages of 22 and 31, and were either university students or young professionals. We recognise that there are limitations to the conclusions that can be drawn from such a specific demographic group. However, as we will show, our focus groups may serve as a limiting case.

The main purpose of focus group research is to draw upon respondents' attitudes, feelings, beliefs, experiences and reactions in a way that would not be feasible using other methods, for example observation, one-to-one interviewing, or questionnaire surveys. There are many definitions of a focus group in the literature, stressing different features like organised discussion, collective activity, and interaction. These groups comprise six to eight previously unacquainted people meeting for between one and two hours with one or more moderators.

An analysis of their discussions allows us to study the similarities and differences between each group in relation to the social representations of biometrics. We found that nationality played a significant role in the formation of the social representation of biometrics. In the U.S., the events surrounding 9/11, the *USA PATRIOT Act*, and the subsequent creation of the Department of Homeland Security have shaped the way Americans view biometrics. In the UK, media coverage of the debate over the National Identity Cards has dominated public discussion and understanding of biometrics. More generally, movies, documentaries and editorial commentaries have been strongly influential. Nevertheless, when the groups expressed their ideas about biometrics, along with its applications and implications, they shared a number of similar concerns and arguments.

When we asked our participants, *What comes to your mind when thinking about biometrics?* The British group immediately related the topic to the National Identity Cards. "I don't know anything about biometrics except from the ID cards." "The press, ID cards" "I hadn't heard about it until last summer [during the ID debate]." Likewise the British group and in particular the American group based their knowledge of biometric applications on what they had seen in action and science fiction films. References such as "I think of Top Secret Agent films," "Scanning eyes like in Mission Impossible," "It is used for marketing like in Minority Report," "I first heard about

biometrics in Charlie's Angels," or "Identification through physical characteristics like in the movie Gattaca" were reiterative and generalised.

In addition we found that the struggle for understanding biometrics has taken place though personal conversations, newspaper readership, and other forms of mass media. It should be noted that respondents in the more heterogeneous international group did not share any tendency or reference in common towards biometrics. In fact, for some members there was an absence of meaning or points of reference; additionally, some commented that it was the first time that they had reflected on the topic. Consequently, it can be argued that the conceptualization of biometrics is still in an embryonic stage of development or for some, it is simply not there.

In the three focus groups we found that biometrics was predominantly linked to the following descriptions:

- Security
- Criminal investigation
- Surveillance
- Most people associate it with police
- Identification and security
- In the movies it is always in the context of circumvention; people abusing the power
- I think it will be an invasion of my privacy

We divided these concerns into *security* and *privacy*.

Security

A motivating hypothesis for our research was that the concept of *security* would be an anchor for biometrics. Specifically, we believed that the terrorist attacks of 11 September, 2001 would function as a focusing event, making *security* a salient topic in the public sphere.

In our first investigations into biometric representations through written questions and later on in our focus groups discussion we came across a relevant number of opinions that confirmed the hypothesis that the concept of security was an anchor for biometrics. Our groups frequently related security to biometrics across a series of questions about their general knowledge of biometrics and subsequently about their knowledge of applications of biometrics.

British Responses:

- For security reasons.
- They will use it for immigration, security.
- Biometrics is used for government surveillance.
- For tracking people.

American Responses:

- It is a tool for criminal investigation.
- For police identification.
- Criminal investigations and terrorism.

- To enhance security.
- For identification and security.

International Responses:

- The application of biometrics is security.
- For identification.
- To tackle crime and terrorism.

In the latter parts of the focus group, we returned to the issue of security and biometrics to understand more about the associations between the two concepts. We asked our participants two questions: *How important of an issue is security for you?* (follow-up references we provided to the participants were: national security, identity theft, personal safety) and *Would you feel more secure or less secure if people were identified using biometrics?* We obtained the following surprising and unexpected answers:

British Responses:

- I don't feel insecure.
- In my opinion biometrics can not make much difference in security.
- I don't feel insecure in airports.

American Responses:

- I don't feel insecure at airports.
- I don't feel insecure in general.
- I don't think biometrics will make a difference preventing an attack.

International Responses:

- I am sick about it (security), warnings all the time, we hear about it all the time, for me is a bit too much, I am bored with this problem.
- It's not healthy to worry too much about security all the time.
- You can not think that a bomb is going to explode.
- It doesn't make much of a difference to me.
- You can not get completely paranoid and stop doing everything and stay at home.

Even though security is an important anchor through which the participants judge, comment and categorise biometrics, they neither identified security as a pressing issue nor perceived any advantage of this technology in their everyday lives in terms of security benefits. Across all three groups, participants felt that they lived in a secure environment and did not see the relevance of implementing biometrics for security purposes. Quite simply, associations of security with biometrics did not translate into perceptions of benefits: any demand for biometrics is not driven by a demand for security.

Privacy

Privacy was the most controversial issue discussed in the three focus groups and the main issues raised reflected most of the principal concerns of biometrics' critics. From the overall discourse it is possible to establish two conclusions. Firstly, participants had large concerns about data collection and management. Second, these concerns implied that the individuals' demand for privacy was reduced when they dealt with an agent they trusted.

Across the three groups, our participants displayed a feeling of uncertainty and mistrust in the public and private sector about the collection and management of information. These feelings matched perceptions in the public at large. In the Detical/MORI poll, when asked, "how confident are you that the Government can be trusted to hold identity cards information securely?", 88% of the answer range between 'Fairly confident' to 'Not at all confident'.

In general this fear is based on the possibility that information might be filtered, sold or extracted without the citizen's knowledge and/or consent. The biometrics case is particularly worrisome for people given that it operates with characteristics that can not be replaced, for example iris, fingerprint or voice data. Once information is stolen there is no way to change it, as is easily done with a password or a credit card number. The responses highlighted fears about ownership and the life-cycle of information:

British Responses:

- Someone can know where you shop.
- It's scary that anyone might have the information.
- Consumers may not be aware that their information is given.
- I see negative implications… information should always be the minimum
- demanded…It should not be shared.

American Responses:

- All kinds of implications!! Who voluntarily gives the information?
- Most implications on privacy are negative, you see them in the movies.
- Gattaca is the perfect example, you can manipulate and change information.
- Someone can scan your genetic information and use it against you if they somehow duplicate your fingerprints. They can pretend they are you.
- People can know if someone has HIV.

International Responses:

- There's a medical impact, it will be very easy for people to know your medical background.
- It could lead to discrimination; they may not want to employ you.
- For me the question is, how can they impact my privacy? how can it be misused?

Secondly, attitudes towards privacy change when participants identify a person or organisation, public or private, which they do or do not trust. In a general sense, trust is the degree of confidence when someone thinks about a relationship. One aspect of trust is predictability, which refers to our ability to predict someone else's specific behaviour. A predictable person or organisation is someone whose behaviour is consistently good or bad. But consistency is not enough for confidence to grow. A sense of trust must be based on the knowledge that someone else acts in consistently positive ways. For all its value in conducting day-to-day exchanges, predictability is at best a starting point for the development of trust. After all, we predict particular actions, but we trust people or organisations. We do not trust an institution to protect our information just because the institution says that they will not abuse that trust, but rather we trust the institution only because we know of its disposition, their available options, the consequences and their ability and so we expect they are trustworthy.

For our participants, trust in data collection and management was an issue of ownership and the individual's relationship with whomever information was being shared. Uncertainty in ownership lowered predictability, and thus trust, in a given information-sharing relationship. All three groups shared concerns about ownership, suggesting that their demand for privacy would decrease the more trust in the information-sharing relationship increased:

British Responses:

- What happens if the government changes? What happens if regulation changes? That's what worries me the most, if they have my information.
- You should give your consent when your information is shared. For me the important issue is who holds the information.

American Responses:

- As an organic consumer I would be totally happy to give information, fill a survey, to one of those macrobiotic shops.
- I would give information to my doctor.
- The answer is going to change depending on who the government is. Could be your citizens council vs. Washington DC. Depends on what part of the government you are talking about.
- Depends on the definition of security and who is in charge of providing it. I feel better without the current administration.
- They seem to violate my trust in their provision of security. If it were another administration… I wouldn't be so suspicious.
- Privacy issue, yes that bothers me. Security issue, no, well… depends who will use the information at the airport.

International Responses:

- I don't care about how much information I am giving; the most important thing is who is going to see my information and how is going to be used.
- If it is for my own safety it does not matter, just depends on who is in charge of the data.
- You must be very careful with this kind of information. There could be dangerous applications under a regime like the Nazis, where they used the information against the Jews – it depends on the kind of government.

These responses suggest that the level of trust towards the generic term "government" may change depending on the perceptions and relations that the individual has established with the different tiers of government (local, regional or federal) and on the public officials in charge of them.

Similar attitudes are observed with the level of trust in the private sector. Our participants consistently identified the profit motive of the private sector as a reason to doubt the information sharing relationship. It is easy to mistrust big supermarkets when they conduct market studies, but when considering a local corner store with which one is familiar and trusts, one is much more likely to provide substantial amounts of personal information.

In order to have a better understanding of these responses and the possible behavioural patterns that they may explain, we asked our participants to discuss and develop their arguments about the possible impacts on them by the governments' use of biometrics

and, specifically, *Who should control the collection and dissemination of personal data?*

British Responses:

- National agency accountable [to the public].
- Private body accountable to government, but not the government itself
- Independent bodies who will protect privacy.
- People themselves should have ultimate control and must be involved in the decisions that concern them.
- Not certain that government won't use the information inappropriately.

American Responses

- Government under strict regulation.
- Whoever can protect it from use outside what has already been authorised.
- Government but without disseminating it. Corporations never unless consent.
- Government should regulate the dissemination of personal data.
- Government with consent. Private companies also but with permission.
- If anyone, government.

International Responses:

- The government has to be accountable, we assume a government with constitutional set up.
- Government if it has an interest in public safety.
- If it is for security purposes, who has the discretion to use it?
- Who is monitoring the data? That is very important.
- The compromise should be to protect the data.
- I think that information could be shared but there should be an agreement between the government and the public… for what are they going to use this information…so we can trust.

Overall we found a strong demand for governments' regulation of the collection, storage and distribution of biometric information. Because there is a strong mistrust of the public and (more so) the private sector, the feeling of uncertainty about complete contracting raises the demand for privacy.

When confronted with hypothetical tradeoffs between security and privacy in biometric applications, the participants opted for privacy. And when asked, *What makes giving information to businesses different from giving information to governments?* participants raised several concerns about business:

British Responses

- I have more trust in giving biometric information to the government than giving it to businesses. Businesses will use your information for advertising.
- In theory the government is to protect people. Businesses care only about profit
- There is no guarantee on what they (businesses) will do with it (information).

American Responses

- The business sector can sell the information to somebody else.
- The Business sector wants to know everything about your consumption habits.
- The Business sector always wants to sell you something. Although governments' objectives can change.
- They (private sector) can sell the information to the highest bidder.

- The government is not going to call me in middle of a dinner.
- If business sector can be defined as my doctor… I trust my doctor more.

International Responses

- Businesses can use it for profit purposes.
- Businesses can sell the information to other companies.
- I would give my information more easily to my government than to business.

We recognise the limits of possible conclusions that can be drawn from a study with an unrepresentative population. However, we argue that their responses may serve as a limiting case. Our participants are highly informed and highly educated compared to the average person. As part of their regular activities they actively engage in discussions about global politics, economics and relevant social issues. Therefore, we consider that their social representations, as gathered through the focus groups, could be a limiting case for our research in biometrics. This group of young, well-informed, and well-educated citizens conceptualise biometrics in terms of science-fiction movies, yet they are to a certain extent also able to separate fact from fiction. While recognising potential benefits from biometric authentication, they expressed doubt and uncertainty as to how personal data would be used. It is fair to assume that the rest of the population may draw even less rational inferences from the same images seen in films. The general public is more likely to be confused about the use of biometrics, and thus, the average person's perceptions may be relatively more influenced by fantasy than reality.

Conclusion

The results of our focus groups suggest that the social representation of biometrics is objectified primarily in science fiction movies and, predominantly for the British group, in the ID cards debate. In the U.S. and British groups there was a stronger influence from science fiction films and in the international group we did not find any tendency or reference in common towards biometrics. Nevertheless, when the groups expressed their ideas about biometrics, along with its applications and implications, they shared a number of similar concerns and arguments anchoring biometrics in terms of security and privacy. Even though security is an important reference through which participants discussed biometrics, they did not perceive any security benefits resulting from the use of biometrics.

Participants believed that they live in a secure environment and do not see the relevance of implementing biometrics for security purposes. In terms of privacy all groups showed a great concern that the government and the private sector could misuse biometric information. These concerns were much more accentuated toward the private sector. In any case, these attitudes are susceptible to change when participants identify a person or organisation, public or private, that they trust. Overall there is strong demand for governments' regulation of the collection, storage and distribution of biometric information. These attitudes underscore the importance of information ownership and trust relationships between citizens and relevant service providers.

Appendix Three: Memorandum of Laws on EU Freedom of Movement

Introduction

This memorandum[151] describes certain of the issues associated with the United Kingdom's (UK) proposed Identity Cards Bill, introduced and published by the UK Government on 29 November 2004. A report issued by the Joint Committee on Human Rights on 2 February 2005 already has examined the Bill for compliance with human rights legislation and principles, including notably the European Convention on Human Rights. This memorandum thus does not address that particular subject, but notes that the Bill does give rise to a number of potential issues as a matter of UK and European human rights law.

This memorandum instead focuses on certain other legal issues raised by the proposed legislation. In particular, we consider the extent to which the Bill -- as currently envisioned by the UK Government -- could conflict with existing European Community principles governing the free movement of persons within the European Union (EU). We also tentatively outline other issues that the Bill raises, such as issues relating to third party liability and possible indirect discrimination arising from phased implementation of the identity card scheme. We do not discuss here the details of the proposed legislation, and assume some familiarity with its requirements.

EU Freedom of Movement Principle

Summary

The Government's Identity Card Bill would appear to require the mandatory registration on the National Identity Register of all EU citizens resident in the UK for more than three months.[152] This requirement arguably conflicts with EU freedom of movement principles and, in particular, with the recently enacted EU Directive on the Free Movement of Persons, Directive 2004/38/EC (the Directive). The Directive's provisions suggest that EU citizens should not and cannot be compelled to register with the National Identity Register and obtain an identity card, at least not on the conditions set forth in the proposed Bill.

EU Free Movement Principles and Directive 2004/38/EC

The free movement of persons within the EU remains one of the four pillars of the EU's Internal Market. Under the free movement principle, EU citizens retain a fundamental

[151] This Memorandum of Laws was prepared for the London School of Economics and Political Science by Covington and Burling.

[152] "Registration certificates and residence permits for foreign nationals would be issued, taking account of EU standards, but to the same level of security as the UK identity cards and as part of a single overall system of recording and verifying the identity of all legal residents". Cm 6359, Identity Cards: The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130, p 4.

right to freedom of movement and residence within the EU, as conferred directly by Article 39 of the EC Treaty, subordinate legislation and related case law. The precise rights of entry and residence now are governed by a complex body of EU legislation.

Under legislation that preceded the new Directive, EU citizens could enter another Member State "on production of a valid identity card or passport" and stay in that Member State for up to three months without the need to comply with any formalities, such as obtaining a residence card. Workers, self-employed persons and their families were entitled to a five-year residence permit that could be renewed automatically.

Then, in 2001, the European Commission issued proposals that ultimately resulted in the enactment of Directive 2004/38/EC. The Directive's principal aim is "to simplify and strengthen the right of free movement and residence of all Union citizens" by codifying existing directives into a single legislative act. The Directive creates a new right of permanent residence and sets forth the limits that can be placed on these rights by Member States on public policy, public security or public health grounds.

The UK Government has until 30 April 2006 to implement the Directive and, prior to implementing the Directive, is precluded from enacting conflicting legislation. As noted by the European Court of Justice in Case C-129/96 *Inter-Environment Wallonie ASBL v Région Wallonie*, "it is during the transposition period that the Member States must take the measures necessary to ensure that the result prescribed by [a] directive is achieved at the end of that period" and to refrain "from adopting measures liable seriously to compromise the results prescribed".

The Proposed Scheme is Arguably Incompatible with Directive 2004/28/EC

The Directive requires Member States to allow EU citizens "to enter their territory with a valid identity card or passport" (Article 5) and to reside there for up to three months "without any conditions or any formalities other than the requirement to hold a valid identity card or passport" (Article 6). EU citizens, therefore, have the express right to stay in the UK for up to three months without any conditions or formalities. Requiring them to acquire a UK identity card during that period of time would qualify as a condition or formality. The Government appears to have accepted this and has stated that for "legal reasons, it is not feasible to require EU nationals to register until they have been in the UK for three months and intend to stay longer."[153]

Article 7, in turn, confers on all EU citizens the right to reside in another EU Member State for more than three months, if the citizen falls into one of the following categories of persons: workers and self-employed persons, students and those with sufficient resources to support themselves without becoming a burden on the relevant Member State's social welfare system.[154] Article 8 describes the administrative formalities that a Member State may apply to such EU citizens -- namely, the host Member State may require the EU citizen to "register with the relevant authorities" (Article 8(1)). Article 8(2) goes on to clarify that a "registration certificate shall be issued immediately [by the

[153] Cm 6359, Identity Cards: The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130, p 10.

[154] Family members (whether or not EU citizens) have a corresponding right of residence if they are accompanying or joining the EU citizen.

Member State], stating the name and address of the person registering and the date of registration." The "registration certificate" is, however, all that the Directive requires.

The Directive is unclear as to whether the "registration certificate" itself may or should contain any additional information beyond the individual's name, address and date of registration. The indications are that it should not. When originally proposing the Directive, the European Commission commented:

> The residence certificate states the name and address of the person concerned; it does not have a period of validity and simply states the date of registration. *The purpose of the certificate is merely to record that an administrative formality has been carried out.*[155] (emphasis added)

In other words, and consistent with the notion that residency in another EU Member State should not entail onerous registration requirements, the residence permit should only require the bare minimum amount of information specified in Article 8. There certainly is nothing to suggest that additional personal information about an EU citizen, such as the individual's date and place of birth, previous addresses, photograph, fingerprints or biometric data should be included. Indeed, just the opposite result would appear to be called for given the underlying aims of the Directive.

Moreover, for the registration certificate to be issued, Member States "may only require" under Article 8 that the EU citizen present a valid identity card or passport and, where they qualify as a worker, confirmation that they are entitled to work from an employer in that Member State or a certificate of employment. If the EU citizen falls into one of the other categories of person entitled to residence over three months, the Member State can require "appropriate proof" (Article 8(3)). Recital 14 of the Directive, however, clarifies that the documents specified in Article 8 serve as an exhaustive list of the supporting evidence that a Member State may require before issuing a registration certificate.[156]

Significantly, the Government appears to equate registering, as that term is understood under the Directive, with registering for purposes of the National Identity Register.[157] However, the process of registration under the Directive is limited and carefully prescribed, as noted above. Indeed, the UK proposal would call for further evidence or information that would appear to be contrary to the spirit of the Directive, which is "to simplify and strengthen the right of free movement and residence of all Union citizens" and generally to reduce and harmonise the administrative formalities that may be applied to this right. At a minimum, this suggests that the UK Government should not

---

[155] Com(2001) 257 final, p 12.

[156] Recital 14 provides, in particular, that: "The supporting documents required by competent authorities for the issuing of a registration certificate or of a residence card should be comprehensively specified in order to avoid divergent administrative practices or interpretations constituting an undue obstacle to the exercise of the right of residence by Union citizens and their family members".

[157] The UK Government has stated that: "For legal reasons, it is not feasible to require EU nationals to register until they have been in the UK for three months and intend to stay longer. EU Free Movement legislation provides that all Member States may require nationals of other EU states resident in their territory to register with the authorities 'not less than three months from the date of arrival'". Cm 6359, Identity Cards: The Government Reply to the Fourth Report from the Home Affairs Committee Session 2003-04 HC 130, p 10.

require that EU citizens residing in the UK apply for and obtain an identity card that contains unique biometric identifiers and would compel the citizen to submit, or have third parties submit on his or her behalf, extensive documentation and other supporting evidence.[158]

The Directive's Derogations Do Not Appear to Permit Blanket Restrictions

The Directive permits limited restrictions on the freedom of movement and residence of EU citizens "on grounds of public policy, public security or public health" (Article 27(1)). The Directive carefully limits the scope of these public policy and public security derogations, stating that measures taken must "comply with the principle of proportionality and shall be based exclusively on the personal conduct of the individual concerned" (Article 27(2)). This is consistent with European case law, which has interpreted these derogations narrowly and introduced the notion of "proportionality". Significantly, Article 27(2) provides:

> The personal conduct of the individual concerned must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society. *Justifications that are isolated from the particulars of the case or that rely on considerations of general prevention shall not be accepted*. (Article 27(2)) [emphasis added]

Therefore, the Article 27 derogations can only be used on a case-by-case basis and not against an entire class of individuals, as these "shall not be accepted". Thus, it would not appear possible for the Government to rely on general claims of "public security", for instance, to resolve any conflict between the Identity Cards Bill and the provisions of the Directive. As a consequence, any blanket rule that would require all EU citizens residing in the UK to become registered on the National Identity Register would appear to fall outside the scope of any applicable derogation permitted under Article 27 of the Directive.

[158] The Directive creates a new right of permanent residence. EU citizens who have resided legally in another Member State for five years may, but are not obliged to, apply for a "document certifying permanent residence" (Articles 16 and 19). The Directive does not specify the form of the application or the document, so it is possible that the document could be similar to the identity card as proposed. What is clear, however, is that the document must be valid indefinitely, not renewable after a prescribed period as in the case of a UK identity card.

Appendix Four: Data protection analysis

> "I want to make it very clear to the public that this draft Bill is not just about an ID card, but an extensive national identity register and the creation of a national identity registration number. Each of these raise substantial data protection and personal privacy concerns in their own right. The introduction of a national identity register will lead to the creation of the most detailed population register in the UK." - Richard Thomas, Information Commissioner, Press Release July 2004.

This appendix will seek to identify some of the data protection and privacy concerns referred to by the Information Commissioner.

The National Identity Register

Although the Register forms a substantial part of the Bill its existence is not acknowledged in the title of the Bill. The problems in the development and maintenance of such a database are well known with difficulties including the identification of the appropriate technology and running systems. The DPA requires any personal information held in a database to be accurate, up to date, relevant, adequate and not excessive for the stated purposes; standards which provide sufficient challenges to data controllers. However, should compulsion for the whole nation become fact, the scope of the Register, the amount of information to be held and the necessary complexity of the infrastructure will present additional problems in terms of compliance with the DPA.

The Bill states that the Register is to be a convenient method for individuals to prove registrable facts about themselves to others and to allow those facts to be ascertained by others where it is in the public interest; only one of those 'registrable' facts is a person's identity. Identity per se is listed in cl 1(6) of the Bill as being a person's full name, other names by which they have been known, place and date of birth and identifying physical characteristics.

The Bill lists another 15 classes of information that may to be included on the Register. It is difficult to see how the requirement for all of this information can satisfy the 3rd Data Protection Principle by being relevant, adequate and not excessive for the proposed purposes. A person will be required to provide their present main address, alternative addresses and previous addresses; a great deal of historical information will be collected that will not contribute to a person's 'identity'.

The Register will also include a great deal of transactional data such as dates of applications, modifications and disclosures of information on the Register; the purposes of the Register are insufficiently precise to understand how such data retention will not be in breach of the 3rd , 4th and 5th Data Protection Principles.

The information held on the Register will be disclosable without the consent of the individual to the Security Services, Chief Police Officers, Inland Revenue and Customs & Excise, any prescribed government department and any other person specified by Order by the Secretary of State. Again the potentially wide audience to whom this large and powerful amount of information might be disclosed to will go the fairness and transparency features of the 1st Data Protection Principle and the specificity requirement of the 2nd.

Section 29 of the Data Protection Act does make provision for disclosures to bodies such as the police and Inland Revenue, however, the body making the disclosures is required, in the absence of warrant, court order or other legal compulsion, to assess on a case by case basis whether the information should be passed on. Cl. 19 of the Bill does not require such an assessment, but is merely qualified by Cl. 23 which states it is not reasonably practicable to expect the requestor to obtain the information by other means. There is no exposition of this test and with a growing centralized database of information about the UK populace one can imagine both security and law enforcement forces arguing that obtaining information from other sources will not be 'reasonably practicable', particularly if they believe their request is likely to fail the s.29 test.

If the argument for a National Register is accepted then the actual practical aspects of administration, maintenance and compliance with the information quality principles (3rd, 4th, 5th) present very serious concerns.

One particular concern is the requirement upon individuals to notify the Secretary of State of any changes to the registrable facts on the Register in Cl. 12 of the Bill. Under the provisions of the 4th principle, it is the responsibility of the data controller to take all reasonable steps to ensure the information they hold is accurate and up to data. Not only does Cl. 12 shift this responsibility onto the individual but imposes a penalty of up to £1,000 for failing to do so even though later on at Cl. 37 an individual may eventually have to pay a fee in order to alter their records. One can anticipate the difficulties that are likely ensuring that it is up to date bearing in mind the range of information that is going to be held on the Register. There may well be issues about policing of such requirements.

Finally, there are already several other initiatives underway to collate information about citizens in the UK: the Citizen's Information Project initiated by the National Census Office and the database of all children under the Children's Bill. There is clearly further potential for the amount of information to be linked or transferred to the National Identity Register if the Secretary of State chooses to make this happen by Order. It is unclear at present how these initiatives are to work together in practice. Other policies such as the retention of communications data by communications service providers and the tracking of vehicles for taxation of road usage also have the potential to be combined to provide the government with a comprehensive and all pervasive database on the lives of its citizens.

The Identity Card

The purposes of the National Identity Card still remain to be clarified: referring back as it does to the entries in the Register – the 1st Data Protection Principle therefore remains to be satisfied within the legislation itself. There is also general concern that even if such purposes were to be listed in sufficient clarity within the legislation, the production of an ID card would be required in order to access a wide number of as yet unanticipated services both in the public and private sector – the 'function creep' referred to by so many commentators on the legislation.[159] The notion of function creep is nothing new; the same process happened with the ID card issued during World War II when there were originally three purposes for the card (national service, security and rationing); eleven years later thirty nine government agencies made use of the records for a variety of services.[160]

It is also unclear from the Bill precisely what information will be held on the face of the card and which parts will be encrypted on the card chip, and even where some parts are encrypted, who will have access to the full information on the card. The 1st and 7th Data Protection Principles may be breached if there is insufficient security surrounding the information on the card. Without clear limits on who may access information on the card and then go on to retain the information they have obtained there is a danger of the 3rd and 5th Principles being breached.

The issue of ID cards to those applying for the issue or renewal of certain documents such as driving licences and passports will not only contribute to the lack of clarity as to purposes but will also undermine the idea that the compulsion to hold an ID card will be the subject of scrutiny in Parliament before it is extended to the wider populace. When an individual is asked to present an ID card based on one of these documents it is very likely that not all information will be relevant on every occasion. The risk is that excessive information will be disclosed and possibly retained even where it is not necessary for the particular circumstances in which the card was presented and the 3rd Principle will again be breached.

If the aim of the ID card was to merely confirm identity it would be possible to achieve this purpose through a far simpler process and much less personal information would have to be gathered and retained than that which is being proposed by the Bill. This would present far fewer difficulties with compliance with the Data Protection Act and Human Rights Act.

National Identity Registration Number

The introduction of a unique identifier which will be linked to information stored in the National Identity Register and linked to other nationally used numbers such as National Insurance and Driving Licence numbers raises further concerns particularly in terms of security. The value of the National Identity Registration Number will mean that steps will have to be taken to ensure the number does not gain common currency and is

[159] Information Commissioner's evidence to Select Committee on Home Affairs, 3rd February 2004.
[160] Information Commissioner, Response to the Government's Consultation on Legislation on Identity Cards, 2004, http://www.informationcommissioner.gov.uk/cms/DocumentUploads/the%20information%20commissioners%20response%20to%20the%20draft%20bill.pdf.

protected from cloning, duplication and other practices that might lead to identity fraud. The 1st and 7th Data Protection Principles will have to be adhered to closely if the Number is to be properly protected and used.

General Issues

There are some general data protection issues that run as a common thread throughout the Bill and the next section aims to highlight those particular areas of concern.

Fair and lawful processing

There are three main elements to the First Data Protection Principle: processing must be legitimate, fair and lawful. The very enactment of the enabling legislation will ensure that any processing will be legitimate.

There may be questions however, surrounding the other two elements of fairness to individuals and lawfulness. Although the Bill does list more clearly the purposes for which the ID card and Register will be used than in earlier proposals, the provisions within the Bill for wide ranging powers of the Secretary of State to make amendments to the legislation by Order without full consideration by Parliament or public debate mean that the existing purposes and consequent disclosures may become less clear over time and any Fair Processing Notices provided by either the Home Office or participating public bodies will become inadequate.

The overall test of fairness may, in the view of some, not be satisfied either: charging individuals for the issue of the cards themselves and for keeping that information up to date may not be fair if it disadvantages certain groups of people. Cl. 2(4) states that an entry may be made in the Register for a person whether or not the individual has applied to be, or is entitled to be in it.

Furthermore, once the decision to make the ID card compulsory for all is taken, some of the safeguards in the Bill such as the Cl. 18 prohibition on making the production of an ID card a condition of providing a service will be undermined and remove the opportunity for a person to choose to rely on alternative means of identification.

The third element of the 1st Data Protection Principle (that of lawfulness) brings into play the human rights considerations mentioned earlier. Both the European Convention on Human Rights and the Human Rights Act allow for intrusions on the right of privacy where they are necessary to safeguard national security, defence, public security…the rights and freedoms of others… and is necessary in a democratic society. One of the questions which needs to be asked is whether the actions being taken are a proportionate response to the harm seeking to be avoided. The Home Secretary has stated that he believes the provisions of the Bill are compatible with the Convention Rights but has yet to demonstrate why he feels able to make this statement. However, it has long been accepted by the European Court of Human Rights that the storing of information and the use of it amount to an interference with the right to respect for private life.[161] Compatibility therefore remains to be tested in the courts.

[161] Leander v Sweden, March, 1987; Amann v Switzerland, February 2000, Rotaru v Romania, 2000

Security

The Bill proposes that the ID card and National Register will provide for an individual to establish his identity and obtain the services to which they are entitled. It is quite clear therefore that the ID card and Register will become a target for identity fraudsters; protecting against unauthorized access, use and disclosure as required by the 7th Data Protection Principle will present huge technical and logistical challenges which are not addressed within the Bill apart from the expected criminalization of certain behaviours. Given the potential damage and risk to an individual whose information and identity is unlawfully obtained and used, the Bill is worryingly silent on how the infrastructure will be kept secure and how individuals whose identities are stolen will be dealt with. Recent failures of existing governmental computer systems such as those at the Child Support Agency, Department for Work and Pensions and even the police fingerprint database, illustrate the need for a robust, secure and foolproof technology.

The Bill anticipates that various public bodies will be able to access the 'registrable particulars' of the individual in question. A comprehensive set of standards of processing and procedures are going to be necessary in order to protect the integrity of the National Register and the information held by those public bodies.

The 7th Data Protection Principle also requires data controllers to ensure their suppliers take steps to keep the information they process on behalf of the data controller safe from loss and disclosure. If any of the functions of the ID card and Register are outsourced, the government will have to ensure the contractual arrangements are sufficiently rigorous to protect the data and provide for the independent auditing of those outsourced functions. Clearly if any outsourcing were to be overseas the 8th Data Protection Principle would also be engaged.

Data sharing

One of the main results of the provisions of the National Identity Register will be that a great deal of information will be shared between public bodies. The government undertook a large exercise several years ago via the Performance and Innovation Unit which considered the obstacles to data sharing between public bodies. Some of those obstacles were overcome by legislation which established lawful gateways for data sharing but also required memoranda of understanding to ensure data was only shared where necessary and that all the information held by various public sector bodies did not end up being pooled. This approach recognized that public bodies' powers only extended to the extent of their enabling legislation and that there were also public concerns about their information being shared widely across the public sector.[162]

The proposals in the present Bill will undermine those protections and at the same time make data sharing much less visible and transparent. Cl. 19(4)f gives the Secretary of State powers to specify when the information contained in the Register may be disclosed on top of those crime prevention, customs and tax purposes already enumerated in the clause.

[162] Cabinet Office, Privacy and Data sharing – The way forward for Public Service, PIU, 2002.

Conclusion

The Identity Cards Bill raises many questions concerning compatibility with existing Data Protection legislation. The remaining lack of clarity of purpose and the wide ranging scope for the Secretary of State to amend the various elements of the legislation by Order, mean that the elements of transparency and certainty sought by the First Data Protection Principle may not be provided. The lack of clarity has a knock on effect for satisfying the remaining principles – if the purpose is not clear it is difficult to assess whether information stored is relevant or excessive. The Bill also proposes turning the principle that it is the data controller's duty to ensure the accuracy of their data on its head by laying this onus on the individual themselves. Furthermore, though not clearly stated, it is implicit that the information fed into the Register will be kept indefinitely.
The Bill in many ways seeks to obviate the requirements of the DPA by taking the whole ID card outside the data protection regime: "The Government's commitment to make the scheme consistent with the data protection legislation can be summarized as outline proposals to exempt the scheme from five of the eight data protection principles through the use of statutory powers."[163]

Definitions

Data subject means an individual who is the subject of personal data.
Personal data means data, which relate to a living individual who can be identified –
a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Sensitive personal data means personal data consisting of information as to-
a) the racial or ethnic origin of the data subject,
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether they are a member of a trade union,
e) their physical or mental health or condition,
f) their sexual life,
g) their criminal convictions or alleged convictions.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including-
a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data: *this will include simply* looking at information on a computer screen and making a decision about the individual based on that information which is then recorded elsewhere.
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data.

Data controller means, a person who (either alone or jointly or in common with other persons) determines the purposes for which and manner in which any personal data are, or are to be, processed.

[163] Memorandum submitted by the Editors of 'Data Protection and Privacy Practice' to the Select Committee on Home Affairs.

enterprise privacy group