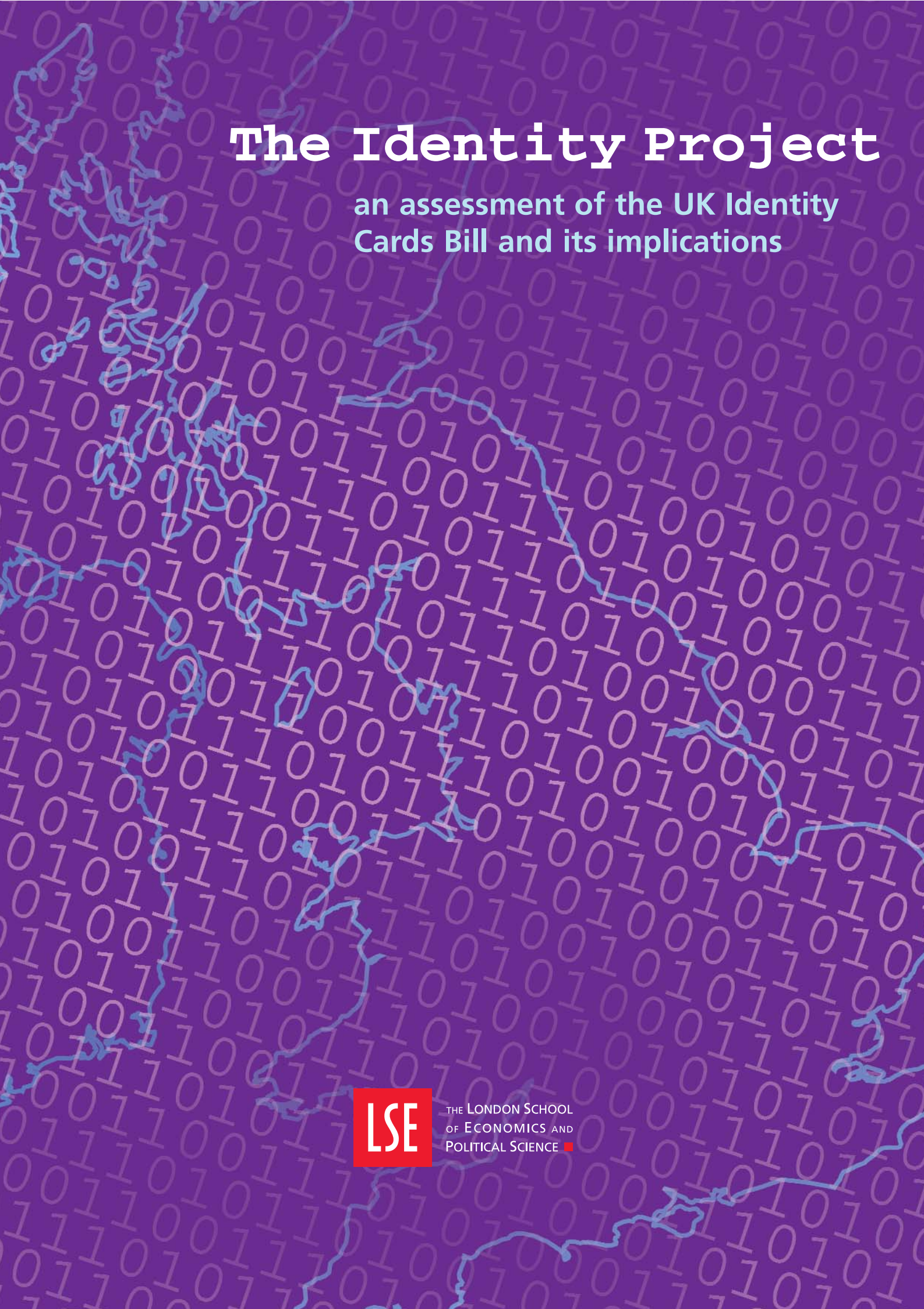


The Identity Project

an assessment of the UK Identity Cards Bill and its implications

LSE
THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

The Identity Project

An assessment of the UK Identity Cards Bill and its implications

Project Management by

Hosted and Published by

Version 1.09, June 27, 2005

Credits

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, Contributors, Advisors and Reviewers

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

Professor Ross Anderson, Cambridge
Adrian Beck, University of Leicester
Ralf Bendrath, University of Bremen
Krista Boa, University of Toronto
Nicholas Bohm
Daniel Boos, Switzerland
Dr Stefan Brands, McGill University
Dr Ian Brown
Tony Bunyan, Statewatch
Dr Nadia Caidi, University of Toronto
Marco A. Calamari, Italy
Shami Chakrabarti, Liberty
Professor Roger Clarke, Australia
Professor Andrew Clement, Canada
Dan Cooper, Covington and Burling
Mike Cushman, LSE
Ian Dowty
Terri Dowty
Mark Dzięcielewski
Alberto Escudero-Pascual, Sweden
Joseph Ferenbok, University of Toronto
Federico Ferretti, University of Leeds
Jens Franz, SOAS
Teresa Hackett, Ireland
Kathrin Gerst, Germany
Marc Gilman
Dr Brian Gladman
Andrea Glorioso, Italy
Wendy Grossman
William Heath, Kable
Rikke Frank Jorgensen, Denmark
Jeegar Kakkad
Philippe Martin, Kable
Meryem Marzouki, France
Ariosto Matus-Perez
Dr Eileen Munro, LSE
Sjoera Nas, The Netherlands
Dr Peter Neumann, SRI International
Professor Toshimaru Ogura
Joe Organ, Oxford Internet Institute
Nicholas Pauro
Daniele Pica, LSE
Dr Chris Pounder, Pinsent Masons
Professor Angela Sasse, UCL
Bruce Schneier, Counterpane Systems
Dr Susan Scott, LSE
Dr Barbara Simons
Dr Steve Smithson, LSE
Nina Somera, Philippines
Jay Stanley, ACLU
Barry Steinhardt, ACLU
Toby Stevens, Enterprise Privacy Group
Peter Szyszko, Covington and Burling
Gohsuke Takama, Japan
Sarah Thatcher, LSE
Prodromos Tsiavos, LSE
Rosemary Walsh
Jeremy Wickins, University of Sheffield.
Johan Wilhelmsson, Swedish Ministry of Justice
Derek Wong

Project Mentors: Simon Davies and Dr Gus Hosein

Acknowledgements

The LSE would like to thank the 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.

We would also like to express our appreciation to the many people and organisations that contributed to this study, and especially to the organisations that participated in the expert roundtables.

Thanks also to William Heath and Philippe Martin of Kable, who supplied the costings framework that formed the basis of our estimates.

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

Finally we would like to thank the LSE Reprographics Unit, the Design Unit, and the LSE Press Office for support above and beyond the call of duty.

Outline

Table of Contents

Foreword

The government's identity card proposals have far-reaching implications. The creation of a nation-wide population database on such a scale and with such complexity has rarely been attempted anywhere in the world. It is not surprising, therefore, that the proposals have sparked a lively debate throughout British society.

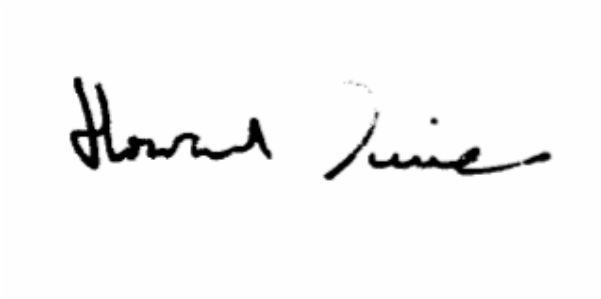
The Government asserts that its version of a national identity system offers the potential to combat the threat of terrorism, identity fraud and illegal working. Critics of the proposals warn that the scheme is fraught with challenges and pitfalls. It is of utmost importance that we reconcile these views and find a constructive way forward.

Six months ago the LSE began a wide-ranging research project intended to resolve these issues. More than a hundred experts, business leaders, and research staff from across the LSE joined forces with colleagues throughout the world to produce a comprehensive analysis of the scheme's implications.

The report's conclusions are first, that, the scheme will involve considerable expenditure. Second, the proposals will alter the nature of British society. The proposals involve important choices that necessitate a wide ranging national dialogue. The LSE's report is an important contribution to that dialogue.

The report also outlines a possible alternative system that promises to be flexible, less expensive and as friendly to civil liberties and privacy as any card system can be in the modern age. It also creates a consumer based platform for the development of e-government and e-commerce services.

We hope the government will be prepared to reflect on the analysis, and the implications for their own proposals.



Howard Davies
Director, LSE

Preface

I welcome the report commissioned and undertaken by the LSE as a valuable contribution to an issue which engages significant data protection and privacy concerns. I have expressed my unease that the current proposal to establish a national identification system is founded on an extensive central register of personal information controlled by government and is disproportionate to the stated objectives behind the introduction of ID cards. It raises substantial data protection concerns about the extent of the information recorded about an individual when the ID card is used in their day to day lives and sparks fears about the potential for wider use/access to this information in the future.

In my response to the government's original consultation on ID cards I made clear my concern that alternative methods of identity management had not been fully explored. I am pleased that this report has been able to identify a blueprint for a national identity system that does not involve the creation of an extensive central register and government held data trail of each time a card is used. The report makes clear that a system which minimises the amount of personal information generated and held by the government on card holders can be established without sacrificing the essential attributes of security, reliability and trust in the system.

I hope that during the scrutiny of the ID Cards Bill, as it passes through the parliamentary process, this report helps focus debate on the actual system for administering ID cards and the need to ensure that this is one which is proportionate to the reasons for wishing to introduce ID cards. Eradicating unnecessary personal information and ensuring that individuals, rather than government, have appropriate control over how their personal information is handled will go a long way towards achieving the essential pre-requisite of establishing a system that inspires full public confidence: one where individuals can be correctly identified when they really need to be rather than one which has the intrusive side effect of the government identifying and recording information about how individuals go about their daily lives. This welcome report demonstrates that such objectives should be achievable in practice. It deserves a wide audience and its findings careful consideration.

Richard Thomas
Information Commissioner

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.

We estimate the likely cost of the ten-year rollout of the proposed identity cards scheme will be between £10.6 billion and £19.2 billion, with a median of £14.5 billion. This figure does not include public or private sector integration costs, nor does it take into account possible cost overruns.

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.

1

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, to assess the costs and implications arising from its provisions, and to suggest areas for improvement.

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 (these are set out in detail in Appendix 1). This concurrence is a crucial test of the strength and validity of both reports.

This Report provides a comprehensive foundation for further debate about many key aspects of the government's proposals. Over the coming months we will continue to build on these findings to assess a wider range of issues relating to the impact and implications of an identity scheme for the UK.

2

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 does, however, challenge assumptions that an identity card system is an appropriate, safe and cost-effective way to achieve those goals.

The Report *concludes* that the establishment of a secure national identity system has the potential to create significant, though limited, benefits for society. Secure identity, if implemented in the right way, can reduce identity fraud and promote the development of the e-commerce environment. However, the proposals currently being considered by Parliament are neither safe nor appropriate. There was an overwhelming view expressed by stakeholders, experts and researchers 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.

There is no evidence to support the use of identity fraud as a justification for the current identity card model. Many of the claims made about the prevalence of identity fraud are without foundation. A card system such as the one proposed in the Bill may even lead to a greater incidence of identity fraud.

The concept of a national identity system is supportable, but the current proposals are not feasible. The Report therefore outlines an alternative model for an identity card scheme that will achieve the goals of the legislation more effectively.

The Government seems intent on pointing to international obligations and precedents to justify the introduction of a national identity card. Our research indicates that a national identity card need not resemble the one that the Government is proposing, nor is any nation under an obligation to create such a card. Indeed, no other country has done so with such a pretext.

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 and the creation of a more flexible "citizen centred" model.

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 fraud 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.

We accept that there is some evidence that the government's scheme could be used as a means of combating illegal working, though measures have already been put in place to address this issue. Beyond these existing measures, an identity card is unlikely to achieve any significant effect

We also accept that the proposed scheme is likely to have an impact on false identity within the benefits sector. However, the government has already put in place vetting regimes that are rigorous and effective. Benefit fraud through false identity is relatively rare and we believe the cost of introducing an identity card in the benefits environment would far outweigh any savings that could be made.

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.

From a security perspective, the approach to identity verification outlined in the Identity Cards Bill is substantially – perhaps fatally – flawed. In consequence, the National Identity Register may itself pose a far larger risk to the safety and security of UK citizens than any of the problems that it is intended to address.

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 will 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.

We estimate the likely cost of the ten-year rollout of the proposed identity cards scheme will be between £10.6 billion and £19.2 billion, with a median of £14.5 billion. This figure does not include public or private sector integration costs, nor does it take into account possible cost overruns.

	Low	**Median**	**High**
Issuing Identity Cards Over a 10-Year Period	814	1015	1216
Passports (Based on Passport Service Figures)	3936	3936	4065
Readers for Public Sector (As Specified in the Bill)	291	306	317
National Identity Register	1559	2169	2910
Managing the National Identity Register	2261	3658	5341
Staff Costs Over a 10-Year Period	1719	3368	5308
Miscellaneous	22	64	117
TOTAL	**10602**	**14516**	**19274**

The National Identity Scheme – Projected Costs (All figures £'m)

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 feature 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 compulsory acquisition of fingerprints in passports may violate the common law right to exit and re-enter the UK. This common law right of each UK citizen is now enshrined in the Immigration Act, which does provide for exceptions. However, if a right to leave the UK exists and a passport is a prerequisite, then a right to a passport must exist also, subject to those exceptions. That right would likely be hindered if new biometrics were introduced. The Act's exceptions are aimed in spirit at immigration control of foreign nationals, not control of UK citizens leaving the country.

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 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 find 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. Even in countries with identity cards, numerous safeguards prevent the development of a system similar to the one proposed here. We were unable to identify any country that established identity cards through an open parliamentary process.

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 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.

3

The Development of This Report

Origins and Objectives

On 29 November 2004, the government published the National Identity Cards Bill. As the Bill passed through Parliament, there was increasing concern within business, academia and civil liberties groups about the lack of informed public debate about its implications for the United Kingdom. As the Information Commissioner told The Times newspaper in August 2004:

> "My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than British society would feel comfortable with."

In response to that concern, in January 2005 the London School of Economics (LSE) initiated a project to examine in detail the potential impacts and benefits of the Identity Cards Bill. The objectives of the project are to:

- Provoke debate about the nature and impact of the National Identity scheme;
- Gather a broad spectrum of opinions from diverse stakeholder groups;
- Consider possible architectures for delivering the infrastructure;
- Interpret the proposed legislation and debate its implications;
- Publish a detailed report that explores the key issues and recommends changes to the Government's plans where necessary;
- Establish a working party that will continue to consider identity issues after the publication of the report.

Work on the project began in January 2005.

The principles outlined in this report are derived from the recommendations of Expert Panels representing business, government, academia, non-government organisations and industry/professional bodies. These groups have met on several occasions to debate the impact of the Identity Cards scheme. Further input has been obtained through one-to-one meetings, documents submitted by Expert Panel members, and the ongoing debate within the project team.

The Expert Panel findings supported the principle and objectives of the Identity Cards Bill, but recommended numerous changes to the system architecture, development and management.

The LSE project team has developed the Expert Panel recommendations into the broader analysis and recommendations in this report. The team has solicited opinions, analysis and criticisms from a large group of industry and academic specialists covering technology, security, privacy, public sector, procurement and legal disciplines.

The LSE team has made several attempts to engage the Home Office Identity Cards Unit in the project, but at the time of publication there has been no meeting between the two parties.

Sponsorship

The Identity Project is a project of the London School of Economics, and is hosted by the LSE's Information Systems Department. The project is facilitated by Enterprise Privacy Group[1] (EPG) Ltd. The Expert Panel meetings were supported by the Financial Times, and the first and second meetings were chaired by senior journalists from the Financial Times.

Expert Panel Consultation

At the outset of the project, the LSE team recognised the need to gather the broadest spectrum of opinions on the National Identity scheme, and to engage in debate with as many interested parties as possible. To achieve this, Expert Panels were formed from a group of 85 individuals in 43 organisations, representing business, government, academia, non-government organisations and industry/professional bodies.

Expert Panel members include companies that have designed and implemented national identity schemes in other countries, and companies that may have an interest in delivering the UK scheme. Representatives of the IT industry, business management, legal profession and affected Government departments were involved. Views of strong support for the Government's scheme and strong objection to it were expressed. Since the meetings were held either off the record or under the Chatham House rule, these individuals and organisations are not identified in this report.

At each meeting, the Expert Panel Members were asked to assume that the Identity Cards Bill will be passed into legislation, although it may be amended. The Members were also asked not to debate the principle behind identity cards, since this emotive subject could undermine the independence of the debate. Instead in each meeting the debate focussed upon how best to deliver a National Identity scheme.

The Expert Panels met on the following dates:

- 7th February 2005
- 10th February 2005
- 23rd March 2005
- 10th May 2005
- 19th May 2005

[1] http://www.privacygroup.org

After each meeting, the recommendations were written up and circulated to the Expert Panels for comment and approval. They were then published on the EPG website.

The Expert Panels were not offered the opportunity to review the report drafts, and participation in the Expert Panels does not imply support for this report, the Interim Report or the overall project.

Expert Panel Findings

The Expert Panels made numerous recommendations, which are provided in full in the appendices of this report. The key recommendations can be summarised as follows:

- **Architecture:** The provision of e-government services just requires a trusted National Identity Registration Number, backed by a biometric(s). Existing government systems can link to the National Identity Register without a need for further personal information to be held in that Register. The amount of data stored in the National Identity Register can be minimised through storage and processing of data in smartcards, which can themselves work 'offline' where either required to do so (through lack of network connectivity) or chosen to do so (where 'strong' authentication of the card for high-integrity authentication is not an issue, eg proof of entitlement to access local authority services).
- **Value-Add:** The system should provide a platform to enable use of the scheme in a business environment (potentially through the integration of digital certificates) delivered on the identity card itself.
- **Enrolment:** The government needs to spend 'disproportionate' effort on enrolling citizens into the National Identity Register to ensure that the content of the Register can be trusted.
- **Transparency:** The Government should adopt a cooperative approach to development of the scheme, including open consideration of other countries' identity card schemes, and greater transparency of the total accrued and forecast costs and how those figures were derived.

These recommendations established the spirit and tone of the report: the Expert Panel unanimously approved the principle of identity cards, and agreed that the correct scheme could cost-effectively address some of the Government's objectives. The Panel also identified numerous benefits that would derive from its preferred scheme, such as the rationalisation of the number of identifiers carried by each citizen, and the elimination of certain identity-related frauds. However, the majority of Expert Panel members agreed that the Identity Cards Bill not only fails to deliver these benefits, but also potentially closes off any opportunity to achieve them. In response, the Expert Panel called for changes to the legislation, architecture and proposed delivery process.

Academic Collaboration and Other Sources of Research

In addition to the Expert Panel facilitated by EPG, the LSE team has engaged numerous academic and industry experts from around the world to contribute to the project. Some of these people are listed at the front of this report.

The Interim Report

The Identity Project's Interim Report was published on 21st March 2005. This report, which covered a narrow spectrum of issues, was released to support the debate on the Bill which went to second reading in the House of Lords on the same day. The Interim Report was widely quoted in that debate.

Whilst the feedback from the Interim Report has been overwhelmingly positive, the LSE team acknowledges the individuals and organisations that have provided constructive criticism of its content and delivery. This feedback has, where appropriate, been incorporated into this report.

Government Participation

The LSE and EPG have actively cooperated with all interested stakeholders throughout this project, including the Government.

Representatives of the Home Office Identity Cards Unit were invited to the first three Expert Panel meetings. The Unit accepted the invitation to the first meeting a matter of hours before it began, leaving no time to ensure that the Government would be fairly represented, and by mutual agreement the Home Office representative withdrew. No Home Office representative was available for the second meeting.

The results of the first two meetings were forwarded to the Home Office, and all meeting results have been published on the Internet.

In the House of Lords second reading debate on 21st March 2005, Baroness Scotland stated that:

> "My Lords, first, as I made absolutely clear, we will read the report and consider its findings as everyone has suggested. Secondly, throughout the passage of the Bill it has been clear that the Home Office has been assiduous in trying to ensure that, wherever possible, we or our officials have attended meetings, engaged in consultation and given briefings. I do not know the history regarding the LSE but I can assure the noble Baroness that consultation is one thing on which we seem to have excelled on this Bill, as on so many."[2]

The Home Office agreed to send a speaker to the third meeting, held on 23rd March 2005, but due to illness that speaker withdrew on the day, and no replacement was available.

An Enterprise Privacy Group representative met with the Identity Cards Unit on 12th May 2005 to discuss the findings of the Expert Panel meetings. The meeting was good-natured and productive, but the Home Office did not respond to further offers to engage them in the project.

[2] Hansard, 21st March 2005

Since that time, there has been a single telephone conversation between representatives of the Identity Cards Unit and the LSE, but at the time of publication the two parties have not met.

Alternative model consultation

On 5th June the LSE published the draft blueprint of its alternative national identity cards model. The purpose of this exercise was to provide an opportunity for public debate and input. A number of constructive responses were received, and these have been taken into account in the final publication of the model in this report.

Ongoing Work

This report does not mark the end of the Identity Project, but rather another milestone in the development of a preferred architecture for the National Identity scheme. The LSE team will continue to develop its ideas, and there will be further Expert Panel meetings over the coming months.

4

Overview of the Legislative Proposals

The Identity Cards Bill outlines an identity system that has eight components: the *National Identity 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 the 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 Identity 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.[3] 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 took place on 21st March, after which the Bill was suspended pending the general election.

A revised version of the Bill was presented to the House of Commons on 25th May. The revisions, which are generally minor, are as listed by their relevant clauses below:

- 1(h) deleted to remove the power to store old addresses;
- 1(6)(c) now contains a reference to gender in the definition of an individual's identity;
- 2(4) now includes a safeguard to only add individuals to the National Identity Register when their details are known (eg failed asylum seekers) if "the Secretary of State considers that the addition of the entry to the Register would be consistent with the statutory purposes.";

[3] Identity Cards Bill (as amended by Standing Committee B), http://www.homeoffice.gov.uk/comrace/identitycards/.

- The original 2(5) has been removed, taking away the power of the Secretary of State to "modify the Register for the purpose of correcting information ...";
- Changes to age of enrolment being an affirmed statutory instrument in 2(6) and 2(7);
- 4(3) now requires an affirmative statutory instrument for document designation;
- 9 has been reworded to remove the explicit reference to clause 6, which provides the power to compel an individual to renew a compulsory registration;
- The crime of not notifying the Secretary of State of a lost/stolen/damaged/tampered/destroyed card, or not surrendering a card, as defined in clause 13, has been redefined as a civil penalty not exceeding £1,000;
- 19(4) updated to refer to "Her Majesty's Revenue and Customs", rather than "Inland Revenue" and "Customs and Excise";
- The reference to disclosure from the National Identity Register to government agencies without consent in clause 19 now includes Jersey Police and Guernsey Police;
- Clause 22 (disclosure from the National Identity Register to other users without consent) now refers to "provide a public authority with information", instead of "provide a person with information", explicitly excludes provision of the audit trail ("paragraph 9 of Schedule I"), and now includes (as a new clause 22(2)) a public interest requirement;
- Clause 23 (which governs the creation of any power to disclose without the data-subject's consent) now requires affirmative statutory instruments, not non-negated ones (as a new clause 23(6));
- Clause 24 has the word "any" deleted from 24(2)(a) and 24(2)(b);
- The Commissioner's powers no longer exclude (sic) "the imposition of civil penalties" or "objections to such penalties" (clause 24(3)(b)), nor does it now exclude (sic) the operation of the clauses dealing with the Commissioner (so the Commissioner can now complain of censorship) (clause 25(3)(f));
- The powers now exclude the operation of clause 39 ("verifying information provided with passport applications");
- A new clause 24(7) refers to the Freedom of Information Act, listing the Commissioner under Part VI ("Other public bodies and offices: General") of Schedule I ("Public authorities");
- Clause 25(4) has reduced what the Secretary of State can redact from the Commissioner's report. In place of anything that "would be prejudicial to national security, the prevention or detection of crime or the continued discharge of the functions of any public authority, or would be otherwise contrary to the public interest", the Bill now refers to anything that is "prejudicial to national security or the prevention or detection of crime";
- The amendment of the Police and Criminal Evidence Act in the original clause 32(1) has been removed (making possession of a false document, disclosure of information from the National Identity Register and providing false information to the National Identity Register no longer Arrestable offences);

- On civil penalties (clause 33(6)), the Bill now states that "In proceedings for recovery of a penalty ... no question may be raised as to ... the amount of the penalty.";
- Clause 34(1)(b) has been added, making it possible to "give notice to the Secretary of State that [the defendant] objects to the penalty [on the grounds] that the circumstances of the contravention in respect of which he is liable make the imposition of a penalty unreasonable". The same grounds have been added to appeals in clause 35(1)(b);
- Clause 37 (Fees in respect of functions carried out under Act), now has a new subclause (part 6) reading "References in this section to expenses that will be incurred for any purpose include references to expenses that the Secretary of State considers are likely to be incurred for that purpose over such period as he thinks appropriate, including expenses that will be incurred only after the commencement of particular provisions of this Act.";
- Clause 40, dealing with amendments to references to "passports" in other legislation, has been modified to remove subclause 1, meaning "a valid ID card ... which records that [someone] is a British citizen" would no longer be proof of right of abode under the Immigration Act 1971;
- Clause 41 (Orders and regulations), has a new subclause 5, which deals with powers to authorise or require "anything to be done by or in relation to an individual under the age of 16", and allows someone to be designated to act on the child's behalf;
- Clause 45 has had the reference to the Serious Organised Crime Agency removed.

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 Identity 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.

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[4] for the Bill.

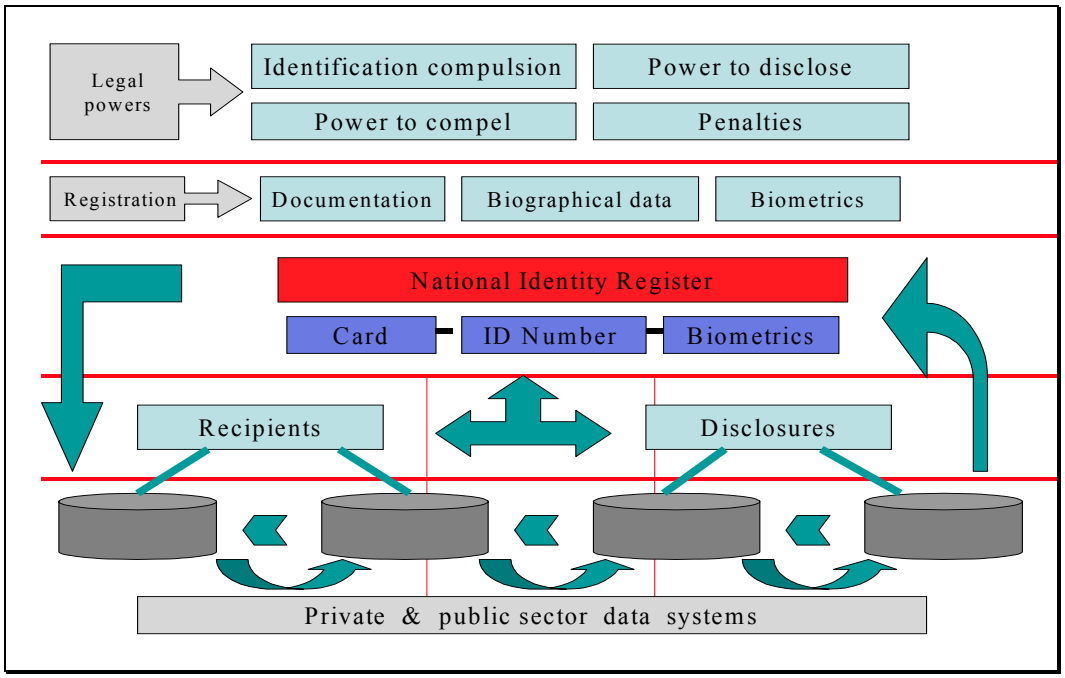


Figure 1 – Overview of the complexity of the scheme

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

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

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,[5] to gain access to health,[6] 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. This could include operating a bank account, using professional services[7] 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[8] 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."[9] 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."[10]

---

[5] '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/.

[6] '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.

[7] 'New client? ID card please', Accountancy Age, December 2, 2004, http://www.accountancyage.com/news/1138822.

[8] '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.

[9] 'Talks consider use of ID cards for business', James Watson, Computing, December 1, 2004, http://www.vnunet.com/news/1159786.

[10] 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.

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[11] in November, resulting in a robust response[12] 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 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, HM Revenue & Customs and the Department for Work & Pensions.

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

[11] Rt. Hon David Blunkett, Speech to the IPPR, November 17, 2004, http://www.homeoffice.gov.uk/docs3/identitycards_041118speech.htm.
[12] 'Blunkett concern on loyalty cards', BBC News online, November 17, 2004, http://news.bbc.co.uk/1/hi/uk_politics/4018939.stm.

Bill was published in November 2004 the government acknowledged that the cost[13] 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[14] 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 £93. An ID card without a passport will on current estimates cost[15] between £35 and £40. There will be a charge for the renewal or replacement of cards.

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 Identity 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

[13] '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

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

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

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[16] 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."[17]

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[18] 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[19] 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[20] by the Parliament's Joint Committee on Human Rights[21] 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:[22]

---

[16] Home Affairs Committee, Fourth Report, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm.
[17] '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.
[18] Legislation on identity cards: a consultation, Home Office, http://www.homeoffice.gov.uk/comrace/identitycards/publications.html.
[19] Action on Childrens Rights, http://www.arch-ed.org/chldrnbill.htm.
[20] '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
[21] Joint Committee On Human Rights - Nineteenth Report, http://www.publications.parliament.uk/pa/jt200304/jtselect/jtrights/161/16102.htm.
[22] House of Commons, Hansard, July 3, 2002, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo020703/debtext/20703-07.htm

> "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 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)).

5

The Government's Consultation Process

The Identity Cards Bill is a significant legislative and technological initiative. It has the potential to transform government systems, the relationship between the individual and the state, and develop technology at an unprecedented scale. Developing a policy of this type requires consultation, which builds confidence by allowing individuals and organisations to engage development of the project. A consultative process also facilitates the creation of a more informed policy.

The policy idea of an identity or entitlement card first emerged a number of years ago. Over this period the Government has solicited input through a number of consultation processes. As early as 2002, David Blunkett stated that consultation was an integral process to the establishment of the card:

> "I have made it clear that the introduction of an entitlement card would be a major step and that we will not proceed without consulting widely and considering all the views expressed very carefully. I want to see a far-reaching and meaningful public debate on the issue of entitlement cards, and a vigorous response from all parts of the community."[23]

The consultation process was intended to inform the policy. According to David Blunkett in 2003:

> "The House will know that since making my statement I have been consulting widely on, for instance, issues relating to secure verification and identification."[24]

With sufficient consultation on the logistics, the Government felt that it was appropriate to introduce a draft bill for consultation. At that time, the Prime Minister argued:

> "In relation to ID cards... I think there is no longer a civil liberties objection to that in the vast majority of quarters. There is a series of logistical questions, of practical questions, those need to be resolved,

[23] 'Blunkett unveils ID card proposals', *The Guardian*, July 3, 2002. http://www.guardian.co.uk/humanrights/story/0,7369,748527,00.html. Also 'ID cards: Blunkett reveals the 'entitlement card'', by Andrew Woodcock, *The Independent*, July 3 2002: http://news.independent.co.uk/uk/politics/story.jsp?story=311490.

[24] Hansard, November 11, 2003, available at http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo031111/debtext/31111-04.htm#31111-04_spmin2

> but that in my judgment now, the logistics is the only time delay in it, otherwise I think it needs to move forward."[25]

However, some contention arose. The Home Affairs Committee report in July 2004 differed from the consultation differed from the Government's stated view:

> "The Home Office is taking decisions about the nature of the card without external assessment or public debate."[26]

When the Bill was first presented to the Parliament, the consultation session was again at issue. In the second reading in the House of Lords, the Government was asked if it would work with the LSE. This followed speeches by a number of Lords during which the interim report had been commended to the House. The response from Baroness Scotland again heralded the consultation process:

> "[T]hroughout the passage of the Bill it has been clear that the Home Office has been assiduous in trying to ensure that, wherever possible, we or our officials have attended meetings, engaged in consultation and given briefings. I do not know the history regarding the LSE but I can assure the noble Baroness that consultation is one thing on which we seem to have excelled on this Bill, as on so many."[27]

It is therefore essential that we review the consultation processes to bring out the variety of comments, ideas and reports that contributed to the legislative process.

There have been three formal consultations with respect to entitlement/identity cards, relating to successive generations of papers and legislation. The first was "Entitlement Cards and Identity Fraud: a Consultation Paper", which was presented July 2002 with responses due January 2003.[28] Next came "Legislation on Identity Cards: a Consultation", presented April 2004 with responses due July 20th 2004.[29] In the meantime, the Home Affairs Committee took oral and written evidence from a variety of organisations, individuals, and private companies between December 11th 2003 and June 15th 2004; its report was published on July 20th 2004.[30]

The "Identity Cards Bill" was published on November 29th 2004 and was amended in the House of Commons Standing Committee B on January 27th 2005.[31] A slightly amended version was re-introduced into the new Parliament on May 25th 2005.[32] All of these documents are archived and publicly available in a special section of the Home Office's Web site.[33]

---

[25] 'Blair puts compulsory ID card on fast track for UK', *The Register*, April 2, 2004, available at http://www.theregister.co.uk/2004/04/02/blair_puts_compulsory_id_card/
[26] Home Affairs Committee, Fourth Report of Session 2003-2004, Volume 1, July 20, 2004.
[27] Hansard, House of Lords, March 21, 2005, available at http://www.publications.parliament.uk/pa/ld199900/ldhansrd/pdvn/lds05/text/50321-26.htm
[28] http://www.homeoffice.gov.uk/docs/entitlement_cards.pdf
[29] http://www.homeoffice.gov.uk/docs3/identitycardsconsult.pdf
[30] Home Affairs Committee Report.
[31] http://www.publications.parliament.uk/pa/cm200405/cmbills/049/2005049.htm
[32] http://www.publications.parliament.uk/pa/cm200506/cmbills/009/2006009.htm
[33] Reachable at http://www.identitycards.gov.uk or http://www.homeoffice.gov.uk/comrace/identitycards/index.html.

On February 3rd 2003, Beverley Hughes, Secretary of State for the Home Department, answered a Parliamentary question regarding government steps to publicize the entitlement card consultation. She listed the following activities:

- press release when the consultation document was published (resulting in national coverage);
- four more press releases for ministerial events; many briefings of national, local, and specialist media;
- 400 regional press packs distributed throughout the UK; and
- 10 ministerial appearances to debate on local radio, Channel 4, and BBC Radio 2.

She added

> "In addition to media activities to raise general public awareness, considerable effort has been devoted to providing information to key stakeholder organisations through officials preparing special summaries of the consultation paper, holding face-to-face meetings and giving presentations at conferences."[34]

The Home Office also says that its Identity Cards Programme team have attended conferences, meetings, and seminars, where they have gathered responses from private companies and other groups. A partial list of these was made public by Des Browne, Minister of State, Home Office in an answer to a Parliamentary question on January 27th 2005,[35] though no details were given.

The process was not always open or consistent. For instance, the Home Office sent Stephen Harrison, head of the Entitlement Cards Unit, to a 2002 meeting at the London School of Economics sponsored by Privacy International and featuring speakers such as Peter Lilley, *Daily Telegraph* editor Charles Moore, Professor Ross Anderson, and other technical experts, civil liberties advocates and politicians.[36] The Home Office declined, however, to send anyone to a second, similar meeting held in 2004.[37] The Home Office has declined to provide information in response to a Freedom of Information Act request requesting detailed information about the activities of the Home Office Identity Cards Programme team, citing an exemption under Section 35(1)(a) of the Act, "the formulation and development of government policy".[38]

Throughout the consultation process, the government has cited opinion polls showing that approximately 80 percent of the public supported ID cards. Stand.org.uk set up a portal to make it easy for people to send their comments to the Home Office and to their

[34] Hansard, February 3, 2003, Available at http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030203/text/30203w20.htm#30203w20.html_wqn5
[35] Hansard, January 27, 2005, available at http://www.publications.parliament.uk/pa/cm200405/cmhansrd/cm050127/text/50127w08.htm#50127w08.html_spnew7
[36] 'Public Meeting on the Government's Proposed 'Entitlement Card'', December 11 2002: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61892
[37] 'Mistaken Identity', May 19 2004: http://www.privacyinternational.org/conference/missingid/
[38] The progress of this request is being tracked at http://www.spy.org.uk/foia/archives/foia_requests_in_progress/ho_identity_cards_programme_meeting_diaries_agendas_minutes_expenses_etc/index.html.

MPs. After a couple of weeks, Stand collected 5,031 emailed responses, of which 96.5 percent were opposed and 1 percent of responses were in favour of ID cards.[39] Yet in its summary of the individual responses to that consultation, the Home Office claimed that 61 percent of responses had been positive, apparently counting the Stand responses as a single "inspired" response arising from an "organised campaign".[40]

Many of the same organisations contributed comments and/or testimony to all three formal consultations, often making similar points. Many of these are not reflected in the final legislation. For example, a number of the technical organisations such as the IT industry trade association Intellect, the British Computer Society, and independent technical experts have warned that the cost and success of such an extensive IT project cannot be controlled without a careful specification of the system. Some remain concerned that the final legislation still lacks detail in this area.

It is not only technical experts who have complained about a lack of detail. The Confederation of British Industry said in testimony:

> "This is a step towards tackling identity theft, which is an increasing threat to companies and consumers, estimated to be costing £1.3 billion a year. However, firms have concerns about the potential impact of a national identity registry. They want to know more about the types of data it will store and how the government will assure accuracy and integrity of information. So far plans have been vague."[41]

In its August 2004 response to the draft bill, the CBI also said,

> "…there is doubt as to whether the actual details of the scheme envisaged by the Government provide a means of authenticating identity that is sufficiently robust, refined and systematic that it can and will be trusted and actively supported by individuals, government departments and businesses. The key area that needs to be clarified by the government in this regard relates to the national registry, the data that it will contain and the way in which data on it will be shared amongst government departments and businesses. Furthermore, the extent to which the proposed scheme can benefit rather than undermine procedures for information security and identity authentication already developed by business remains unclear.

[39] 2.5 percent of these emails were suspected as duplicates and discarded.
[40] 'Home Office 'ignored opposition to ID cards', Ros Taylor, *The Guardian*, November 21, 2003, available at http://politics.guardian.co.uk/homeaffairs/story/0,11026,1090273,00.html.
[41] CBI Statement, available at http://www.cbi.org.uk/ndbs/press.nsf/0363c1f07c6ca12a8025671c00381cc7/57642043e78ce9c28025700400325ab8?OpenDocument.

> The CBI is therefore sceptical as to the positive benefits the scheme outlined in the draft Bill will have for addressing security and ID concerns."[42]

On May 25, 2005, the CBI told *Computer Weekly*,

> "If business support is to be maximised, the bill must offer greater clarity and transparency. Without this, it is likely to fail in its objective of making the UK a more secure place to live, work and do business."[43]

Qinetiq, the former government defence research organisation, has criticised the plans as too complex and too expensive.[44] In written evidence to the Home Affairs Committee, Qinetiq said,

> "The concept of a National ID register held by the Home Office is too narrow and short term in its purpose and driven by passing events, not fundamental principles."[45]

Speaking at a briefing for journalists at the Royal Society, Neil Fisher, director of security solutions at QinetiQ, said the Home Office's rationale for implementing ID cards – to deter illegal working and tackle immigration abuse, and strengthen the country's security – was in his view all wrong.[46]

All of the consultations to date have produced concerns and observations regarding law, social exclusion and technology. A number of firms, experts, and individuals have raised similar concerns to those of the CBI and QinetiQ. Few of these have been reflected in the final bill. In fact, the government's plan for the ID card has changed little since the beginning of its gestation. The first consultation document, issued in 2002 using the term "entitlement cards", lays it out clearly on page 16 the architecture of the scheme:

- a central database ('the central register') capable of covering all of the resident population of the UK. The central register would hold core personal information which is commonly used by all service providers such as name and address;
- secure procedures for establishing entries on the central register and for keeping the information up to date so that

[42] Linked from the accompanying press release at http://www.cbi.org.uk/80256716004baae5/33a87f2eee41b54e80256803004f04e4/eba06badb02f983a80256ee600557828?OpenDocument.

[43] Computer Weekly, May 25, 2005, available at http://www.computerweekly.com/articles/article.asp?liArticleID=138665&liArticleTypeID=1&liCategoryID=6&liChannelID=28&liFlavourID=1&sSearch=&nPage=1

[44] ' ID card plans are too complex and too expensive, government is told', Bill Goodwin, Computer Weekly, February 14, 2005, available at http://www.computerweekly.com/Articles/2005/02/14/208309/IDcardplansaretoocomplexandtooexpensive%2cgovernmentistold.htm.

[45] http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we47.htm.

[46] 'UK 'not ready' for ID card scheme', Jacqueline Ali, BBC News, July 28, 2004, available at http://news.bbc.co.uk/1/hi/sci/tech/3933319.stm.

people would not have to provide the same information time after time to different service providers;
- links between the central register and information held on other systems by service providers so they could make efficient use of the information stored on the central register. The links would need to be designed so that information about specific entitlements (for example medical restrictions on a person's ability to drive) were not made available to other service providers without consent;
- the issuing of plastic cards to everyone on the central register. The cards may incorporate some information and features on a microchip embedded into the card. These are commonly known as 'smartcards'. The cards could provide a convenient way for people to prove their identity and their entitlement to services in some circumstances. In other circumstances such as when services are provided over the telephone, the card-holder's entry on the database would be the main way to prove identity and entitlement."

This is the exact same architecture in the bill today, despite three consultation processes.

For a more comprehensive analysis comparing the final bill introduced into Parliament in May 2005 and the first consultation document, see Table 2.

First consultation (2002-3)

In this first consultation, the cards were referred to as "entitlement cards" and the focus was on preventing identity theft, illegal working, and benefit fraud.[47] From the beginning, the government made it clear that it favoured something very like the system proposed in the final bill: database, smartcard with biometric identifiers, cross-notification, cross-linking.

The consultation document asked respondents to say how an entitlement/ID card could help them. For example, granted that retailers selling restricted goods such as cigarettes and alcohol must verify the buyer's age, an honest question would be to ask what form of document would be the most help in establishing this. Instead, the question was more frequently framed as "Would an ID card help?" The answer is clearly likely to be 'yes'. The ID card was not presented as one of several alternative possible solutions among which respondents might pick. The report notes that "most of Proof of Age stakeholders commented solely on point 14 of the consultation document". That is, they commented solely on the small portion of the proposals that applied to them.[48]

Similarly, organisations such as the Law Society and the Transport and General Workers Union pointed out in this and subsequent consultations that measures are in

[47] Past ID card proposals have focused on preventing football hooliganism (1988), truancy, drugs, and underage drinking (1990), and crime in general (1994).
[48] Consultation summary report, page 123.

place to prevent illegal working and this cause could more cost-effectively be served by more stringently requiring employers to use these.[49]

Even this early in the process, when nominally the government was consulting on whether an ID card should be brought in, and if it were, whether it should be plain cardboard or a chip-bearing sophisticated smartcard, it was clear which options the government favoured and that the key to the whole programme was the central database. This is reflected in some of the contemporaneous press reports.[50] A spokesman from the Home Office told *Silicon.com* in May 2002, two months before the consultation paper was published, that if the entitlement card project went ahead it would "follow the same format as asylum entitlement cards".[51] Those cards are smartcards including photographs and fingerprints.

A large part of this first consultation showed disagreement among respondents over issues such as whether medical information should be included on the card, whether address information should be displayed, and some of this fed into the policy, though not directly. For example, the results of the consultation indicate that people thought 'identity card' was a more accurate description than 'entitlement card', and that some thought describing the card otherwise was dishonest. The government did change the name to 'identity card' in subsequent consultations and in the legislation, but gave the reason that "people prefer it."

Home Affairs Committee consultation (2003-2004)

The Home Affairs Committee heard testimony from a number of organisations and technical experts. Many of those who were consulted were critical of the government's plan, in part because of the long history of cost overruns and failures in large government IT projects.

One particular concern that emerged was the lack of flexibility in the Government's thinking regarding the technology. Technical experts such as Professor Ross Anderson, a security engineer at Cambridge University and chairman of the Foundation for Information Policy Research (FIPR), and Professor Martyn Thomas, representing the UK Computing Research Committee, argued that ID cards and privacy need not be unable to coexist. They raised the example of Germany, where the ID number is changed whenever a card is replaced, making impossible many of the potential abuses of a giant database keyed by a single, lifelong number.

This led to the HAC criticism that the Home Office was not truly consulting on the technical decisions.[52] The HAC concluded in its report that:

[49] Ibid, page 131.
[50] See for example 'Heading for an identity crisis?', Barbara Nielsen, *IT Week*, October 8, 2003, available at http://www.itweek.co.uk/2086001. Also 'net.wars: A highly organised minority (that can be safely ignored)', by Wendy M. Grossman, *The Inquirer* and *NewsWirelessNet*, July 11, 2003, available at http://www.theinquirer.net/?article=10441 or http://www.newswireless.net/index.cfm/article/471.
[51] 'National ID card plan slammed', Heather McLean, *Silicon.com*, May 15, 2002 available at http://software.silicon.com/security/0,39024655,11033371,00.htm.
[52] HAC Report, Page 5.

> "There should not be a central database holding all individual information but the identity card should enable access to all Government databases."[53]

HAC also concluded that although it concluded that identity cards could make a significant contribution to problems such as illegal working, fighting organised crime, terrorism, and identity fraud, and establishing entitlement to public service:

> "However, the introduction of identity cards carries clear risks, both for individuals and for the 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."[54]

The Home Secretary released a press release in response.

> "I am pleased that the Home Affairs Select Committee report confirms that the Government's plans for a compulsory ID cards scheme will deliver real benefits, in particular making a significant contribution to tackling organised crime, terrorism, illegal working and illegal immigration. They also make clear that they believe that 'it is possible to deliver the project on time, to specification and to cost'."[55]

He went on to defend the lack of detailed information about procurement:

> "I do not accept that it is appropriate to release detailed, market-sensitive information about the financial and contractual aspects of the scheme at this stage. I understand the desire for more information, but we need to balance this with our duty to ensure we get the best value for money for the taxpayer."

No further detail has been forthcoming.

Second consultation (2004)

The results of the 2004 consultation were published as "A Summary of Findings from the Consultation on Legislation on Identity Cards" in October 2004.[56] Almost simultaneously *The Daily Telegraph* broke the news that the Home Office was recruiting a marketing manager to sell the benefits of compulsory identity cards, even though legislation had yet to appear before Parliament.[57]

---

[53] HAC Report, Page 4.
[54] HAC Report, paragraph 280 (page 68).
[55] 'Response to Home Affairs Select Committee Report on Identity Cards', Home Office press release issued July 30 2004: http://www.homeoffice.gov.uk/n_story.asp?item_id=1047
[56] Available at http://www.homeoffice.gov.uk/docs3/id_summary_doc_3.pdf
[57] 'Blunkett 'jumps gun' on ID cards', Philip Johnston, *The Daily Telegraph*, October 13 2004: http://www.telegraph.co.uk/news/main.jhtml;sessionid=ZYW41GUQOVHCVQFIQMFSM54AVCBQ0JVC?xml=/news/2004/10/13/nid13.xml&sSheet=/news/2004/10/13/ixhome.html&secureRefresh=true&_requestid=40982. See also

The majority of consultation responses were opposed to ID cards: 48 percent opposed; 31 percent in favour; 8 percent supporting in principle but with reservations about some aspects of the bill.[58] The Home Office also refers to general correspondence received during the consultation period, of which 21 percent was opposed and 31 percent were in favour. However, the introduction notes that:

> "Since July 2002 the Government has been engaged in a wide-ranging public debate about its proposals to introduce a national identity cards scheme. (…) During this first consultation period the Government also carried out an extensive programme of research into public attitudes towards identity cards. This showed an overall level of support at 79% (with 13% opposed and 8% unsure)."

In a separate survey of four ethnic minority groups, the government found that support for ID cards had increased since 2003 and a clear majority was in favour, as high as 84 percent among Chinese respondents. The report also claims that the benefits of biometrics were largely undisputed by focus groups set up to discuss the ID card.[59] However, according to the report over 70 percent of respondents in all categories were largely unaware of the term 'biometric information'.[60]

Although Prime Minister Tony Blair had said in Parliament in April that there were no longer civil liberties objections "in the vast majority of quarters", many organisations submitting comments in this round of the consultation process expressed opposition to ID cards and the national database on one or more civil liberties grounds. These organisations included Privacy International, Rethink, the Civil Service Pensioners Association, the Freedom Association, Justice, The Gypsy Council, Liberty, Stand, *Data Protection and Privacy Practice*, and many others, as well as individuals. Their concerns were numerous, including the invasiveness of the registration process (eg Justice) to concern that the ID card would create an underclass (eg Commission for Racial Equality) to the permanent alteration of the relationship between citizen and state (eg The Law Society).

Many more organisations expressed concerns about the marginalisation of specific groups. Many, including the Information Commissioner, wanted more detail regarding the scheme itself. This detail is so far not forthcoming.

By the time of the Prime Minister's statement, an entirely new organisation, No2ID, had been formed to campaign actively against the ID card proposals. Nonetheless, the government has characterised the opposition to the ID card as "a highly organised minority".[61] This is even though some of the opposition came from organisations such

---

'Blunkett 'arrogant' over ID cards', BBC News, October 13, 2004, http://news.bbc.co.uk/1/hi/uk_politics/3738760.stm.

[58] 'A Summary of Findings from the Consultation on Legislation on Identity Cards', page 12.

[59] Ibid, page 79.

[60] Ibid, page 87.

[61] 'ID cards for all to cost £40', David Cracknell, *Sunday Times*, July 6, 2003, available at http://www.timesonline.co.uk/article/0,,2087-736390,00.html. See also 'net.wars: A highly organised minority (that can be safely ignored)', Wendy M. Grossman, *The Inquirer*, July 11, 2003 available at http://www.theinquirer.net/?article=10441. And 'Now Blunkett wants to charge £39 for ID cards', by Drew Cullen, *The Register*, July 6 2003: http://www.theregister.co.uk/2003/07/06/now_blunkett_wants_to_charge/.

as the Law Society and the British Medical Association (BMA). In fact, the BMA stated in its response to the 2004 consultation document that it was concerned that ID cards may exclude vulnerable groups from treatment. They also worried that any health information included on the card would be inadequately protected, possibly allowing other agencies access to that information. The BMA did express support for the idea that the cards might help ensure that people using the NHS were entitled to do so, but did not want doctors and nurses to be required to police access to health services.[62]

A variety of other opposing views from the public included concerns about: privacy, costs, accuracy, function creep, biometrics, disclosure, racism, enforcement, applicability to foreign nationals, technological weakness, and ineffectiveness for the stated goals.

Consultation impact

The Home Office has frequently said that it has consulted widely. Each consultation report has summarised its efforts to comply with the rules for government consultations. In some areas of consultation – for example, whether or not medical information should be on the card – it seems to have genuinely weighed competing views and fostered debate. But in response the Home Office, in listing the 51 categories of information the database may hold, has ruled nothing out.

In terms of the main components of the legislation – the national database, the permanent identifying number, the biometric smartcard – the Home Office has not altered its proposals since the first consultation document was issued, back in 2002. This can be seen by examining the following table, which compares the key clauses of the original 2002 consultation document to the 2005 version of the legislation.

Table 1 – Comparison between the Government vision before and after consultation.

Element	Entitlement card consultation 2003	Final legislation May 2005
National identification register (the database)	"a central database ('the central register') capable of covering all of the resident population of the UK. The central register would hold core personal information which is commonly used by all service providers such as name and address" (p16)	Bill creates
Registration number (requires that every individual be given a unique number)	"Any card scheme would have to be administered by a database which would require each person registered on the system to have some form of unique personal number or identifier." (p 23)	Required for everyone entered in the Register
Biometrics (requires individuals to submit to fingerprinting and other means of identification such as facial or iris scan)	"Comments are invited on whether an entitlement card scheme should include the recording of biometric information with particular regard to the cost, feasibility and acceptability of the three most likely options (fingerprints, iris patterns and facial recognition). "The Government would like to hear the views of potential partners on how a nation-wide network of easily accessible biometric recording devices could be established and operated, how people who are not mobile or who live in sparsely populated areas could be served and what other value added services potential partners might offer." (p55)	Bill says "may be recorded". Regulatory impact assessment says "including biometric data".

[62] Available at http://www.bma.org.uk/ap.nsf/Content/IdentityCards

Card (generated from information in the register)	"Views are sought on what benefits issuing an entitlement card as a smartcard would bring to card holders, whether the use of a smartcard chip could be shared by a number of organisations effectively and whether any potential partners would be interested in managing the sharing of a chip on behalf of the Government." (p 56) Note that the lead-in material said the smart card would increase costs by 140% and need to be replaced within the 10-year validity period because the chip would degrade with use. The lead-in did lay out the case comparing plain cards, plastic cards, and smartcards, but this is not reflected in the consultation point, which is highlighted in colour. "it could be easier for card-holders to enrol for other services – joining a local library might be as easy as swiping a card at the library counter."(p55)	Included.
Legal obligations (requirement to produce the card in order to obtain public services)	"a card scheme could be used to verify access to particular services or facilities where there is a need to establish identity to a high degree of confidence for example benefit claims or obtaining a VAT Registration Number. (p17) "The card and the central register would therefore be used as a gateway to entitlement to these other services.(p60) "The sanctions for failing to obtain a card would depend on the uses of the card. In most cases the sanction would be denial of service, subject to the need to ensure that people whose cards had been lost or stolen could still receive services while waiting for a replacement." (p22) "Views are welcomed on whether an entitlement card scheme would allow for more efficient and effective delivery of Government services and what services people would most like to see linked to a card scheme."	Power granted to create regulations requiring same for cases where the individual is someone who is subject to compulsory registration. (S15) However, prohibits requiring ID card for access to services that must be provided free of charge or effectively making it compulsory to carry the card.
Administrative convergence (number and card used by variety of agencies and organisations)	"In particular the Government is examining the feasibility of developing a high-quality common population register, holding core data and a unique identifier on UK residents that could be used across the public sector. (p 25) "Views are invited on the development of a national population register which could be used in a sophisticated way across the public sector with the aims of improving customer service and efficiency." (p26) "Any entitlement card scheme would depend on effective information sharing arrangements." (p76)	Included in bill.
Cross notification (agencies notify each other of changes to a person's details)	"A common database would be indispensable for enabling more joined up and internet-based delivery of public services." (p25) "The common database would replace the core data held inaccurately on existing databases and could in time replace the electoral register." (p25) "All these databases would be linked to the central register to share only the core personal information." (p60)	Allowed under S21, S22.
New crimes and penalties (to ensure that people comply with the ID requirements)	"creation of criminal offences for making fraudulent applications for cards, fraudulent use of cards and counterfeiting of cards" (p21); "penalties for failure to notify changes to personal details for example change of address or change of name" (p21) create crime of identity fraud/theft (p44);	Creates (S27-33)
Compulsory	Asked whether should be voluntary or compulsory	Voluntary at first, with later move to compulsory registration

This leads us to the conclusion that the consultation process failed. A consultation process is supposed to generate discussion, feed into the policy process, make individuals feel as though they are part of the decision-making process, and to improve the quality of the policy through the solicitation of a wide spectrum of ideas, opinions, and facts. Although the consultation processes seem to have generated these ideas, opinions, facts and even a national discussion on the issues relating to a national identity

scheme, the Government has failed to listen to concerns and reflect the consultation in the eventual legislation. In essence, the policy was written three years ago, and little has changed since then.

A true consultation process would solicit alternative views, schemes, and architectures. It is surprising that all these years later we are still considering an architecture that is technologically problematic and perhaps hazardous.

6

National Security, Organised Crime and Terrorism

This objective has been subject to claim and counter-claim. On July 3rd 2002, in response[63] 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[64] 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[65] 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

[63] 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.
[64] '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/.
[65] 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.

> 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.
>
> 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"[66] 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[67] 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: "It (the ID system) does not stop it but it helps you police it and interdict it".[68]

[66] Home Affairs Committee, May 4, 2004, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/4050405.htm.
[67] '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.
[68] '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.

7

International environment and obligations

To date, the discussion on the relationship between the proposed National Identity scheme and Britain's international obligations has 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 identity card legislation is merely a harmonising measure, meeting international obligations, and is thus no different from 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. In doing so, the Government has failed to interpret international standards correctly, thereby 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.

The Government is, however, placing British citizens at a disadvantage. As our biometric passport programme will not be ready for the US deadline, Britain will be expelled from the US Visa Waiver Programme. This will result in all Britons being compelled to obtain visas in order to visit the US as of October 2005. It is our belief that a principal reason that the UK is behind on its obligations is that the UK Passport Service has expended vast amounts of its time on consideration of a strategy for identity cards, rather than on devising the means to adhere to actual international requirements. That is, by investing so much time in national registers, iris-scans, fingerprinting, the 'National Identity Agency' and even the Identity Cards Bill, the UK Passport Service has failed to do what was in fact required of it: the digitisation of photographs submitted by new applicants and their insertion within the passport.

Background to the international context

It is certainly true that many countries are moving towards enhanced identity infrastructures, with much of this activity 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 such debates.

Many governments are attempting to create in the public mind an assumption 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 longstanding initiatives that have previously achieved little momentum. Political and financial momentum was generated after terrorism had become a predominant concern.

This situation is best seen in the United Kingdom through the explanations of the desirability and financial viability of an Identity Scheme. 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 in order that 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."[69]

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."[70]

At the Labour conference in the Autumn of 2004, the Home Secretary asserted that if the Government could link the passport to an extended set of social protections, the costs of it would help to 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 our country, who is entitled to work, to services, to the

[69] '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.
[70] 'Blunkett pushes for ID card law 'in 18 months'', Andrew Sparrow, Daily Telegraph, April 26, 2004.

> 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."[71]

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 US 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, Germany and Spain who are now developing the issue of biometrics for travel inside and outside the European Union."[72]

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."[73]

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

[71] 'UK ID cards to be issued with first biometric passports', John Lettice, The Register, October 11, 2004.
[72] Home Secretary 'Identity Cards Speech' to the Institute for Public Policy Research, November 17, 2004, http://www.homeoffice.gov.uk/docs3/identitycards_041118speech.htm.
[73] House of Commons, Hansard, December 15, 2004, Column 1664.

> anyway. We should take the opportunity of that investment to secure wider benefits such as those I set out here."[74]

This line of reasoning concludes that biometric ID cards are inevitable. The Government is linking the Identity Cards Bill 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.

Having established 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 the way in which other countries are dealing with these same pressures, initiatives, and technologies.

Passport Standards: ICAO, the EU, and the US

Background

For a number of years the international community has co-operated in 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 passport information but, in the years that followed, little progress was made.

The US Government enlivened the process with the *USA-PATRIOT Act,* passed by the US Congress following the events of September 2001. This included a requirement that the President certify within two years a biometric technology standard for use in identifying aliens who sought admission into the US The schedule for its implementation was accelerated by a further piece of legislation: the *Enhanced Border Security and Visa Entry Reform Act 2002*, sections 303 and 307 of which 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)."[75]

The *Enhanced Border Security and Visa Entry Reform Act* created pressure on the Visa Waiver Countries[76] to institute new passports that include biometrics, and also generated momentum for the efforts of the ICAO to formulate a standard.

---

[74] 'ID cards defend the ultimate civil liberty', Charles Clarke, The Times, December 20, 2004.

[75] 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.

[76] 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.

ICAO Requirements

When the issue of biometric passports passed to the ICAO, the biometrics policy moved far beyond the Visa Waiver Program countries. As the international standard-setter for passports, the ICAO had begun research into biometric passports in 1995. During the subsequent decade, the performance of some biometric technologies has 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:

- compatibility with enrolment requirements
- compatibility with MRTD[77] renewal requirements
- compatibility with MRTD machine-assisted identity verification requirements
- redundancy
- global public perception
- storage requirements
- performance

The ICAO then assessed the available technologies, separating 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.[78] Intellectual Property issues hindered the acceptance of iris scans, whereas facial recognition was believed to

[77] Machine readable travel documents.
[78] 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.

be more socially acceptable. The ICAO felt that a single standard biometric technology that was used by all nations would ensure interoperability. This biometric implementation would merely require the inclusion of a digital photograph embedded on a chip within the passport.

Following a meeting in early 2003, the ICAO working group, in a somewhat surprising change of position, stated that:

> "ICAO TAG-MRTD/NTWG[79] recognises that Member States currently, and will continue to, utilise the facial image as the primary identifier for MRTDs [Machine Readable Travel Documents] 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."[80]

The ICAO was recognising that "some States may conclude it desirable to deploy two biometrics on the same document."[81] 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 a passport does not aid the travel of its citizens if it is only their home country that can 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 US does not record or verify iris scans. The inclusion of any additional biometrics is unnecessary for added international travel security. The additional biometric can only be of use to the British Government for possible domestic purposes.

The ICAO's new position has given rise to two conditions. Firstly, 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. Secondly, 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 US, there is nothing that would prevent the US, or any other country, from collecting and storing the totality of information on British visitors.

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

[79] Technical Advisory Group on Machine Readable Travel Documents and New Technology Working Group.
[80] ICAO, Report of the Technical Advisory Group on Machine Readable Travel Documents, Fourteenth Meeting, Montreal, 6-9 May 2003.
[81] ICAO, Machine Readable Travel Documents: Introduction, http://www.icao.int/mrtd/biometrics/intro.cfm.

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, States should have regard to the following consideration:

> "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:

> "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."[82]

The ICAO goes on to confirm that while central databases can facilitate additional security confirmation checks, they are not necessary. In response, the European 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."[83]

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."[84]

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.

---

[82] ICAO, Biometrics Deployment of Machine Readable Travel Documents: Technical Report, ICAO TAG MRTD/NTWG, May 21, 2004.

[83] 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.

[84] Privacy International and others, An Open Letter to the ICAO, March 30, 2004, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-43421.

EU Specifications and Actions

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, and 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 EU Council then pressed the European Parliament into hastening the policy through the Parliament in December 2004, without detailed consideration of the decisions made by the Justice and Home Affairs Council. The Parliament was informed by the Council that refusal to accept their demands would result in their 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.[85]

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

Some countries are refusing to contribute to this registry, making the situation far more complicated. Denmark has implemented new passports that do comply with US requirements as they contain a digitized photograph that is kept on a chip in the passport, although not in a central register. Switzerland and Sweden have acted in similar fashion. In Greece, the Data Protection Authority prevented the Government from implementing biometric checks at the borders, forcing it to abandon its plans for a biometric border system for the Olympics.[86]

The German Government announced its intentions to introduce a biometric passport that incorporates a digitised photograph from November 1st. Each time that the passport is read, a unique number will be generated, thus ensuring that the passport is read differently by every reader, and restricting the ability to generate an audit trail of

[85] 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.

[86] 'Biometric checks illegal in Greece, says Data Protection Authority', eGovernment News, November 11, 2003, http://europa.eu.int/idabc/en/document/1775/337.

activity. This protects against the creation of a national database with unique identifiers on every passport holder.

The passports will cost 59 euros, rather than the 23 euros originally cited,[87] and from 2007 every passport will also include two index-fingerprints.[88] This system is generating controversy, with the Federal Data Protection Officer going so far as to call for a moratorium on biometric passports.[89] In 2003 the German Government was warned by its Federal Information Security Agency (BSI) that biometric systems were ill-prepared for mass deployment.[90] In addition, experts doubt that the chips embedded within the passport can withstand the wear and tear of time.[91]

Ireland is moving towards the implementation of biometric passports, although it waited until the EU settled its affairs before moving forward with its own plans. The day after EU approval of its own 'standard', Ireland decided to introduce biometric passports. According to the Minister for Foreign Affairs:

> "The process will involve storing a digital image of the passport holder's face, taken from a photograph supplied by the applicant in the usual way. The information will be held by the Passport Office just as it now holds photograph records. As the data will be used only for passport purposes, there are no legal implications."[92]

Germany and Ireland are only collecting photographs, and only for the purpose of issuing passport documentation. As a result they are avoiding all the legal and technological challenges that the UK is currently facing as the UK Government insists on collecting multiple biometrics for the purpose of establishing a national register.

It is important to note that the United Kingdom is not bound by the EU specifications, yet the Government recently argued that it must comply with them. In the Parliamentary Briefing for the Bill, the Home Office stated:

> "the European Union has gone further and mandated both fingerprint and facial biometrics for Member States' passports within the Schengen area. The UK supports this move. The Government does not want British citizens to have 'second class' passports and will also be moving to incorporate fingerprint as well as facial image data in passports in the future to keep in step with our European partners."[93]

There is no requirement to 'keep in step' with Europe, just as there is no international requirement for additional biometrics. If the UK were to insist on just one biometric in its passport this would not create a problem; in fact the results would be to the

[87] 'Biometric passports are to cost 59 euros', Richard Sietmann and Craig Morris, Heise Online, June 2, 2005.
[88] 'Germany to Issue Passports with Biometric Data This Fall', John Blau, IDG News Service, June 2, 2005.
[89] 'Dispute about biometric passports heating up', Richard Sietmann and Craig Morris, Heise Online, April 21, 2005.
[90] 'Germany launches pilot of iris scan-based border control system', eGovernment News, February 20, 2004, available at http://europa.eu.int/idabc/en/document/2173/336.
[91] 'Germany unveils e-passport', CNN, June 2, 2005, available at http://edition.cnn.com/2005/TRAVEL/06/02/bt.germany.epassport.reut/.
[92] Dáil Debate, Written Answers, Volume 6000 No.1, April 12, 2005, available at http://debates.oireachtas.ie/DDebate.aspx?F=DAL20050412.xml&Dail=29&Ex=All&Page=38.
[93] 'Identity Cards Briefing', the Home Office, May 2005.

advantage of the UK, as it would reduce the costs and administrative burdens. Also, if the UK followed the US requirements for a single biometric, the UK certainly would not have to worry about having a 'second class' passport. Canada and the US have also rejected implementing additional biometrics in their own passports.

US Demands and Requirements

At this juncture it is useful to review the US requirements: the *USA-PATRIOT Act* requires only that the President, within two years, must certify a biometric technology standard for use in identifying aliens seeking admission into the US. 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.

Countries that fail to comply with the deadline 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 US would have to apply for a visa, creating chaos at US consulates and embassies. The Secretaries of State and Homeland Security appealed to the US 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 US would 'vote with their feet' and go elsewhere.[94]

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

The additional complexity that Europe and the UK are introducing to the passport is unnecessary. As a result, these countries will miss the deadline, to the disadvantage of their citizens who will now have to seek visas in order to visit the US. The Chairman of the Congressional committee responsible for the biometric passport deadline, James Sensenbrenner, has warned EU and UK diplomats regarding unnecessary complications.[95] According to one report, Representative Sensenbrenner expressed "dismay" that the European Union has gone further and mandated both fingerprint and facial biometrics:

> "The Border Security Act stipulated only that biometric identifiers and documents meet ICAO standards, and that the passport be machine-readable. (…) (T)hat the EU should choose an elaborate and

[94] 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.
[95] It is important to note that Sensenbrenner also penned the REAL ID Act.

> expensive path to meet the requirement has led to consequences that are regrettable, but not insurmountable."[96]

In a letter to the European Council, Sensenbrenner was even more explicit with his concerns:

> "While the added biometric element will strongly assist in confirming the identity of the passport holder, it further adds to the technical obstacles to completing the process and increases the cost of inspection infrastructure. (…) In my view, much expense and public consternation could have been avoided by a less technically ambitious approach, one that simply met the terms of the Act as written."[97]

Sensenbrenner also said that when Congress established the obligation and the deadline, it anticipated that the ICAO would establish: "reasonable, cost-effective standards which relied upon existing technology" rather than becoming: "enmeshed in new and unproven technology." Apparently the US Congress failed to anticipate the zeal of foreign governments.

In response to continued failures from other Governments to abide by the US requirements, the US recently announced that it was again moving the deadline by one year. By October 2005 all countries will still have to start issuing passports that contain digital photographs, though they are not required to implement chips in their passports until October 2006.[98]

Currently, the US appears ready to meet its own deadline. In order to comply with the ICAO standard, the US is implementing a biometric passport of its own.[99] However, the US, in compliance with the ICAO standard, is requiring only a digital photograph on a chip in the passport, and does not appear to be moving towards a database solution. There are indications of a struggle for more biometrics between the Department of State, normally responsible for passport and visa issuance, and the Department of Homeland Security. In one of his final speeches, outgoing Secretary of Homeland Security Tom Ridge regretted his inability to get all ten fingerprints included within US passports:

> "I for one believe if we're going to ask the rest of the world to put fingerprints on their passports, we ought to put our fingerprints on our passports. I mean you can go out to the rest of the world and say we'd like to engage you in this discussion. We'd like you to consider doing these things. I think you're in a much better position to discuss issues if you have made the commitment to getting them done yourself. (…) I think we ought to take the lead, and that's one thing I'll say publicly.

---

[96] 'Lawmaker Rips RFID Passport Plans', Kim Zetter, Wired News, May 4, 2005.
[97] Letter to His Excellency Luc Frieden, President of the European Council of Ministers and to His Excellency Franco Frattini, Vice President of the European Commission, from F. James Sensenbrenner Jr., Chairman of the House of Representatives Committee on the Judiciary, April 7, 2005, available at http://judiciary.house.gov/newscenter.aspx?A=473.
[98] 'DHS to Require Digital Photos in Passports for Visa Waiver Travelers', Department of State press release, June 15, 2005.
[99] US Department of State, Abstract of Concept of Operations for the Integration of Contactless Chip in the US Passport, April 2004.

> I think one of my recommendations to Mike is be aggressive, go after ten fingerprints on the passport. It's a lot easier to negotiate with your allies if you've already done what you're asking them to do."[100]

The Department of State resisted, and succeeded only in collecting digital photographs. When Secretary Michael Chertoff, Ridge's successor, gave a speech on the same topic to the same institution months later, he made no call for fingerprinting Americans, although he argued for expanding the practice for foreigners.[101]

While the US is photographing and fingerprinting all visitors under the US-VISIT program, it has decided against fingerprinting and iris-scanning its own citizens. This difference will be further emphasised in the future if the UK does implement an Identity Card. The US Department of Homeland Security has already appealed to the UK regarding its identity card: in May 2005, the Secretary Chertoff requested that the UK design its identity card to be consistent with the US standard on passports in order to permit the US to gain access to the data on the National Identity Register.[102] There will, however, be no reciprocity from the US Government because there is no such central register of personal information on Americans.

Meanwhile, some countries are going ahead with adding biometrics that may never be verified by other countries. New Zealand is planning to issue biometric passports by August 2005 and the chip on the passport will likely include a digital photo, and 'eye coordinates'.[103] Few other countries are implementing iris-scanning at their borders, thus it appears unlikely that border officials will have the required technology to verify New Zealand passports; however, this does not appear to be sufficient logic to prevent the New Zealand government from collecting iris-scans on all its citizens without any reciprocity from other countries.

Identity Systems in other countries

A number of countries are moving towards the inclusion of biometrics in identity cards, passports, and government databases; some are even waiting to see how the UK deals with the Identity Card Bill.

Recently the French Government announced its intention to include further biometrics on its ID card, citing "international obligations" from the ICAO to include fingerprints. The French even refer to the "new acceptance of ID cards in the UK" since the "law" of December 2004.[104] 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. These cases emphasise the importance of understanding

[100] 'Homeland Security: International Dimensions', Speech by Secretary Tom Ridge of the Department of Homeland Security to the Center for Strategic International Studies, January 12, 2005, available at http://www.csis.org/hs/050112_HomelandInternational.pdf.
[101] 'International Cooperation in Homeland Security', Speech by Secretary Michael Chertoff of the Department of Homeland Security to the Center for Strategic International Studies, May 19, 2005, available at http://www.csis.org/hs/050519_chertoff_transcript.pdf.
[102] 'US wants to be able to access Britons' ID cards', Kim Sengupta, The Independent, May 27, 2005.
[103] 'Cover comes off e-passports', Tom Pullar-Strecker, Stuff.co.nz, May 2, 2005.
[104] Ministere de l'Interieure de la Securite Interieure et des Libertes Locales, Le Programme INES, January 31, 2005.

the international dimensions to the Identity Card Bill: we must understand what other countries are doing, and the way in which our actions will affect their conduct.

Similar ID Plans

It is often said that the UK proposed ID-scheme is unprecedented. Although this is to some extent true, a number of other countries have implemented, or are implementing large-scale digital identity systems with similar characteristics, some involving the collection of biometrics. Issues arising in those countries may be of some relevance here, just as their experiences with the technology may inform our own practice. It is important to note that not all identity systems are equal.

Malaysia,[105] Singapore and Thailand are among the many countries establishing card systems. China is moving rapidly in this direction with the development of a compulsory ID database and card system,[106] although it abandoned the biometric element after it concluded that the technology was unworkable with large populations.[107] The US military in Iraq is developing a similar system to that proposed in the Identity Card Bill in order to control access to Fallujah[108] and to track those suspected of being insurgents.[109] The UN High Commissioner for Refugees has deployed an iris biometric system to control refugee traffic across the Pakistan-Afghan border.[110] The UAE also uses an iris system for border control.[111] Below, we will look into some systems in greater detail to understand the similarities and differences.

Bosnia

In 2002 the Government of Bosnia-Herzegovina moved to implement a national ID card, one of the goals being to reinforce the country's unity. It was to apply to all citizens over the age of 16.

The selected technology involves a card containing a bar-code, rather than a chip, plus a photograph, signature, and a single fingerprint. All the data is kept on a national electronic residents register, which is accessed over the internet.

Surprisingly, the system setup only took six months. It involved a network of 160 offices (including some mobile offices) to register residents, while the cards were issued centrally. Since then, 2.5 million ID cards and 1.5 million driving licences have been issued at a cost of 20 million euros.[112]

[105] Vericardsys Website information, http://www.vericardsys.com/MyKad.htm.
[106] 'China starts to launch second-generation ID cards', People's Daily, March 30, 2004, http://english.peopledaily.com.cn/200403/30/eng20040330_138863.shtml.
[107] 'Fingerprints Missing From Chinese National ID Card', Dan Balaban, Card Technology, September 11, 2003, http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030911CTDN261.xml.
[108] '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/.
[109] 'US forces issue hi-tech ID cards for insurgent suspects', Phil Sands, Gulf News, May 31, 2005.
[110] '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.
[111] 'Iridian Launches Expellees Tracking and Border Control System in UAE', Biometric Tech News, March 19, 2003, http://www.biometritech.com/enews/031903d.htm.
[112] 'Bosnia-Herzegovina pioneers biometric ID card', eGovernment News, December 3, 2003.

China

Since 1985 the Chinese Government has issued an ID card to every citizen. This card originally held relatively simple information, including nationality, birth date, ID number, and household registration information. Often this was issued and stored by the province.

In 2003 the Government passed a new law to update the ID card. According to one Public Security official,

> "The ID card and the ID number are mainly going to be used to verify a resident's identity, safeguard people's rights, make it easier for people to organize activities and maintain law and order."[113]

The new card contains a chip to store the additional information. Although DNA was considered as a biometric to be stored on the chip and in a database,[114] this was eventually rejected. Similarly, the Chinese did consider requiring a fingerprint but believed that it was too daunting to collect all this information, and they in any case doubted the reliability of the technology. According to an official at the Chinese National Registration Centre:

> "Such an effort to introduce biometrics, the huge quantity (of cardholders), is not feasible to start."[115]

Even the digitized photo on the chip will not be part of a facial recognition system. Information kept on the card can, however, be accessed by a reader held by both public and private sector organizations.

The public response to the new card was reported as relatively mute. It is believed that Chinese citizens were resigned to the collection of information by the Government. According to one professor: "[o]ur security officials already have all the information about us, anyway, so this is not a big change."[116]

From 2004 the Government began issuing a 'second generation' mandatory ID card involving contact-less chips. These chips contain very little storage capacity (4k), so information on the chip will be limited to name, gender, ethnicity, residence, and date of birth.[117]

Japan

The Government of Japan approved a change of a law regarding 'basic resident registers' in 1999. This involved the central government issue of an 11-digit number to all citizens and residents. Previously computerized resident registration information at local databases is now connected to the Resident Registry Network System, otherwise

[113] 'China Readies Super ID Card, a Worry to Some', David W. Chen, The New York Times, August 19, 2003.
[114] 'Chinese ID cards to carry genetic sample', Jo Best, Silicon.com, September 2, 2003.
[115] 'Fingerprints Missing From Chinese National ID Card', Dan Balaban, Card Technology, September 11, 2003, http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030911CTDN261.xml.
[116] 'China Readies Super ID Card, a Worry to Some', David W. Chen, The New York Times, August 19, 2003.
[117] 'China starts to launch second-generation ID cards', People's Daily, March 30, 2004, http://english.peopledaily.com.cn/200403/30/eng20040330_138863.shtml.

known as 'Juki Net'. In essence, Juki Net is a network of registries, each run by local governments.

Since the launch of Juki Net in 2002, it has been plagued with troubles. In the first year only 250,000 citizens signed up for the Juki Card,[118] while a number of local governments refused to connect to the system because of fears for personal information security. The government of the city of Yokohama, for example, at first refused to register its 3 million residents. When it finally decided to join the system, it allowed for citizens to 'opt out'.

In order to address security concerns, the Nagano Prefecture carried out a study employing a team of computer security experts and tested the system's security over the internet and local governments' internal LAN.[119] The study found that residents' information could be accessed and data could even be falsified, but the Government refused to agree that the system needed improvement.[120] One of the researchers involved in the study contends that the Government went so far as to censor a presentation he was supposed to give to a security conference in Japan on the significant failures in security that he had identified.[121]

A number of protests also erupted around the country upon the launch of Juki Net, as well as numerous court cases questioning the constitutionality of the system. In the first case to be decided on May 30th 2005, the court in Ishikawa prefecture ruled that individuals may not be required to agree to obligatory transaction of registered information through Juki Net because of the provisions of Article 13 of the constitution, that protect privacy. The court further ordered that the information of the 28 complainants be removed from the system: this decision prevents the Government of Ishikawa from sharing their information with the central Government. The Court also recognized that giving residents a numeric 'Juki Code' gives the central Government the ability to search and gather further personal information within their databases. It was felt that such powers could create a chilling effect among Japan's residents. The following day, however, another court in Aichi Prefecture ruled in favour of the system. Similar lawsuits have been filed in 13 different courts across Japan, challenging the collection of data for Juki Net. The confusion will not subside in the near future.

Hong Kong

Since 1949 Hong Kong residents have carried ID cards. In 2002, the Government introduced a new card that would include a smartcard. These are being deployed as part of a seven-year plan costing $400 million.[122]

The new card contains basic information on the individual, a fingerprint image and an ID number. The data is stored only on the card, not in a government database, but the legal regime behind the card allows the unrestricted use of ID numbers, thus still permitting the almost unrestricted use for the profiling of activities of individuals across

[118] 'Japan's National ID Card Falls Flat', CardTechnology.com, October 8, 2004.
[119] 'Japanese government, US security expert meet in court', Paul Kallender, IDG News Service, January 25, 2005.
[120] 'Free-speech suit filed against Japan', The Sydney Morning Herald, January 27, 2005.
[121] 'US security expert sues Japanese government', InfoWorld, January 25, 2005.
[122] 'Hong Kongers to get 'smart' ID cards', AP on CNN.com, March 11, 2002.

the public sector.[123] The Hong Kong Privacy Commissioner's smartcard Code does provide limited controls on the private sector use of the number.

The card system was designed from the outset as a multi-use card, with few limits and safeguards on its uses. In response to concerns regarding privacy, Hong Kong's Secretary of Information Technology and Broadcasting stated in January of 2002 that there "will be no more data on the surface of the card, than the data that already appears" and that:

> "… only minimal data will be stored in the card's chip. Except for essential immigration-related data and digital certificates, personal data in respect of non-immigration related applications will be kept at back-end computer systems of the concerned government departments. None of the proposed non-immigration applications (that is, using the card as a driving license and library card, storage of a digital certificate and change of address) will be mandatory. Cardholders will have a choice on whether to include the applications on the card."[124]

As concern grew regarding what could be stored on the card, the Government backed down on proposals for the cards to carry health and bank records. As the card is designed for multiple purposes, there is nothing restricting the Government from placing this information back on the policy agenda.

Malaysia

Malaysia has long had a national ID card, but in 2001 moved towards a smartcard scheme to replace both the older ID card and the driving licence. The card is called 'MyKad', or Malaysian Card.

The chip on the card contains a thumbprint and other personal information, including basic health information. It can be used to pay road tolls, to access automated teller machines and can also act as an electronic-purse.[125] However, banks have dissuaded customers from using the card for banking purposes.[126] The chip on the card originally had a 32k memory storage, but the next generation card consists of a 64k chip, which permits the storage of multiple certificates, issued for specific government services.

The card is issued at age 12 and re-issued at age 18. Children under age 12 are issued with a 'MyKid' card which currently does not contain a biometric, although the Government is now considering the collection of biometrics from new-borns.[127]

Malaysia recognises that it is leading the world on identity systems, and the Malaysian Government is willing to share its findings and technology. According to the director of the National Registration Department:

---

[123] 'Submission on the smart ID Card and the Registration of Persons (Amendment) Bill 2001', Professor Graham Greenleaf, University of Hong Kong Faculty of Law, October 28, 2002.
[124] C. Yau, Letter to the Editor, South China Morning Post, January 25, 2002.
[125] Unisys case study on The Government of Malaysia, available at http://www.unisys.com/public_sector/clients/featured__case__studies/malaysia__smart__card__.htm.
[126] 'Privacy of MyKad Holders to Be Protected by Law,' New Straits Times, May 19, 2004
[127] 'Malaysia to fingerprint all new-born children', John Oates, The Register, May 4, 2005.

> "A lot of governments including the US will be looking at better identification systems to monitor the movement of people within their countries after the terror attacks. We are willing to share our technology. It could be part of the solution to the security issue."[128]

To date, the Malaysians have only detected ten cases of forged cards, issued to illegal immigrants.[129]

Middle East

Throughout the Middle East, governments are introducing identity cards. Recently it was reported that Oman, UAE, Saudi Arabia and Israel are planning to issue 'smart' ID cards.

Oman is leading the region with its card programme. The cards will store a single fingerprint, and the police will be supplied with fingerprint readers to verify the cards.[130] They will be used for immigration management, particularly for workers from Pakistan, Iran, India, and other developing countries. The Government in Oman is also considering including multiple applications on the card, with the possible implementation of PKI.

Interestingly, information held on the card cannot be released to all government agencies, nor to the private sector.

Philippines

On a number of occasions, various administrations in the Philippines have attempted to introduce national ID cards.

One plan involved requiring Muslims in Manila to carry an ID card at all times, supposedly intended to detect terrorists hiding in Muslim communities. Although these measures were supported by the police and intended to be put into effect within one week, the plan disappeared from the agenda after a loud and widespread outcry against them by Muslim groups, politicians and civil liberties groups.[131]

An earlier plan attempted to establish a national ID card linked to a central database. In 1997, President Ramos issued Administrative Order 308, "Adoption of a National Computerized Identification Reference System." The Order met with widespread resistance. The Philippine Supreme Court invalidated the order and questioned whether the President could authorise such an identification system by mere executive order:

> "Assuming, arguendo, that A.O. No. 308 need not be the subject of a law, still it cannot pass constitutional muster as an administrative legislation because facially it violates the right to privacy. ...
> Unlike the dissenters, we prescind (sic) from the premise that the right to privacy is a fundamental right guaranteed by the Constitution,

[128] 'Malaysia pioneers smart cards with fingerprint data', Will Knight, New Scientist, September 21, 2001.
[129] 'MyKad too hi-tech to forge', Jane Ritikos, The Star Online, November 27, 2004.
[130] 'The Middle East Leads the Way in National ID Cards', Dan Balaban, CardTechnology.Com, March 20, 2004.
[131] That some sections of the Muslim community supported such a plan may make sense in the light of the constant harassment Manila Muslims have had to endure from police in their hunt for members of Abu Sayyaf.

> hence, it is the burden of government to show that A.O. No. 308 is justified by some compelling state interest and that it is narrowly drawn. ...
> Given the record-keeping power of the computer, only the indifferent will fail to perceive the danger that A.O. No. 308 gives the government the power to compile a devastating dossier against unsuspecting citizens."[132]

The majority declared the executive order as null and void.

Since 2002 there have been several calls by politicians, police and industry representatives for the introduction of a compulsory national ID card, one of the main arguments for such a system usually being its benefit in countering terrorism. Sceptics continue to point out that such a system would do nothing to stop terrorists, but other groups, such as the Integrated Bar of the Philippines, concentrate on ensuring the implementation of privacy safeguards in any future ID bill.[133]

The Philippine Social Security System already has a Smart-Card with fingerprint information stored digitally, but this card is not compulsory, and the fingerprints have not yet been used for computer-based matching.

The Bureau of Immigration and Deportation (BID) in August 2003 presented its plans for a biometrics-enhanced Smart-Card for all aliens resident in the Philippines. This was introduced as a counter-terrorist measure, as the Immigration Commissioner confirmed:

> "By adopting this new technology the bureau will be at par with other immigration centers around the world and, with proper coordination with international law enforcement agencies, it can now easily deter unwanted aliens from entering the country. The Philippines, being the closest ally of the United States, now becomes a tactical battlefield in war against Al Qaeda and other international terrorist cells."[134]

Besides the biometric data in the form of thumbprint templates and facial structure records, the "Alien Certificate of Registration Identification Card" (ACR-ICard) is supposed to contain personal information, criminal records and ACR payment transactions, as well as the date and time of a subject's arrival/departure.[135]

After a terrorist attack in February 2005, plans were re-introduced for a national ID card. The president signed another executive order calling for its implementation and Interior Minister Angelo Reyes pushed for the system as a solution to terrorism:

> "With a national ID system, you cannot claim to be somebody else because there will be one number for each person. (…) If you have nothing to hide, you have nothing to fear. There will be no curtailment

[132] Blas F. Ople, Petitioner, Vs. Ruben D. Torres, Alexander Aguirre, Hector Villanueva, Cielito Habito, Robert Barbers, Carmencita Reodica, Cesar Sarino, Renato Valencia, Tomas P. Africa, Head Of The National Computer Center And Chairman Of The Commission On Audit, Respondents, G.R. No. 127685, 1998.
[133] URL: http://www.ibp.org.ph/mainframe/pressrelease/pressrelease.php?id=27
[134] URL: http://itmatters.com.ph/news/news_08182003f.html
[135] ibid.

> of civil liberties. When terrorists attack, that's when civil liberties are curtailed."[136]

Although the exact details of the card remain to be known, there are indications that the Government of the Philippines is watching the UK process carefully.

Taiwan

For a number of years Taiwan has attempted to implement a biometric identity card. New national identity cards were to be issued as of July 1st 2005. In accordance with a 1997 Household Registration Law, these new cards were to include a fingerprint of all citizens over the age of 14. Premier Frank Hsieh argued that the programme would protect the human rights of all:

> "My commitment to human rights is no less than anyone else. (…) The principle of administration based on law restricts government (… and) in fact guarantees the human rights of the great majority of the people."[137]

The status of the fingerprinting programme came into question in April 2005 when the Cabinet actually decided to recommend its abolition to the President and the Parliament. Pressure against the Cabinet rose when the Interior Ministry purchased 9000 fingerprint scanners at an estimated cost of NT$500 million.[138]

In May 2005, Vice President Annette Lu launched a public campaign against the fingerprinting of all Taiwanese residents. She warned that fingerprinting was unnecessary because they are not decisive factors in solving criminal cases. She also argued that creating a database of fingerprints will likely create risks of computer crime. The vice president also argued that the requirement was unconstitutional:

> "The government's collection and storage of fingerprint records constitutes a collection of individual data and involves the questions of guarantees of the individual right of privacy and information autonomy."[139]

The Vice President was also concerned that the adoption of a fingerprinting programme would hurt Taiwan's international image as a democratic society. She predicted that Taiwan would "probably become an international laughing stock."

An alliance of over 100 human rights groups formed to oppose the programme. The ad hoc "Movement to Refuse Fingerprinting" includes as members the Taipei Bar Association and the Judicial Reform Foundation. Supporters were planning to apply for identity cards but will refuse to be fingerprinted. They would then lodge formal complaints with their local governments if they are then not issued with a card.

---

[136] 'DILG chief pushes national ID system against terrorism', Joes Fancis Guinto, INQ7.net, February 18, 2005.
[137] 'Premier promises to abide by justices' ruling on fingerprinting', Dennis Engbarth, Taiwan News, May 26, 2005.
[138] 'Vice president takes fight over prints to print', Dennis Engbarth, Taiwan News, May 24, 2005.
[139] Ibid.

Opposition parties claimed that the majority of Taiwanese supported the fingerprinting programme. According to one party leader, 70 percent of respondents to polls agreed with the programme.[140]

In June 2005, the Council of Grand Justices issued a temporary injunction to halt the programme. This was the first time that the Council had used this power.[141] The court froze the section on the collection of fingerprints, on grounds that the database of fingerprints would involve considerable administrative costs, and if the database was later found to be unconstitutional, these resources would be wasted. A final judgement on the constitutionality of fingerprinting is pending at the time of this report's release.

Thailand

During the 1980s, the Thai Government introduced the Population Information Network (PIN) to centralize in Bangkok all information held on individuals and households at provincial and district level.[142]

One of the current priorities of the Government is to replace that system with a chip-based smart-card capable of holding much larger amounts of data. When the Communications Ministry was finalizing its specification for the new ID Cards in January 2004, it was announced that the first major batch of the cards would be issued to citizens in the three provinces of Pattani, Yala, and Narathiwat from April that year.

The Government intends that the card should hold biometric information, and consideration is being given to what other information it should contain. There have been arguments over the inclusion of individual social security records, medical records and DNA profile, although the plan to include medical records and DNA information was eventually dropped, as was the indication of a card-holder's religious affiliation.[143]

The principal reason for the roll-out of this new technology in the troubled Southern Provinces can be found in the unease the Thai government feels about its Muslim-Malay population. Many people in the Patani region still have family-contacts across the border in Malaysia, and dual citizenship is a widespread phenomenon, though not recorded by either state. Thai officials have long complained that insurgents/ bandits can too easily slip across the border and find refuge in Malaysia, and they want to eliminate dual citizenship in the region. The Government now intends to create a DNA database of all suspected militants in the region, and of all teachers at private Islamic schools.[144] Both the Thai Law Society and the National Human Rights Commission (NHRC) have expressed concerns and pointed out that the collection of DNA samples must be on a voluntary basis.[145]

---

[140] 'Premier promises to abide by justices' ruling on fingerprinting', Dennis Engbarth, Taiwan News, May 26, 2005.
[141] 'Grand Justices suspend fingerprinting program', Dennis Engbarth, Taiwan News, June 11, 2005.
[142] For a full account of the Thai state's use of IT to control it's citizens, see: Pirongrong Ramasoota (1998): 'Information technology and bureaucratic surveillance: a case study of the Population Information Network (PIN) in Thailand' in *Information Technology for Development*, 8, pp51-64.
[143] The final word on what data to include on the chip has not yet been spoken though, since the winning bid to manufacture the cards was deemed to high and a new round of bidding for the contract meant a delay in their roll-out of over a year.
[144] It would also seem that one element in arresting such a large number of Muslim men in Tak Bai on October 25th 2004 was to collect DNA samples from all of them, as the forensics expert Dr. Pornthip Rojanasunan had been sent from Bangkok to Pattani specifically to collect DNA samples – before it transpired that so many detainees had died in custody. see URL: http://www.nationmultimedia.com/2004/10/28/national/index.php?news=national_15214003.html
[145] *The Nation*, 12/10/2004.

From July 1st individuals may apply for the new cards; everyone over the age of 14 must currently submit a full set of fingerprints when applying. Procedures have begun to test the constitutionality of the system.[146]

ID in Europe

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."[147]

There is a wide variety of identity systems in Europe, just as there is a wide array of concerns regarding the systems, and each country's domestic politics varies, just as their cultural values differ. German privacy law, for example, prevents a centralised registry of biometric information, while, according to one study, Polish citizens are not troubled by extensive databases; rather, they are more concerned about access to Government information [148] – but only recently has the German Government passed a Freedom of Information law.

Therefore one must be careful when drawing conclusions about the dynamics of identity cards within Europe. Below we will review some of the systems in some detail in order to examine these dynamics.

Belgium

In Belgium, cards were first issued in 1919 to anyone over the age of 12. They were renewable every 10 years. Recently the Government announced a new 'electronic' card that will cost almost three times as much – up to 15 euros per card. These cards will have to be renewed every five years, again leading to a rise in costs.

The Belgian Personal Identity Card (BELPIC) makes Belgium the first country in Europe to include a digital certificate in an ID card. The Belgian Government's goal is to enable citizens to carry out online secure transactions with government agencies, to access e-government applications, and to perform e-banking, or other private

[146] 'Wrong tack taken on ID card law', Wen-chih Lin, Taipei Times, June 5, 2005.
[147] Home Affairs Committee, Fourth Report, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm.
[148] 'A National Identity Card for Canada?', Report of the Standing Committee on Citizenship and Immigration, October 2003.

applications. Under current plans, every Belgian citizen will receive an identification card bearing his or her name and photograph, and two digital certificates, one of which can be used for authentication, the other as a digital signature for documents such as declarations or application forms.[149]

In February 2003, the Parliament approved the introduction of BELPIC, and the new cards were tested in 11 municipalities (*communes*) until September 2003. Following this, the government decided to roll out the cards to around nine million citizens by the end of 2006. Every Belgian citizen will be required to own an electronic ID card by the end of 2009.[150]

It appears that the Belgian Government is intentionally making spelling mistakes on its cards in order to confuse fraudsters,[151] which can only lead one to conclude that they accept that the card can be forged.

France

The French have a long history of identity documents, numbers, and markings. In 1832, the French stopped branding criminals, but the following year they implemented a central store of information on repeat offenders. In the 1800s all movement within the country was monitored through the use of internal passports, permitting police to follow the travels of migrants. Eventually this was abandoned on grounds of civil liberties in the 3rd Republic. But at the same time, the new Government invented a new identity card with a fingerprint and central records storage, implemented in the 1920s, though only in one French Department (Seine). This system was not implemented across the entire country due to strong resistance, mainly from the French Human Rights League, the CGT Union.[152] This changed under the Vichy regime. The system was then generalized and complemented by an identification number, together with the mandatory declaration of any change of residence address.[153]

In response to the fall of the Vichy regime, the card was changed in 1955 to remove reference to religious belief (particularly the tag 'Juif'). The central records-file was also abolished. In 1974 the Government decided to phase out the collection of the fingerprint, and began moving towards an optional card, where the holder's address had only an indicative value. This gradual reduction in the regime represents a stronger regard for civil liberties in the face of identity cards.

A first attempt to introduce a digitized ID card (originally promised to combat illegal immigration, terrorism, and identity theft) was halted in 1981 after a change of Government, but 1987 saw the introduction of a new identity card, made of plastic and designated as 'secure'.[154] This is the form of the current national ID card. It is not mandatory and, while a fingerprint is taken, it is not digitized and does not appear on the

[149] 'Privacy and Human Rights 2004', Electronic Privacy Information Center and Privacy International, October 2004, available at http://www.privacyinternational.org/phr.
[150] 'Price hike for Belgium's e-ID cards', Expatica, July 26, 2004.
[151] 'Belgians in cunning misspelt ID card plan', Jan Libbenga, The Register, May 26, 2005.
[152] Audition de M. Gérard NOIRIEL historien, directeur d'Etudes à l'Ecole des Hautes Etudes en Sciences Sociales (EHESS), presentation given to the Commission Nationale de L'Informatique et des Libertés, February 15, 2005.
[153] Audition de M. Pierre Piazza, presented to the Commission Nationale de L'Informatique et des Libertés, April 8, 2005.
[154] Décret n°87-178 du 19 mars 1987 portant création d'un système de fabrication et de gestion informatisée des cartes nationales d'identité. Journal officiel du 20 mars 1987, pages 3174-3175.

card. It is stored securely, and only on paper. While it can be accessed by a judge, in a specific case where the police already have a suspect, conditions for access are tightly regulated.[155]

A central database has been introduced, but it is limited only to the delivery of the card system. The information on the database is kept to a minimum, and apart from the information on the card, it includes information on the history of the card, though no audit trail of its use is generated. This information may only be accessed by those responsible for the management of the card system. Although the police may access information in the database, they are limited to accessing the name, sex, birth date, and card number, only in circumstances involving an offence.[156] The linking of one file with any other is disallowed. There are also strict rules regarding the reading of the cards: when read electronically, the card information cannot be stored unless it is for card management purposes. Contact with the central register is only permitted to verify whether the card has been stolen.[157] To this day, in France there are continued negative responses to the centralisation of personal information.[158]

Currently, there are two separate innovations planned for the French card. One is emerging from the Ministry of State Reform, the other from the Interior Ministry.

France I: 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.[159] The plans emphasises the need for user-friendly and accessible solutions that create a climate of trust.

In its plan to enhance e-government, the French Ministry of State Reform aims for a user-oriented system, allowing for multiple forms of identification. The emphasis is on simplicity and proportionality, and the amount of information collected will be minimised to increase the confidence of users. The French Ministry of State Reform 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 Ministry of State Reform is clear on how to resolve this conflict:

> "Government guidelines are clear: do not authorise uncontrolled generalised exchanges between departments. However, the

[155] Article 5, 'Décret n°55-1397 du 22 octobre 1955 : Décret instituant la carte nationale d'identité', available at http://www.legifrance.gouv.fr/texteconsolide/PQHEU.htm
[156] Article 11.
[157] Article 12.
[158] Audition de M. Gérard NOIRIEL.
[159] The French E-Government Strategic Plan (PSAE) 2004-2007, http://www.adae.gouv.fr/IMG/rtf/Le_plan_strategique-GB.rtf.

> 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)."[160]

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 :

Decentralised Storage of Data

The French Ministry of State Reform 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"[161]. Instead the French Ministry of State Reform 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

[160] Ibid, page 13.
[161] Ibid, page 15.

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

The French Ministry of State Reform 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.

France II: The Ministry of Interior Proposal

The interior ministry is at the same time proposing a completely different card. The project is entitled 'Identité national électronique sécurisée', or 'INES' project. It was officially announced in February 2005.

This system in many ways mirrors the UK's Identity Card Bill. The card will contain facial and fingerprint biometrics (2 fingerprints, among the 6 taken). These biometrics will be stored in a central database. As in the UK, the French Government asserts that this is inevitable because of international requirements from the ICAO to adopt a biometric passport, and adds that it should comply with the EU Council decision of December 13, 2004, which applies to countries party to the Schengen agreement.

There will also be a few variations on the UK proposal. The chip on the card is predicted to be a contact-less card, allowing card-readers to ascertain the information at a distance. The card will also be programmable, as the Government wishes it to become an electronic wallet. The Government is clear that it wishes this card to be made mandatory.[162]

Civil liberties groups have voiced numerous concerns regarding the proposal,[163] asking for clarification of the nature of the 'international requirements', and recalling imagery from the Vichy regime.[164]

Identity theft and fraud, particularly by terrorists, is given as one of the principal reasons for the new card system; however, a coalition of civil liberties groups, among them unions of attorneys and of magistrates, has pointed out that the French Ministry of Interior itself recognizes that France has no statistics to evaluate the scope and the nature of the identity theft phenomenon. The French Government relies only upon the statistics from the US and the UK.

The coalition also considers the argument that the cards would aid in combating terrorism to be merely 'an alibi', and points out that, in almost all of the most violent

[162] Public Declaration to the press by Dominique de Villepin, the then Ministry of Interior, April 12, 2005.
[163] 'INES de la suspicion au traçage generalise', Ligue des droits de l'homme, Syndicat de la magistrature, Syndicat des avocats de France, association Imaginons un reseau Internet solidaire (IRIS), intercollectif Droits et Libertes face a l'informatisation de la societe (DELIS), Association française des juristes democrates, May 2005, available at http://www.iris.sgdg.org/actions/ines/argument-petition-ines.pdf.
[164] Audition de Mme Meryem Marzouki, Présidente de l'association IRIS (Imaginons un réseau Internet solidaire), chargée de recherches au CNRS, presentation given to the Commission Nationale de L'Informatique et des Libertés, May 9, 2005.

attacks in France, the terrorists used their own identities. A similar conclusion was reached by the President of the French National Observatory of Delinquency, who considers that identity fraud: "remains quantitatively marginal in criminal matters, while it is increasing in the commercial sector".[165]

The proposal is likely to face significant scrutiny. When the Government first introduced this project, it opened up a consultation session. However, during this consultation process, it was announced that the policy had already been decided. A draft law was released and is under review by the CNIL, the equivalent to the UK Information Commissioner (although with far greater powers).

In June 2005 a consultative report was released by the Forum for Civil Liberties on the Internet ("Le Forum des droits sur l'internet").[166] This NGO was asked by then-Minister of the Interior Dominique de Villepin to conduct a consultation on the proposed scheme. The report found that the plans were overly vague, and therefore called for:

- better studies on identity fraud
- the decoupling of the project from the passport system
- studies on the risks of using a single identifier
- the responsibility for the project be shifted to the privacy commission
- the creation of a new social contract between the citizen and the state
- studies on the contact-less nature of the chip
- a clear statement from the Government on whether the card will be required for commercial transaction
- assurances that the card would be free at enrolment (though individuals could be charged for renewal or loss)
- a clear Parliamentary debate on the obligatory nature of the card.

A law implementing the system is likely to be introduced into the French Parliament in September 2005.

Germany

Germany provides one of the most interesting examples of identity cards. Most Germans readily carry around their identity cards but, because of past abuses, are also quite wary of the collection of personal information by the Government.

Compulsory registration began in 1938, and cards were introduced in 1950. It is not mandatory to carry the cards, although the police have powers to compel production of the card. From age 16, everyone is compelled to hold an ID card, and the only authentication required is a birth certificate.

Under Federal Data Protection Law, the Federal Government is forbidden from creating a back-end database of biometrics for the identity card. That is, German privacy law prevents the creation of a central database.

---

[165] Audition de M. Alain Bauer, Président du conseil d'orientation de l'Observatoire national de la délinquance, de l'Institut national des hautes études de sécurité, presentation given to the Commission Nationale de L'Informatique et des Libertés, April 12, 2005.

[166] 'Project de carte nationale d'identite electronique', un rapport part Le Forum des droits sur l'internet', 16 juin, 2005, available at http://www.foruminternet.org/telechargement/documents/rapp-cnie-20050616.pdf.

Instead, any information that is collected for the ID card system is stored locally at the registration offices. A private contractor, *Bundesdruckerei GmbH*, uses this information to issue the card, but as soon as the document is completed, all personal data is deleted and destroyed.[167]

No federal agency or private sector organisation can use the ID card number for registration. The scheme is organised at the level of the Länders (provinces), which collect the address, and details of secondary places of residence. This information is not protected by law because it is not considered private; as a result, it is made generally available for a fee.[168]

Biometric identification cards have not yet been developed. The German Prevention of Terrorism Act of 2002 includes a specific provision that biometric data in passports and ID cards may only be stored on the cards and not in centralised databanks. However, the Federal Government is pursuing the policy through the EU.

Data Protection authorities are concerned that a biometric system must meet some basic criteria. Firstly, the biometric data must not be used to gain other information about personal attributes (for example, reviewing photos in order to determine race). Secondly, individuals must know which biometric data will be stored and how it will be used. Thirdly, the biometric data should only be used for the purpose of identification. Finally, mechanisms must be put into place to ensure accuracy in the use of biometrics, and to prevent discrimination.[169] These criteria are simply a restatement of German privacy law.

The costs and feasibility of biometrics are an issue. The Federal Parliament's Office of Technology Assessment advised against complex systems involving centralised databases, warning of "a gigantic laboratory test", and varying costs. The report says that, depending on different scenarios and document features, 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 of systems for passports and ID cards.[170]

As there are other cards in use within Germany, including a separate card for access to health care, identity cards are not required for access to all public services. In May 2002, the Government announced plans for the development of an electronic universal healthcare card. The proposed card will contain, among other data, a patient's identification and emergency healthcare information. Patients will be able to use the card to fill prescriptions and disclose healthcare information to physicians on a voluntary basis.[171]

An interesting controversy arose surrounding a proposed "smart jobcard", envisioned for all employees in Germany. It was intended that data such as current employer, salary

[167] 'A National Identity Card for Canada?', Report of the Standing Committee on Citizenship and Immigration, October 2003.
[168] HAC report, July 2004.
[169] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, March 7-8, 2002, available at http://www.bfd.bund.de/information/DS-Konferenzen/63dsk_ent1.html.
[170] '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.
[171] 'Privacy and Human Rights 2004', EPIC and PI.

and working hours would be stored in a centralized database, which all social security departments could access, albeit only with consent. However, the Data Protection Commissioners have argued that this project constitutes a systematic data collection without a specific purpose, and therefore violates the right to self-determination expressed by the Constitution and jurisprudence. The commissioners also feared that the use of the social security number as a personal identification number would create serious privacy challenges.

Greece

In Greece, all individuals are compelled to carry cards because the police have the right to demand their production. Cards are issued at age 14, when the individual must register at their local police station, bringing along a birth certificate and a witness (often a parent). The police have argued that forgery and counterfeiting of the cards is quite rare because of the enrolment process.[172] The data collected in the enrolment process is sent to three Government departments and stored centrally, with the police maintaining control over the central database.

The situation is Greece is also very interesting because of the legal challenges to the information held on the cards. Since a decree in 1969, Cards have been required that include a photo, a unique number, fingerprint, surname, father's name, mother's name, spouse, place of birth, shape of face, blood type (optional), place of residence, profession and religion.

In 1986 the card was changed to include blood type and the status of the individual's military service; the freedom to withhold details of religion was also sanctioned. A further innovation occurred in 1991 when the Unique Code number of the Register was abolished.

In 2000, the Data Protection Commissioner called for a reconsideration of the items on the card. The Commissioner argued that a number of items were irrelevant and inappropriate, thus exceeding the purpose of processing, and called for the removal of:

- The fingerprint, as it is: "not necessary for the verification of the identity of the data since this is, in principle, evident from the photograph. In addition, according to the common perception, the fingerprint ("record") is associated with the suspicion or the ascertainment of criminal activity ("branded criminals");
- Spouse name;
- Profession;
- Nationality, as according to legislation only Greeks can bear cards;
- Residence, as it is likely to change; and
- Religion.

The Commissioner maintained that the processing of this information was "unlawful even if the data subject has given his/her explicit consent".[173]

[172] 'A National Identity Card for Canada?', Report of the Standing Committee on Citizenship and Immigration, October 2003.
[173] Hellenic Republic Authority for the Protection of Personal Data report to the Ministry of Public Order and Ministry of Internal Affairs, May 15, 2000.

Since that decision, the card no longer holds this information. More recently, the Greek Data Protection Authority prevented the Government from implementing biometric checks at the borders.[174]

Hungary

As with the situations in Greece and Germany, the Hungarian case is notable because of a particular legal case of 1991.

The State Census Bureau collected data on every Hungarian citizen. Each individual was issued with a personal number arising from this record, which was used to create a trail of his/her interactions with the State. A record was maintained on each citizen; this included: "basic personal identification and residential address data", and data on educational and professional qualifications. This information was collected in order to "gather data needed for a uniform basic personal record system", but lacked a clearly established purpose. The law enabling this system[175] also permitted the bureau "to utilize in the course of providing its services data obtained from other records – with the concurrence of the affected organizations." Such data could also be shared with other private persons and organisations.

In 1991, a case went to the Constitutional Court on a petition for judicial review. The Court found that under paragraph 59 of the Constitution, everyone has the right to protection of personal data. The collection and processing of personal data for arbitrary future use without a specific purpose is unconstitutional. Therefore, a general and uniform personal identification mark (personal number) for unrestricted use is unconstitutional.[176]

Italy

In Italy, citizens must agree to have their fingerprints taken and recorded in a database in order to be issued with a national ID card; however, a ministerial decree states that the association between the ID card and the fingerprint can be made only if expressly requested by the citizen.[177]

According to the Italian Privacy Commissioner:

> "identity cards continue to be part of Italian culture, even though they were introduced under the fascist government of Benito Mussolini in the 1930s. As such, many privacy issues that have been raised in the common law countries with respect to national identity cards do not have the same impact in Italy. However, he informed us that the proposed use of biometric identifiers has begun to raise some eyebrows. In particular, taking fingerprints is often, as in Canada, associated with criminality. Although the current national identity card has a blank spot for a voluntary fingerprint, the Committee was

[174] 'Biometric checks illegal in Greece, says Data Protection Authority', eGovernment News, November 11, 2003, http://europa.eu.int/idabc/en/document/1775/337.
[175] Decree with the Force of Law No. 10 of 1986.
[176] Hungarian Constitutional Court Decision No.15-AB of 13 April, 1991.
[177] Ministerial Decree of July 19, 2000.

> told that almost no one provides an imprint. Using fingerprints as the biometric identifier could provoke a negative response in Italy."[178]

A decree from the Council of Ministers in February 2004 called for a smartcard 'national services card', the aim of which is to boost internet-based e-government services. It will contain: identification data of the holder (name, date of birth, place of residence, etc.), a unique number identifying the card, the issuance and validity data, and the name of the issuing administration. This information will be both written on the card and stored on the card's chip, which will also contain a basic digital signature function and a container for qualified certificates.[179]

This smartcard is not the same as the electronic ID card. It does not contain a photograph of the holder, and therefore cannot be valid as a proof of identity. However, it is instructive to look at the challenges that the Italians faced in adopting this new card. They identified three principal problems: firstly, the process of standardising the smartcard without recourse to proprietary solutions; secondly, overcoming difficulties caused by the fragility of the microchips on the card; thirdly, uncertainty as to what information would be contained in the chip.

The Netherlands

Events in the Netherlands provide insight into the transformation of public opinion due to concerns of crime and national security, and into the challenges of enforcement.

Historically, the Dutch have been opposed to centralised government systems. In 1971 there was widespread resistance to the census: 268,000 people refused to comply with the census, despite threats of a substantial fine or a 14-day prison sentence. An even larger number of people entered false answers. Ten years later, a census was cancelled when polls indicated that resistance to it would be significant. Since then, the Government has pursued other forms of data collection, through the use of a national insurance number and databases of the national bureau of statistics. The national insurance number is used widely, and is even printed within passports.

The idea of a mandatory ID card was circulated a number of times in the 1980s. Successive Ministers of Justice concluded that there was neither sufficient support nor any proven need for mandatory carrying of the ID card.

In January 2005, the Dutch Government implemented the 'Extended Compulsory Identification Act', requiring compulsory identification for all individuals over the age of 14. Individuals are required to show identification to the police when asked, but are not required to carry identification at all times.

The law does not mandate a new identification card; the existing passport and driver's licence will be used instead. All three are valid ID documents. Drivers are warned that they should also carry their passport or ID cards with them at all times, as their licence may be confiscated after a car accident, leaving them vulnerable to fines if they are stopped.

---

[178] 'A National Identity Card for Canada?', Report of the Standing Committee on Citizenship and Immigration, October 2003.

[179] 'Italy to start distribution of e-government services cards', eGovernment News, May 12, 2004.

The costs of the regime are complicated. Many people are forced to buy an ID card, particularly if they do not have a passport or a driver's licence. This applies particularly to younger and older people. Anyone losing their ID card must pay a fine of EUR30. In addition, in order to ensure possession of a card at all times, it is necessary to pay EUR30 for next-day-service. As the card itself costs EUR30, losing a card can cost EUR90.

According to reports, the proposal is widely seen as a symbolic gesture to satisfy public concerns over crime and security. The Council of State, the highest legal advisory body in the Netherlands, strongly criticised the proposed law for the lack of any substantive evidence that it would help in the battle against terrorism.

According to the Dutch Public Prosecution Service, the ID checks mainly take place in specific circumstances:

> "ID control mostly occurs in situations of disorder or possible violence, for example at night in entertainment districts. Also in situations with an elevated risk of disorder, such as soccer matches, the police may verify the identity."

The Public Prosecution Service has indicated clearly that it wants to make an example of those who do not carry ID:

> "The main rule is there will be few escapes available for people who can't immediately present their ID. There is no right to an easy-going treatment, because it will in the end undermine the value of mandatory ID for law enforcement."[180]

Under the law, the police can demand an ID under any circumstance where the police think it is reasonably necessary. Frequently, it is demanded for minor offences such as using a bicycle without a light. The Public Prosecutor's guidance on the matter[181] outlines a few examples of a reasonable exercise of duty when 'maintaining the public order', including

- a car driving at night through an industrial park
- following a shooting on the street or in a bar when it is relevant for the investigation to determine the ID of possible witnesses
- if there is an unknown, new member in a group of known drug dealers
- where youths are causing nuisance in public space
- in the event of a fire, where it is suspected that a person amongst a crowd may have started the fire
- at events such as football and demonstrations in case of riots or the threat of riots
- in response to public unrest or disturbance, or threat of violence in popular night time districts, or at public events where there is a risk of disturbance of the public order.

[180] '3300 keer geen identificatie op zak', Openbaar Ministerie, February 2, 2005, available at http://www.om.nl/info/nieuws.php?p=pg&id=4358

[181] 'Aanwijzing uitbreiding identificatieplicht', December 7, 2004, available at http://www.om.nl/beleid/beleidsregel.php?vv=0&cid=1&rid=254

One notable case involved an elderly woman who used a pair of nail scissors to cut some twigs in nearby woods. Cutting twigs is forbidden, and she was spotted by a forester, who demanded her ID. Because she could not produce it, she received two fines; one for cutting the twigs, one for not showing ID. She burst out in rage and was given a third fine: for insulting an officer in the course of his duty.[182]

Within the first 24 hours of operation of the new Act, the city of Rotterdam issued 20 fines. In the first month 3,300 fines were issued to those who could not immediately show a valid ID when asked. During the following two months, the average rose to 5,300 individuals per month fined for being unable to produce their ID. After three months in operation, 15,984 fines had been applied, generating EUR800,000 in revenues for the Government.[183]

The law will be evaluated in 2008, at which point the police and all those with the same power to demand ID, such as park-wardens and environment control staff, will be consulted. There will be no consideration of the effect of the law on crime or terrorism. According to the Minister of Justice:

> "the law is part of a quantity of measures to enhance security in NL and reduction of crime and nuisance. The question if criminality and nuisance are reduced exclusively because of the law thus cannot be answered."[184]

There are indications that the police are not happy with the new law because it increases the amount of reporting that they must perform. They are also frustrated that they always have to find justification for stopping individuals.

Spain

Spanish ID cards were first introduced by General Franco, with the primary motive of controlling the populace. The primary motive now is to control illegal immigration.[185]

Application for the card requires a fingerprint. This is not on the card itself, although Spain is trialling a new card that would include it.

In 2003 it was reported that the Spanish were also trialling a social security smart card, containing a microchip with national identity number, medical information, and fingerprint access. Information on the chip could be accessed by health professionals using their own chips and a special reader. The project to develop and distribute 8 million cards was originally costed at EUR55 million.

---

[182] 'Identificatieklucht', De Volkskrant, 15 January 2005.

[183] 'Al bijna acht ton boetes id-plicht', Het Parool, April 13, 2005, available at http://www.depolitiebonden.nl/Nieuwsberichten/april2005/130405IDplicht.htm.

[184] Translated from 'De Wet op de uitgebreide identificatieplicht maakt deel uit van een veelheid aan maatregelen ter bevordering van de veiligheid in Nederland, en het verminderen van criminaliteit en overlast. De vraag of criminaliteit en overlast afnemen exclusief als gevolg van de Wet op de identificatieplicht kan derhalve niet worden beantwoord.' From Antwoorden op vragen van de Vaste Commissie van Justitie over de opzet van het evaluatieonderzoek naar de Wet op de uitgebreide identificatieplicht, April 28, 2005, available at http://www.justitie.nl/pers/kamerstukken/include.asp?bestand=/extern/documentportal/Brieven%20TK/20050428_5348798b%20uitgebreide%20identificatieplicht.doc.c

[185] 'A National Identity Card for Canada?', Report of the Standing Committee on Citizenship and Immigration, October 2003.

A Canadian Parliamentary Committee that travelled to Spain to observe their identity card scheme was surprised by the amount of information that is collected. When they discussed the invasive nature of the proposals and the problems of mass databases in Spain with the Spanish Data Protection Authority, they were disappointed by the:

> "evasiveness of data protection officials when questions were asked regarding the potential for data misuse by government departments or the state security apparatus. We were told that laws exist to protect personal data, but when probed further, officials were unresponsive."

In February 2004 the Spanish Council of Ministers approved a new card. It included:

- An electronic certificate to authenticate the identity of the cardholder.
- A certified digital signature, allowing the holder to sign electronically.
- A biometric identifier (fingerprint).
- A digitised photograph of the holder.
- A digitised image of the holder's handwritten signature.
- All the data that is also printed on the card (date of birth, place of residence, etc.)[186]

At the time, the proposal was criticized for the lack of Parliamentary debate on the issue, and the use of a Government decree to implement the system through an opaque process.

By the time that the project was approved, the predicted cost was EUR100 million over the next four years. The launch of a pilot system was delayed by one year, with the result that the new cards will not be ready for distribution until late 2007 or early 2008.[187]

Sweden

Identity cards in Sweden are not compulsory, but are helpful for interaction with government services and also to open a bank account. The card costs about £20, and is issued so long as your application is supported by a person already carrying a valid Swedish card who can vouch for your identity. Cards are issued by post offices and banks.

According to the HAC report, although there is no proper card in Sweden yet, all individuals must have a personal number and a record on the national register. Access to the register is tightly regulated. It has existed since the 17th century and, according to one report, was run by the Church until 1990.

There are plans to introduce ID cards with biometrics on them when the passports are updated. As in Denmark, the biometrics will only be on the chip, and the card will be merely for travel within Schengen, not for other purposes such as combating crime or identity fraud. It will not be compulsory to carry the card and, according to the HAC

[186] ''Spanish Government officially launches electronic ID cards', eGovernment News, February 16, 2004, available at http://europa.eu.int/idabc/en/document/2154/343.
[187] 'Introduction of Spanish electronic ID cards delayed', eGovernment News, December 10, 2004.

report, the card will not be linked to the register because of opposition on grounds of civil liberties.[188]

EU Initiatives

From the review of the cards in some EU member states, it quickly becomes apparent that there is a diversity of approaches to identity systems. Some countries have biometrics, some contain health information and some involve central databases. There is no common profile to all of these systems.

The European Union is working to minimize this variety. Through a number of initiatives, the EU is hoping to standardise cards of all types. All too often, this is effected through minimal debate, and even less awareness regarding the proposed policies. The passport policy is a prime example of this practice. As discussed above, the passport proposal received a bare minimum of analysis and debate within European institutions, and few therefore noticed the insertion of the requirement for fingerprints. Now member states are busy trying to implement not only the ICAO standards but also the EU requirements that were decided with minimal scrutiny.

EU Driving Licence

In another initiative, the EU is working to standardise the 110 different types of driving licences that are issued within Member States for Europe's 200 million licence holders. The new licence will involve a photograph on a smartcard. The policy was supported quite strongly by the European Parliament,[189] where the rapporteur for the legislation suggested that the new rules:

> "would be good for tourists, preventing the countries from applying restrictions to their driving licence. They will be also beneficial for fighting fraud, by creating a legal security system network in Europe."[190]

Some significant disagreements led to a simpler licence than originally envisaged. For example, some countries were keen to standardise policies on drivers aged over 65. The new standard will be rolled out over next twenty years.

The Hague Programme's Standardised ID

The most significant programme will also be the most influential. In November 2004, the European Council adopted a new multi-annual programme, entitled the Hague Programme; this builds on:

> "the ambitions as expressed in the Treaty establishing a Constitution for Europe and contributes to preparing the Union for its entry into force."[191]

[188] HAC report, July 2004.
[189] 'MEPs back EU driving permit', Henrietta Billings, EUPolitix.com, February 23, 2005.
[190] 'EU driving licence hammered out', Lucia Kubosova, EUObserver, February 24, 2005.
[191] 'The Hague Programme', Presidency Conclusions of the Brussels European Council, November 2004, available at http://europa.eu.int/comm/justice_home/news/information_dossiers/the_hague_priorities/doc/hague_programme_en.pdf.

It is intended that the Hague Programme will facilitate the establishment of agreed areas upon which Member States' ministers for Justice and Home Affairs wish to work at the EU level. The aim is to harmonise policies within the EU that can then be taken back to national parliaments.

Among the many policies within the Hague Programme, the Council called for "a coherent approach and harmonised solutions in the EU on biometric identifiers and data."[192] This was later elaborated as:

> "The European Council invites the Council, the Commission and Member States to continue their efforts to integrate biometric identifiers in travel documents, visa, residence permits, EU citizens' passports and information systems without delay and to prepare for the development of minimum standards for national identity cards, taking into account ICAO standards."

The European Commission then had the responsibility to develop an action plan; it identified ten priority policy-areas.[193] Under the priority of 'Internal borders, external borders and visas: developing an integrated management of external borders for a safer Union', the Commission has set a deadline:

> "In order to enhance travel documents security while maintaining full respect for fundamental rights, biometric identifiers will be integrated in travel and identification documents from 2005 onwards."[194]

This means that most of these decisions are likely to take place under the UK presidency of the EU, placing the UK in the awkward situation of being the only country with a Bill before its Parliament questioning the need for an identity card, even as it has the task of harmonising and standardising identity cards across Europe. It is the more challenging because the UK is not party to the Schengen agreement, and is thus under no obligation to adhere to the requirement for standardised identity documents.

An initiative that began as an EU policy of ensuring a coherent standard for driving licences has expanded incrementally to include visas, passports and residence permits for third-country nationals.[195] It has now reached a point where it is likely that the EU will decide not only whether any given member state will have ID cards, but also their form and structure.

ID in Common Law, Commonwealth, English-Speaking Countries

When a Canadian Parliamentary Committee reviewed the idea of a biometric identity card, it decided to conduct a tour through countries with ID cards. Following a visit to the UK, they moved on to mainland Europe:

---

[192] ibid.
[193] 'The Hague Programme: Ten priorities for the next five years – The Partnership for European renewal in the field of Freedom, Security and Justice', Communication from the Commission, COM(2005)184final, May 10, 2005.
[194] 'The Hague Programme: Ten priorities for the next five years', A Partnership for European Renewal,
[195] See the European Commission Justice and Home Affairs website on 'Making EU visa and residence documents more secure', available at http://europa.eu.int/comm/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm.

> "The relationship between the individual and the state in Canada, the US, the UK and Australia was also discussed as a commonality that distinguishes our countries from those with a long-standing tradition of national identity card systems. This cultural difference became readily apparent to Committee members during our travel in continental Europe."[196]

It is difficult to explain exactly why there is a cultural difference between European countries and those countries identified by the Canadians.

It is possible to say that it is because of the common law system: 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.

It could simply be an aspect of 'our culture' to reject ID cards. The Australian[197] and New Zealand[198] public have rejected similar proposals outright. Following widespread criticism,[199] Canada abandoned its proposed biometric ID card 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. However, cultural explanations are unconvincing: in all of these countries, polls have at some point appeared to demonstrate a firm support for ID cards, similar to the oft-quoted 80% in support of the UK card.

Another possible explanation is socio-legal: the citizens of these countries enjoy rights to be left alone, and these are embedded within their histories. It may be that rejection of ID Cards is symptomatic of the restraint expressed in both the unwritten and written constitutions of these countries.

Other explanations abound. The controversies that have arisen in each country during consideration of ID cards may be the product of a clearer and more open parliamentary process. Often practical issues of costs and technologies have been powerful counterbalances to claims regarding the ability of cards to provide efficient government, effective law enforcement, and even the prevention of terrorism.

These Governments frequently contend that since other countries have ID cards, then so, too, must they. The Canadian Government argued that, as 100 countries have ID cards, Canada was clearly being left behind. The Home Office argues that the UK is one of only three EU Member States that still does not have an ID card. Although many people find this argument persuasive, the fact remains that more often than not, even after all these arguments are presented, the proposals tend to fail prolonged public

---

[196] 'A National Identity Card for Canada?', Report of the Standing Committee on Citizenship and Immigration, October 2003, available at http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-e.pdf.

[197] 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.

[198] Smart Cards as National Identification Cards, School of Computing & IT, University of Wolverhampton, 1998, http://www.scit.wlv.ac.uk/~c9479633/cp3349/smrtid.html.

[199] '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.

scrutiny. Those countries without ID cards remain to be countries without, and those with cards tend to stick with them, though under strict legal regimes.

The following section will examine the processes that have occurred in those countries that display significant opposition to ID Cards.

Australia

Australia has an exceptional history with ID cards. The debate on proposals to introduce a card in the late 1980s provided significant insights into the whole issue of ID cards in every country.

ID cards are not alien to Australia. Like the British, Australians were given an identity card during the Second World War which relied on the imposition of rations as an incentive for registration and production of the card. It was dropped soon after the hostilities had ended.[200]

Thirty years passed before the idea of a national identity card was again raised. Three government reports [201] suggested that the efficiency of the Commonwealth Government could be increased, and fraud better detected, through the use of an ID card system. Two Cabinet Ministers of the Fraser Government were reported as viewing such a proposal as politically unworkable, and the idea went no further.[202]

The issue surfaced again in the early 1980s, when widespread concern about tax evasion and avoidance, coupled with concerns over the extent of welfare fraud, led to a belief that an identity card or national registration procedure might assist the government's administration processes. Fears over the extent of illegal immigration added fuel to these suggestions.

The identity card idea was raised at the national Tax Summit in 1985 (initially by Labor MP David Simmons and later by the chief executive of the Australian Taxpayers Association[203]) and found its way into legislation the following year. Playing on patriotism, the government called it the "Australia Card".

The Australia Card was to be carried by all Australian citizens and permanent residents (separately marked cards would be issued to temporary residents and visitors). The card would contain a photograph, name, unique number, signature and period of validity, and it was intended that it be used to establish the right to employment. It would also be necessary for the operation of a bank account, provision of government benefits, provision of health benefits, and for immigration and passport control purposes.

The plan consisted of six components:

---

[200] 'Private Lives and public surveillance; Social control in the computer age', James Rule, Schocken Books, 1974. Supra note 3.

[201] Asprey, Australian Government Publishing Service (AGPS) Report of the Taxation Review Committee (1975), Mathews (AGPS)Report on inflation and taxation (1975), Campbell (AGPS) Report on the Australian Financial Systems, (1975)

[202] 'The Australia Card : A technology driven policy?' 45, (1990). Peter Graham, unpublished M.Phil thesis. Griffith University, Brisbane.

[203] 'The resistible rise of the national personal data system', Roger Clarke, Software Law Journal, Chicago, February 1992, p.36.

- **Register:** A central register containing information about every member of the population, to be maintained by the Health Insurance Commission (HIC).
- **Code:** A unique numerical identifier to be given to every member of the population, and assigned by the HIC.
- **Card:** An obligatory, multi-purpose identification card to be issued by the HIC to every member of the population.
- **Obligations:** The law would require all individuals to produce the card for a variety of reasons, and would require organisations to demand the card, apply sanctions to people who refused to do so, and to report the data to the government.
- **Use:** The number and the Australia Card register were to be used by a variety of agencies and organizations as their administrative basis.
- **Cross-notification:** Agencies using the system would be required to notify each other of changes to a person's details.[204]

Despite the extraordinary change that the plan was likely to prompt in the relationships within the Australian Community, the proposal caused hardly a ripple of concern. Early opinion polls showed that 70% of the public supported the scheme.

Not everyone was enthusiastic about the plan: a few journalists ran occasional stories raising questions about the proposal. The parliamentary opposition opposed the plan. Most significantly, a small number of committed academics and advocates worked to provide a critical analysis of the scheme and its implications.

Legal centres, civil liberties councils, academics and advocates joined in opposition to the ID card plan, and over the next two years, a strong intellectual foundation was developed.

Australian data protection expert Graham Greenleaf, one of the pioneers of the anti ID card movement, warned:

> "Is it realistic to believe that the production of identity cards by children to adults in authority to prove their age will be "purely voluntary"? The next generation of children may be accustomed to always carrying their Cards, to get a bus or movie concession, or to prove they are old enough to drink, so that in adult life they will regard production of an ID card as a routine aspect of most transactions."[205]

Advocates pointed out that, whilst it is true that some civil law countries (such as Spain, or France) have an ID card, none would have been as intrusive or dangerous as that proposed by the Australian Government. The Australia Card would go much further than the mere identification purpose of ID cards in other countries by creating a central information register that would touch many aspects of a person's life.

[204] Ibid p.38
[205] Law Society Journal, Sydney, October 1987.

At the end of 1985, the opposition-controlled Senate forced the appointment of a Joint Select Committee to investigate the proposal. The Committee raised a wide spectrum of concerns. The majority of the Committee, including one government member, opposed the scheme, warning that it would change the nature of the relationship between citizen and state and create major privacy and civil liberties problems. The Committee further commented that the cost benefit basis for such a scheme was speculative and rubbery, and that all common law countries had rejected such proposals.[206] The fact that no common law country has accepted an ID card was crucial to the whole debate over the Australia Card.

The Committee's report formed the basis of the parliamentary opposition's rejection of the scheme. On two occasions the Government presented the legislation to the Senate, where it does not have a majority, only to see the bill rejected. After the second rejection by the Senate, the Government used the issue as the trigger to employ its constitutional right to call an election on the ID card legislation, and to call a joint sitting of Parliament, where it would have a majority.

In fact, the election campaign of July 1987 contained almost no reference to the ID card issue. In the opinion of the media, the ID card was simply not on the agenda.[207] The government was re-elected, and promptly re-submitted the ID card legislation.

Within weeks, a huge and well-organised movement was underway. Rallies were organised on an almost daily basis, and although these were described as "education nights", the reality was that most were hotbeds of hostility rather than well-ordered information sessions.

On the night of September 14th, 4,000 angry people packed the AMOCO hall in the central New South Wales town of Orange. One in seven of the city's population attended the meeting. Other towns responded in similar fashion.

The massive wave of public outrage was generated by scores of ad-hoc local and regional committees across the country. Rallies formed on a daily basis, culminating in a gathering of 30,000 outside Western Australia's Parliament House. The Australian Privacy Foundation, which had organised the campaign, had planned rallies in Sydney and Melbourne that were likely to block the Central Business District.

A major national opinion poll conducted in the closing days of the campaign by the Channel Nine television network resulted in a 90% opposition to the card. The normally staid Australian Financial Review produced a scathing editorial which concluded:

> "It is simply obscene to use revenue arguments ("We can make more money out of the Australia Card") as support for authoritarian

[206] Report of the Joint Select Committee on an Australia Card, AGPS, Canberra, 1986

[207] Neither the Government nor the Opposition raised the ID card as a key issue during the election campaign.

> impositions rather than take the road of broadening national freedoms."[208]

By mid-September, the Government was facing an internal crisis. The left of the party had broken ranks to oppose the card,[209] while right wing members (particularly those in marginal seats) were expressing concern within caucus.[210] Deputy Prime Minister Lionel Bowen urged the Party to tread with caution, and suggested that a re-think might be necessary.[211]

Within weeks, in the face of mass public protests, a party revolt and civil disobedience, the government scrapped the ID card proposal. It was provided with the convenient face-saver of a technical flaw in the legislation revealed by opposition senator John Stone. The government had the option of re-introducing the legislation, but did not need to do so. Journalists reported that the government was overwhelmed with joy that the flaw had been discovered.

All these years later, this case sounds a warning to other governments on identity cards, although it should be said that it has not prevented a slow movement towards a national identity system.

Australia is imposing basic biometrics into passports, but this will be limited to a digital photograph. It will result in a AU$19 increase in the cost of passports.[212] As part of a broad National Identity Security Strategy, the Government is also planning a national "document verification service" designed to combat identity-related fraud. This would enable the cross-checking of birth certificates, driver's licences and passports through a central data exchange hub.[213] The Government is opposed to the introduction of a single number to identify every Australian.

Canada

The issue of identity cards in Canada had a short lifespan. This may in part be because the Canadian Government never actually introduced a specific proposal. Rather, the Minister of Citizenship and Immigration proposed a national discussion on identity cards on the grounds that if Canada did not consider and identity system, it might instead be imposed upon Canadians because of US border restrictions. According to the minister at the time, Denis Coderre:

> "If you have that entry-and-exit program when you will have to be fingerprinted, you will say, 'I'm a Canadian citizen, why do you need my fingerprints and what are you going to do with it?' Well, wouldn't you like to have a debate among ourselves and say, as Canadians, we will build that the Canadian way? If we can have the technology with

[208] The Australian Financial Review, 28 August 1987
[209] Daily Telegraph, Sydney, September 8, 1987
[210] The Sun Herald, Sydney, 13 September, 1987
[211] Daily Telegraph, Sydney, 19 September, 1987
[212] 'ID fraud on Budget hit-list', James Riley, Australian IT, May 10, 2005.
[213] 'Privacy 'risk' in national ID plan', James Riley, The Australian, January 21, 2005.

> our own scanners, we can say we will take care of our own people with our own scanners."[214]

Although no proposal was tabled, it was left open to a Parliamentary Standing Committee on Citizenship and Immigration to investigate the case for the cards. The Committee held a number of consultation sessions, met with local leaders, and travelled internationally to consult with countries with identity cards, and those without. After a few months it released an interim report. The interim report outlined a number of concerns. These included a transformation of the relationship between the individual and the state, data protection and privacy, function creep, the weaknesses in the technology, over-reliance on a single card, identity theft generated by the card, costs, and race relations.

The interim report concluded by stating:

> "This report is intended to summarize what we have heard thus far and we reiterate that we are continuing our study. It is clear that this is a very significant policy issue that could have wide implications for privacy, security and fiscal accountability. Indeed, it has been suggested that it could affect fundamental values underlying Canadian society. A broad public review is therefore essential. The general public must be made more aware of all aspects of the issue, and we must hear what ordinary citizens have to say about the timeliness of a national identity card."

No further work followed, and no final report was issued. Rather, with those words the initiative was abandoned.

A parallel situation arose during this formal consultation. Every province in Canada is responsible for issuing driver's licences. Increasingly these licences are becoming digitized, and photographs are being collected and stored on databases. The province of Alberta has even implemented facial recognition into their licensing system. In the case of George Bothwell, whose licence was issued by the province of Ontario, this resulted in a constitutional challenge. As a Christian fundamentalist, Bothwell mounted the challenge to prevent his driver's licence from being entered on a database. He considered that this was not in accordance with his religious beliefs (with reference to Revelations from the New Testament):

> "The danger is when the central authority captures digital identifiers from people and stores them in a central data base for any authority with the right technology to access."[215]

Bothwell argued that this was a violation of the Charter of Rights and his right to freedom of religion, particularly if the database contains face, fingerprints or eye scans.[216] Clearly Bothwell was concerned with his right to privacy. According to Canadian jurisprudence:

---

[214] 'Coderre pushes Ottawa to adopt national ID cards', Campbell Clark, Globe and Mail, February 7, 2003.
[215] 'Ontario farmer challenges driver's licence photo', Kirk Makin, Globe and Mail, October 15, 2003.
[216] 'National ID cards slammed at immigration hearing', CBC Online, February 11, 2003.

> "Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state."[217]

Bothwell was pursuing his right to privacy on the basis of his freedom of religion, but he lost his case. The Court decided that his religious beliefs did not meet the criteria under the religious freedom section of the Charter. As he was not part of an organized religion, his beliefs were not recognized as religious. The court therefore managed to avoid dealing with the other issues, specifically privacy, because they were focused on establishing whether he met the test(s) for religious freedom.

As is the case in Australia, despite setbacks on ID cards, the Canadian Government is moving to implement biometric passports. Although the national ID card was abandoned officially in March 2004, in April 2004 the Government announced its plans for biometric passports. While outlining the Canadian National Security Policy, the Government declared:

> "Canada will deploy facial recognition biometric technology on the Canadian passport, in accordance with international standards."[218]

The Canadian Government justified this change, like most other countries, as necessary "to maintain our reputation as a First World nation".[219]

The policy refers to the ICAO statement from May 2003 to explain its choice of facial biometrics. This was decided on grounds that this biometric was the most unobtrusive.[220] The National Security Policy states that:

> "Canada will begin issuing a biometrically enabled smart chip passport in early 2005. There will be no change in the way that Canadians apply for a passport. However, the photo that they submit will be digitized and stored on a chip imbedded in the passport."[221]

There are no plans to compile a searchable electronic database of the images or other data encoded on the chip,[222] although there are reports that the Passport Office has been testing the idea of screening applicants' photos against images of suspects on terrorist watch lists, with an accuracy rate of 75% to 90%.[223]

There are further developments under the Smart-Border Agreement. This is an agreement with the US Government on data-sharing and common standards between the two countries at border points. The "Smart Border Declaration and Associated 30-Point Action Plan to Enhance the Security of Our Shared Border While Facilitating the

[217] *R. v. Dyment*.
[218] 'Securing an Open Society: Canada's National Security Policy', April 2004, chapter 7.
[219] 'The IT in your ID', Shane Schick, ITBusiness.ca, July 19, 2004.
[220] 'Passports go high-tech', Luma Muhtadie, Globe and Mail, April 28, 2004.
[221] 'Securing an Open Society'.
[222] 'Canadian digitized passport stamped', Canadian Press, Calgary Sun, July 19, 2004.
[223] 'Plan to match Canadian passport photos with terrorist watchlists in works', Jim Bronskill, August 29, 2004.

Legitimate Flow of People and Goods" was signed in December 2001. The Action plan includes the development of common standards on biometric identifiers, an agreement to use interoperable technologies to read the biometrics, and an agreement to use cards that can store multiple biometrics. Given the date of this document, it is likely to have been the driving force behind the national ID initiative. The two countries continue to work on methods of sharing data, and standardising policies and technologies.

United States and REAL-ID

Americans are generally opposed to ID cards and have rejected all prior proposals to implement such a system, but in February 2005 the US House of Representatives approved H.R. 418, the REAL ID Act. It became law in May 2005 following unanimous approval in the Senate after it had been attached to a funding bill for the military operations in Iraq, and Tsunami relief. Up until this point, the legislation had encountered significant opposition from politicians and groups from across the political spectrum.

A relevant aim of the law is to establish and rapidly implement regulations both for State drivers' licenses and for identification document security standards. The law requires States to deny drivers' licenses to undocumented immigrants: this requirement is seen as moving the license into the realm of a national ID card.

The first step lays the foundations by requiring 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 US 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:

> "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 US-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."[224]

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

[224] 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.

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

The law also repeals earlier statute 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."[225]

However, even at its worst, the REAL ID Act only gives the Federal Government the same powers that the UK Government already has over the information held in the DVLA. The general response to the Act in the US is one of widespread concern, and there are reports of a number of plans to appeal to the courts on the matter. For instance, the National Governors Association threatened lawsuits on the grounds that it will cost States up to $700 million to comply with the law.[226] The Mexican Government is prepared to lodge a diplomatic complaint regarding the law, referring to it as "negative, inconvenient and obstructionist."[227]

In an interesting development, the state of Georgia has prohibited the use of fingerprints in drivers' licenses. This followed concerns regarding identity theft, and acknowledgement by the law enforcement community that the fingerprints were not being used for combating crime.[228] The state assembly of Georgia responded by passing a law, by a wide majority,[229] prohibiting the collection of fingerprints. The law also requires that all existing fingerprints be deleted from the licensing databases:

> "Not later than 30 days after the effective date of this paragraph, the department shall destroy all records of fingerprints obtained on and after April 15, 1996, and prior to the effective date of this paragraph from applicants for drivers' licenses, identification cards, and identification cards for persons with disabilities issued by the department and shall compile and make available for public inspection a list of all persons or entities to whom the department provided such fingerprint records. Notwithstanding the provisions of this paragraph, fingerprint images electronically stored on existing drivers' licenses will be destroyed upon application for a renewal of the driver's license."[230]

The Act goes on to state explicitly that applicants shall not be required to submit (or otherwise obtain) fingerprints, biological characteristics such as DNA, nor retinal scan identification. In an unrelated event, the state's database was maliciously hacked shortly

[225] Executive Office of the President, Statement of Administration Policy: HR 418 – REAL ID Act of 2005, Office of Management and Budget, February 9, 2005.
[226] 'National ID Battle Continues', Kim Zetter, Wired News, May 12, 2005.
[227] 'Mexico furious at tough US law on migrants', John Authers and Edward Alden, The Financial Times, May 13, 2005.
[228] 'Driver's License Fingerprints Debated', Associated Press, February 23, 2005.
[229] 'Fingerprint bill deserves Perdue's OK', Bob Barr, as published by the Atlanta Journal-Constitution, May 4, 2005, available at http://www.bobbarr.org/default_print.asp?pt=newsdescr&RI=624.
[230] Georgia General Assembly, House Bill 577, 05 HB 577/AP, to be effective 1 July 2006, available at http://www.legis.state.ga.us/legis/2005_06/fulltext/hb577.htm.

afterwards.[231] This law may conflict with the REAL ID Act, depending on the established standards for biometrics, if any, that emerge once the Act is implemented.

United States and Border Controls

Since September 30 2004, all visitors to the United States[232] are face-scanned and fingerprinted at the border. These measures are part of a vast integrated information storage, matching and profiling system. In 1996 Congress called on the Attorney General to develop an automated entry and exit monitoring system for foreigners. This was expanded significantly by the USA-PATRIOT Act that suggested the use of biometrics. The Enhanced Border Security and Visa Entry Reform Act took the USA-PATRIOT Act even further by calling for the integration of the border monitoring system with other databases.

The US Visitor & Immigration Status Indication Technology System (US VISIT) collects and retains biographic, travel, and biometric information on all visitors, except Canadians and Mexicans. The purpose of this collection is to identify people who are believed to potentially pose a threat to the security of the US, are known or believed to have violated the terms of their admission to the US, or who are wanted in connection with a criminal act in the US or elsewhere. This information will be shared with "other law enforcement agencies at the federal, state, local, foreign, or tribal level" who "need access to the information in order to carry out their law enforcement duties."[233]

Personal information collected by VISIT will be retained for 75 to 100 years. It is kept alongside data collected from nationals of countries that threaten to wage war, are or were at war with the United States.[234]

The system is to be used for a plethora of purposes. These include national security, law enforcement, immigration control, and: "other mission-related functions and to provide associated management reporting, planning and analysis." It will assist in:

> "identifying, investigating, apprehending, and/or removing aliens unlawfully entering or present in the United States; preventing the entry of inadmissible aliens into the United States; facilitating the legal entry of individuals into the United States; recording the departure of individuals leaving the United States; maintaining immigration control; preventing aliens from obtaining benefits to which they are not entitled; analyzing information gathered for the purpose of this and other DHS programs; or identifying, investigating, apprehending and prosecuting, or imposing sanctions, fines or civil penalties against individuals or entities who are in violation of the Immigration and Nationality Act (INA), or other governing orders,

[231] 'State of Georgia Driver's License Files Hacked', Dick Petty, Associated Press, May 19, 2005.
[232] With the exception of citizens of Canada and Mexico.
[233] US Department of Homeland Security. 2003. US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary, December 18.
[234] Federal Register. 2003. DEPARTMENT OF HOMELAND SECURITY [DHS/ICE–CBP–CIS–001] Privacy Act of 1974; System of Records, Federal Register, Volume 68 Number 239. December 12.

> treaties or regulations and assisting other Federal agencies to protect national security and carry out other Federal missions."[235]

This information will then be shared with other government departments and used in other programs of surveillance.[236] The US Government has already made visa information available to law enforcement officials across the country, including photographs of 20 million visa applicants. This 'sensitive' information will be shared with 100,000 investigators across the country, and they will have access to seven terabytes of data on foreigners.[237]

The Government Accountability Office, the US equivalent to the National Audit Office, assessed US-VISIT in March 2004 and declared that it is:

> "inherently risky because it is to perform a critical, multifaceted mission, its scope is large and complex, it must meet a demanding implementation schedule, and its potential cost is enormous."

Pointing to other data collection and mining initiatives, the GAO warned that the project is "increasingly risky".

The project is also quite costly, particularly as it grows larger and more complex. The US Government has commissioned a $15 billion contract to fully develop VISIT into a system that creates detailed dossiers on all visitors to the US (even though DHS had originally budgeted $7.2 billion)[238]. The system is likely to include other biometrics in the future; according to the contract winner, Accenture:

> "Part of our approach is to continually assess technology innovations. For a 10-year contract that's a generation or two of technology, and biometrics is a very hot area."[239]

In its Privacy Impact Assessment, the Department of Homeland Security (DHS) has contended that VISIT actually protects the privacy of foreigners. When VISIT was first put into operation, however, there were no rights of redress for individuals who faced any sort of adverse consequences.[240] Following a review by the GAO (and some outcry by legal and civil rights advocates) there is now a limited appeal process, including a human review of the fingerprint matching process, and provision for some correction of faulty information.

A further assessment by the GAO was carried out in February 2005[241]. This found that a security risk assessment has not yet taken place, and that the privacy impact assessment was lacking. The problems arose particularly because VISIT is made up of various pre-

[235] Ibid.
[236] Ibid.
[237] Lee, Jennifer 8. 2003. State Department Link Will Open Visa Database to Police Officers. The New York Times, January 31.
[238] GAO. 2004. Data Mining: Federal Efforts Cover a Wide Range of uses, GAO-04-548, May.
[239] Lichtblau, Eric, and John Markoff. 2004. Accenture Is Awarded US Contract for Borders. The New York Times, June 2.
[240] CDT. 2004. Comments Of The Center For Democracy And Technology on US-VISIT Program, Increment 1, Privacy Impact Assessment, Center for Democracy and Technology. February 4.
[241] GAO. 2005. Homeland Security: Some Progress Made, but Many Challenges Remain on US Visitor and Immigrant Status Indicator Technology Program, GAO-05-202, February

existing systems, operated in different ways by various DHS organisational components.[242] The GAO found conflicting protections under the Privacy Act for information that came from a variety of sources, arising from the fact that VISIT is an amalgamation of a number of different data sources. The GAO found that, while access to travel information was limited to authorized users, the data stores for fingerprints and face-scans: "do not consider privacy at all"[243]. This was considered to be symptomatic of the wider problems with VISIT, including rising costs and the lack of reliable cost estimates, management problems, and capacity issues. The GAO concluded that the DHS should reassess plans for deploying an exit-capability.

An earlier GAO report makes the point that the False Non-Match Rate for fingerprinting can be extremely high – up to 36 percent.[244] With 300 million visitors to the US every year, the potential for mass error increases, yet little attention had been paid to these issues.

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.

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 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."[245]

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

[242] Ibid. p.119.
[243] Ibid. p.71.
[244] General Accounting Office, Technology Assessment: Using Biometrics for Border Security, November 2002.
[245] House of Commons, Hansard, December 20, 2004 : Column 1992, http://www.publications.parliament.uk/pa/cm200405/cmhansrd/cm041220/debtext/41220-31.htm.

> "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."[246]

This position was confirmed by Home Office 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".[247]

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 it 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."

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.

---

[246] Hansard, Written answers, January 10, 2005, Column 305W, http://www.parliament.the-stationery-office.co.uk/pa/cm200405/cmhansrd/cm050110/text/50110w83.htm.
[247] Hansard, Written answers, January 26, 2004, Column 214W, http://www.publications.parliament.uk/pa/cm200304/cmhansrd/vo040126/text/40126w51.htm.

Conclusions

There are many conclusions to draw from a review of identity systems in other countries. The Home Affairs Committee observed that:

> "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."

These comments are consistent with our research, but the review that we have conducted leads us to believe that there are still more conclusions to be drawn.

One of the more difficult issues to explain is the reason why some countries have ID cards while others do not. Sometimes the answer is framed in assertions that countries of a certain type are less likely to have them, for example English-speaking countries, common law countries or federalist countries, but these are inadequate explanations because there are always exceptions.

A conclusion that may be drawn from this review is that while many countries do have ID cards, a large number of them never had a national debate about the need for them. Where such a debate does occur, there is usually broad support for ID cards, that ebbs away when the flaws of the system are seen, the penalties of non-compliance are noticed, costs are disclosed and reviewed, and the implications are considered in detail.

Such debate is a rare occurrence. The identity systems of many countries have been inherited from prior regimes of a completely different kind: under Franco in Spain, registration by a Nazi Government, national ID numbers by the Vichy regime in France, national registration by the Church in Sweden, unstable governments in Greece, and Mussolini in Italy. Sometimes they are implemented in times of war, as was the case in Australia, Hong Kong, and even the United Kingdom. In a significant number of cases, ID cards have been implemented by decree rather than through a national law. This was the chosen method in Spain, Greece, Italy, the Philippines, and Thailand.

That cards were introduced within such environments does not lead immediately to the conclusion that they are merely tools of oppression. Such a conclusion would be rash, although it merits further study. We are merely observing that, for many countries, identity cards became a national custom and part of the political culture in a different era. They become customary only through usage and adaptation, not because of general approbation.

Putting aside the issue of acceptance or rejection of ID cards, it should be noted that not all systems are built equally. Even within the European Union, cards vary widely in their size, content, and substance. Some have very large registries. Some rely on mandatory use. Some involve biometrics. Registration processes vary from registering at police stations to banks; requiring a live witness to a signed photograph by referees; central storage of biometrics to distributed systems that may be deleted once the cards are issued.

The reasons for this variety are largely attributable to national legal culture. The fact that a country has a national ID card does not mean that its populace supports the type of system proposed in the UK. ID systems in each country are designed with specific safeguards, and it is this which leads to the variability in design. Sweden refused to make use of the registry; Germany cannot construct a database of biometrics; France has not previously made its card mandatory; Italian regulators have wide powers to ensure the adequate protection of data. Outside Europe the situation is even more fragmented: some countries require iris scans and are considering the use of DNA, while the state of Georgia has removed fingerprints from its licences, and China has abandoned biometrics, and Taiwan is on the verge of declaring its fingerprinting programme as unconstitutional. Bosnia decided against using a smartcard chip, but other countries are considering the use of chips that broadcast a person's identity and this personal information can be read at a distance. Until recently, every country made its own decisions about the constitution of their ID systems, and to a considerable extent it was based on the legal and political culture.

Whether it is under constitutional law or because of public sentiment, Governments are not free to change their systems without some form of public or legal negotiation. Even when systems were first implemented under oppressive regimes, safeguards were eventually implemented. The French and German systems are prime examples of this, with their variety of restrictions and powerful regulators. Greece, where previously religious faith, profession, and residence were indicated on ID cards, was compelled to remove this by its national regulator. In Italy it is said that, although Italians like their identity cards, the implementation of a fingerprint biometric would provoke a negative response. In fact, we have serious doubts as to whether any other European country would be able to implement a system similar to that proposed in the UK.

Reviewing the practices of other countries is not merely an academic exercise. We can learn from their achievements and failures. We can understand the risks to networking and creating a central registry from the experience in Japan with the weak security surrounding the Juki-Net. We can learn from the Malaysian MyKad, where Banks are advising that they should not be used to their full capabilities to access ATMs. Hong Kong conducted a Privacy Impact Assessment before moving forward with its card. Bosnia decided against using a chip, and managed to reduce costs significantly. Germany deletes registration information from central stores when they are no longer needed, and data is only collected locally. A number of countries do not have onerous enrolment procedures, reducing costs and also minimising the inconvenience for individuals. Some countries restrict the use of ID numbers. Others have acknowledged that identity cards do affect the relationship between citizens and police, and have tried to find ways to resolve the tensions that may arise. Many countries endow their national regulators with broad powers to monitor abuse.

The Government seems intent on pointing to international obligations and precedents. Our research indicates a fragmented approach to ID cards around the world, and there is much to learn from the experiences of others. A national identity card need not resemble the one that the Government is proposing, nor is anyone under any obligation to create such a card. Indeed, no other country has so far done so.

This is linked to another finding from our research: the nature of the system implemented in a given country is related to the institution proposing it. A control-oriented regime implements one system, a democratic system another. When ID cards are implemented to enable electronic commerce and e-government, they tend to be less centralised and less focused on the collection of significant amounts of personal information. When a system is devised by an Interior or Home Affairs ministry, the system always proposes a centralised solution involving the mass collection of personal information and the intensive use of biometrics. This was best exemplified by the varying proposals in France, and it appears to be the situation in the United Kingdom.

Our fundamental conclusion, that open deliberation on ID cards is the reason why some countries have refused to adopt them, is called into question immediately by international dynamics. Numerous mechanisms are currently being used to reduce public debate and create a sense of inevitability. Increasingly Governments are arguing that identity cards are essential because of international obligations, in particular the calls for harmonization from within the EU, or passport requirements emerging from the US. This has the effect of minimising debate and deliberation because the system is seen as inevitable; but this needs not be the case, because the averred obligations do not yet exist.

The Prime Minister has repeatedly stated that the UK must implement facial, finger, or iris-based biometrics because of obligations imposed by the US. Our research has shown that this is simply not the case. Even if the Prime Minister were to argue that new regulations from the EU require biometric passports with fingerprints, this could not be true because the UK is not party to the agreement that establishes this standard.

Governments are increasingly using international agreements and standards as a defensive strategy in order to minimize debate. Canada is implementing biometrics on the grounds of its ‘Smart-Border’ agreement with the US, yet these claims are not questioned in Parliament or by the general public. The European Union is working on harmonizing identity cards, despite the variances within countries and the legal restrictions on the collection of further information. These international agreements are often beyond the reach or attention of the Parliaments of individual countries, and so the apparent element of compulsion is rarely questioned. However, it is important that these assumptions of inevitability are interrogated, particularly as the UK takes over the presidency of the EU and begins working on The Hague Programme action point of harmonizing identity documents: something that the UK Parliament has yet to approve in the UK. Similar dynamics are emerging in Germany, where the Government is pursuing policies abroad that they are prevented from pursuing nationally. In France, the Government argues that perceived international obligations and developments in the UK, oblige them to ignore all the legal and cultural precedents of their country and develop a system similar to our own proposed identity system.

The Government is certainly in an awkward position when it comes to the international dynamics of identity. It argues that the UK must follow the path of other countries, despite the fact that no other country has a system similar to that which is proposed here. It insists that it must follow international obligations, but then incorrectly interprets those obligations. It states that the world is moving to greater use of biometrics, but is itself responsible for developing and pushing an 'international standard' on biometrics.

While we can disagree on detailed issues, this section shows that we must above all foster debate in order to ensure that any implementation of an identity card in the UK is the product of an open and transparent process of deliberation.

8

Identity Fraud

There is growing concern and controversy over identity theft. Numerous surveys have indicated increased worry amongst the general public in the UK. This has occurred alongside an apparently growing number of cases of reported identity theft around the world.

The Identity Cards Bill has been offered by the Government as the solution to identity theft. When the bill first went through Parliament, the discussion of identity theft was marginal. A few mentions were made on both sides of the debate, but it was never a large component of the discussion. When it was discussed, it was always in tandem with the Cabinet Office estimate that identity theft cost the UK £1.3 billion per year. Yet none of the claims for or against the linking of the card to identity theft involved much detail.

Identity theft is now taking a more central role in the second round of the Bill's passage through Parliament. The first item of the parliamentary briefing on ID cards states that:

> "Criminals are recognising that our identities are just as valuable, if not more so, than our material possessions. A few items stolen from a rubbish bin such as utility bills and credit card statements can lead to huge financial losses as well as distress and inconvenience for victims in putting their records straight. On average victims can spend 60 hours restoring their records. An ID cards scheme – as the legislation says – is first and foremost for the benefit of citizens, giving them a means to protect their identity and to be able to prove it in a secure and straightforward manner."[248]

It is difficult to find any flaw within this statement, and since the release of the bill much of the emphasis of the debate has been on identity theft. Similarly, in Parliament the issue of identity theft was raised in order to promote Identity Cards Bill as the solution:

> "Siobhain McDonagh (Mitcham and Morden) (Lab): What can my right hon. Friend do to help people like Gavin Fisher, a young man from Mitcham whose identity has been stolen? On more than one occasion his parents have been sent frantic by calls from the police to say that he has been arrested, only to go to the police station to find

[248] 'Identity Cards Briefing', the Home Office, May 2005.

> that it is not him. He receives threatening letters and court summonses from train companies on whose trains he has never travelled; Thameslink says that there is nothing that it can do. How can my right hon. Friend help my constituent and his desperate parents?"
>
> "The Prime Minister: We will be introducing some measure of help later today. It is important to emphasise that the abuse of identity costs this country billions of pounds a year."[249]

The public is naturally concerned about this increasingly prevalent crime, and the Government is proposing a solution.

This debate over identity theft is not without controversy. The definition of the term is unclear. It may be an assortment of various forms of fraud that are unrelated to problems of identity. In cases where there is a theft of personal information, other solutions do exist that do not require identity cards. While there are cases where identity theft does involve the fraudulent use of another's identity, as was the focus of the Cabinet Office study that predicted £1.3bn in costs per year, it is questionable how much of this cost would be prevented by an identity card.

The greatest challenge in solving the *identity theft* problem is to ensure that solutions do not make matters worse. In some cases, the use of unique identifiers for citizens has become the key enabler of identity theft. In others, the use of identification documents has presented a key opportunity for forgery. According to Interpol, one country has reported the theft of more than 50,000 blank passports;[250] and it was reported in the US Congress that thousands of French passports were stolen in 2004.[251] Centralised identity systems often give rise to fraud through the abuse of centralised data either by insiders (staff) or outsiders (malicious hackers). Australia lost 2042 passports from 1997 to 2002, and investigators believe that some of this was due to insider fraud.[252] In the US there have been mounting thefts and abuses of personal data from banks, driving licensing authorities, and data-aggregating companies such as credit bureaux.

Nature of the Problem

The best studies on the phenomenon of *identity theft* are emerging from the US, compared to relatively limited studies in the UK. Reporting from the US indicates that in 2004 there were 9.3 million victims of identity theft, costing over $50 billion.[253] Another survey found that in the period from 1990 to 2003, over 33.4 million Americans were victims of identity theft, leaving consumers with out-of-pocket expenses amounting to $1.5 billion since 2001.[254] According to the Federal Trade

[249] House of Commons Hansard Debates for 25 May 2005 (pt 4), available at http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm050525/debtext/50525-04.htm#50525-04_spmin8
[250] 'Interpol plans anti-terrorism database', Daniel Woolls, Associated Press, September 29, 2003.
[251] Statement of Chairman Sensenbrenner, House Judiciary Committee, Oversight Hearing on Whether Congress Should Extend the October 2004 Statutory Deadline for Requiring Certain Foreign Visitors to Present Biometric Passports, April 21, 2004.
[252] 'Missing passports hinder terror fight', Australian Broadcasting Corporation, April 29, 2005.
[253] Privacy Rights Clearing House overview of ID Theft surveys, referring to the Javelin/Better Business Bureau from January 2005.
[254] Ibid, referring this time to the Privacy and American Business survey from July 30, 2003, with further information available at http://www.pandab.org/id_theftpr.html.

Commission, in 2002 4.6% of Americans encountered some form of identity theft.[255] Indeed, one survey notes that one in six consumers are willing to buy privacy protecting products and services to prevent having their identities stolen, spending on average $75 per year, representing $2.5 billion per year.[256]

In response, the US Government has developed laws to prevent and investigate identity theft. Under these laws identity theft is defined as taking place when someone:

> "knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."[257]

Numerous states have also passed laws that provide assistance in recovery from identity theft.[258]

The primary regulator in the US, the Federal Trade Commission (FTC), defines identity theft as follows:

> "Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes."[259]

The FTC recognizes the source of this crime as being wide and disparate. The FTC contends that thieves get information from businesses through theft, hacking, or bribes; from individuals by rummaging through rubbish bins; from credit reporting agencies; skimming credit cards or theft of wallets; performing a 'change of address' on existing accounts; and through scams by posing as legitimate businesses.[260]

The FTC separates victims of identity theft into three categories. The first is theft through the creation of "New Accounts & Other Frauds". The second is the "Misuse of Existing Credit Card or Credit Card Number", and the last and least serious was the "Misuse of Existing non-Credit Card Account or Account Number".[261] The greatest incidence of theft occurs through this last form of misuse of account information. 'New Accounts' fraud only occurs to 1.5% of the population, though amounts to $32.9 billion in costs, while mis-use of accounts (both credit card and non-credit card) amounts to $14 billion, where the vast majority of this occurs through credit card fraud (67%). The

[255] Federal Trade Commission – Identity Theft Survey Report, September 2003, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf., page 7.
[256] Ibid.
[257] Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028).
[258] Federal Trade Commission, Take Charge: Fighting Back Against Identity Theft, February 2005, available at http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.
[259] http://www.consumer.gov/idtheft/.
[260] Understanding and Detecting Identity Theft, FTC, available at http://www.consumer.gov/idtheft/understand&dectect_IDT.html
[261] Federal Trade Commission – Identity Theft Survey Report, September 2003, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

majority of new accounts opened by identity fraudsters were credit card accounts, followed by loans, telephone services, banking, and internet transactions.[262]

No government department has argued for identity cards in the US on grounds of combating identity theft.[263] In fact, the dominant argument is that a national ID card in the US would make identity theft more of a problem because of the centralisation of personal information it would entail.[264] This argument was supported by the theft of personal data from three state ID issuing agencies over a two month period.[265] In one case, the criminals stole blank licenses, along with an equal number of laminated covers with state seals, a digital license camera, a desktop computer and a license printer.[266]

In the US, the Social Security Number has become an identity hub and a central reference point to index and link identity.[267] Obtaining a person's SSN provides a single interface with that person's dealings with a vast number of private and public bodies. There have been countless cases of identity thefts that were enabled by first obtaining the SSN. It is arguable that the existence and ease of obtaining the SSN and its importance across private and public databases is the reason why the level of identity theft in the US is extremely high. This situation applies equally in Australia where the introduction of an extensive Tax File Number has also increased the incidence of identity theft beyond the levels experienced in the UK.[268]

Consumer groups in the US have recently criticised the Senate Banking Committee for failing to take action to reverse this trend. The Consumers Union argues 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.[269]

In the United States, Blue Cross and Blue Shield recently decided to discard the use of Social Security numbers in order to reduce 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.[270]

As a result, Identity Cards with a new global unique identifier are not considered a reasonable solution to the challenges faced in the US. Rather, the measures that are promoted to combat identity theft include promoting the reporting of the crime to authorities (which only 25% of victims do), and notifying credit bureaus (only 37% have). The FTC also recommends credit fraud-alerts to notify individuals when

[262] FTC report, page 34.
[263] E.g. the FTC document on 'Remedying the Effects of Identity Theft' recommends many measures but none include more identity document. Available at http://www.ftc.gov/bcp/conline/pubs/credit/idtsummary.pdf
[264] American Civil Liberties Union, 'Real ID' Tacked Onto Military Funding Measure, Bill Would Enact Broad Changes Without Congressional Review, May 4, 2005. The ACLU states that an ID system is 'a system ripe for identity theft.'
[265] 'National ID Battle Continues', Kim Zetter, Wired News, May 12, 2005.
[266] 'Authorities warn of consequences of DMV break-in', Omar Sofradzija, Las Vegas Review-Journal, March 9, 2005.
[267] 'Proposed California Bill Bans Distribution of Social Security Numbers', Information Week, December 6, 2004, http://informationweek.com/story/showArticle.jhtml?articleID=54800697.
[268] 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.
[269] Consumers Union statement, September 23, 2003, http://www.consumersunion.org/pub/core_financial_services/000407.html.
[270] 'Blue Cross to drop Social Security numbers from ID cards', The Business Journal, March 8, 2005.

suspicious activity takes place in their name. The FTC also calls for improved mechanisms to deal with investigations, which is the leading complaint from victims, and for better data management practices, reducing the amount of personal information available to others. The FTC found that victims preferred stronger authentication measures for credit cards, as well as more thorough identification measures for employees during credit transactions.[271]

A recent project at Johns Hopkins University illustrated the ease of identity theft in the US. Post-graduates involved in the study were encouraged to use legal, public sources of information, in order to try to steal identities for less than $50. The project concluded that this could trivially be achieved, and that there was a need for better regulation of the use of personal information.[272]

In the US data-mining institutions are not tightly regulated. In the period of February to May of 2005 there have been over twenty cases of security breaches at large organisations in the US, resulting in the theft or loss of over 5.5 million records.[273] The cases vary in form and motive:

- employees selling information, e.g. Bank of America employees were caught after selling 676,000 customer records[274];
- malicious hacking of databases, e.g. LexisNexis found that 310,000 files may have been accessed[275];
- theft of computers, e.g. the University of California-Berkeley discovered the theft of a university laptop computer containing 98,000 applicant records[276];
- loss, e.g. Bank of America lost backup tapes containing the personal information of 1.2 million federal employees.[277]

One of the most recent breaches of security involved the loss of 3.9 million records by CitiFinancial, the consumer finance subsidiary of Citigroup.[278] There are continued calls for further regulations in the US on the use of personal information by government agencies and companies in order to rectify this situation.

ID Theft in the UK

Information collection and processing is regulated in the United Kingdom under the Data Protection Act 1998. This law does not limit the amount of personal information that is collected, so long as the amount is proportionate to the purpose. As in the US, there are numerous credit reporting agencies (e.g. Equifax and Experian), the public registers (e.g. the electoral roll), and various data mining companies (e.g. Reed Elsevier Group plc).

[271] FTC report, page 63.
[272] 'Personal data for the taking', Tom Zeller Jr., The New York Times, May 18, 2005.
[273] 'A Chronology of Data Breaches Reported Since the ChoicePoint Incident', Privacy Rights Clearing House, May 4, 2005.
[274] 'Bank security break may be the biggest yet', CNN Money, May 23, 2005.
[275] 'Searches conducted in hacking probe', CNN, May 19, 2005.
[276] 'Thief steals UC-Berkeley laptop', CNN, March 29, 2005.
[277] 'Bank Loses Tapes of Records of 1.2 Million With Visa Cards', Saul Hansell, The New York Times, February 26, 2005.
[278] 'Personal Data for 3.9 million Lost in Transit', Tom Zeller Jr., The New York Times, June 7, 2005.

While the Federal Trade Commission and other government agencies are researching and informing the US public on the nature of the problem and means of controlling access to their personal information, in the United Kingdom the response has been more limited. The Home Office's initiatives on combating identity theft seem to rely solely on the proposed identity documents,[279] rather than the multi-faceted approach emerging from the US including better regulatory enforcement. In fact, the Home Office announced its identity theft initiative in tandem with the introduction of the draft bill in April 2004.[280]

According to the Home Office's Identity Theft Website, located at www.identity-theft.org.uk:

> "Identity theft occurs when your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud, deception, or obtaining benefits and services in your name."

This definition is not precise, however. The Cabinet Office produced a more rigorous analysis in its Identity Fraud report of July 2002.[281] The Cabinet Office report notes that there is no offence of identity theft or fraud per se, but that it exists in conjunction with other offences. The reasons for identity fraud are usually connected with concealing an existing identity, accruing a financial benefit or avoiding a financial liability. For these purposes, an identity is either stolen or fabricated, and there are myriad ways in which this might happen.

The Cabinet Office report distinguishes three elements of identity:

- *attributed identity*, such as name, date and place of birth;
- *biographical identity*, which builds up over time and includes details of education, employment, personal circumstances, electoral registrations, tax paid and benefits claimed, private sector financial details and transactions; and
- *biometric identity*, such as fingerprints, iris, retina and DNA profile.

The report notes that attributed identity is the easiest to assume, and is usually based on fabricated or stolen documents. Assuming a biographical identity is more difficult because details can only be registered in the appropriate public and private sector databases through a degree of social interaction using a fraudulent persona.

According to the Cabinet Office report, biometric identity cannot be assumed by another individual. However, the report acknowledges that genuine biometric information could be inserted into otherwise fraudulent identity documents. Therefore the risk with this type of identifier lies in the issuing process. Whilst it may have been the case in 2002 when the report was written that biometric identity cannot be assumed or forged, the report is no longer accurate in this respect: as our section on biometrics

[279] 'What is being done', The Home Office, 2004, http://www.identity-theft.org.uk/html/whatisbeingdone.html.
[280] 'David Blunkett: National ID card scheme is the key to the UK's future', Home Office Press Release, April 26, 2004, Reference 159/2004.
[281] Cabinet office, Identity Fraud: a study, July 2002, http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf

discusses, there is now a well-documented lack of certainty in the application and use of biometrics. This has implications both for stolen identities and new forged identities.

The Cabinet Office report is generally helpful and illustrates well, in abstract terms, what we mean by the term 'identity fraud' alongside some potential solutions. The government has, however, largely overlooked the useful distinctions made by the Cabinet Office and continues to refer to identity fraud in vague terms. The Home Office insists on using the emotive term 'identity theft', failing to acknowledge that an identity cannot technically be stolen. Rather it is merely copied and used by a person who is not entitled to do so, which is a form of fraud. This illustrates the persistent confusion, perpetuated by the government, over what identity fraud really means.

Similarly, individuals are most concerned by stories of the 'theft' of accounts, with banking accounts being established in their name. However the Economist reports that this is the least common form of identity fraud because criminals are instead buying and accessing existing accounts.[282]

One reason for obfuscating this definitional issue can be found in the government's insistence that £1.3 billion per year is lost because of the activity of identity fraudsters and that identity cards will substantially reduce this problem. According to the Prime Minister's Official Spokesman:

> "[Identity theft] was a growing crime which costs the economy at least £1.3 billion per year. Criminals were recognising that identities were just as valuable as possessions. There was also the sheer inconvenience factor of having to spend up to 60 hours restoring your records of your identity was stolen."[283]

The Home Office identity cards briefing[284] claims that:

> "An ID cards scheme will help the UK counter … identity theft – by giving people a secure means of protecting their identity – a growing crime which costs the economy at least £1.3bn pa."

The Home Office Identity Fraud Steering Committee states:

> "It is estimated that more than 100,000 people are affected by identity theft in the UK each year, costing the British economy over £1.3 billion annually."

Unlike the situation in the US, identity theft is a major plank of the Government's argument in favour of introducing ID cards, due to the quantitative findings of the Cabinet Office report of 2002. Unfortunately, the report does not carry through the rigour demonstrated in its original definitions into its quantitative findings, which suffer from some weaknesses.[285] Below we will examine what activities were counted as

[282] 'Your money and your life', the Economist, June 2, 2005.
[283] Morning press briefing 1100 BST from 25 May 2005 http://www.number-10.gov.uk/output/Page7548.asp
[284] Home Office Identity Cards Briefing, May 2005 http://www.homeoffice.gov.uk/docs4/Id_Cards_Briefing.pdf
[285] 'Your money and your life', the Economist, June 2, 2005.

'identity fraud' for the purposes of this estimate and calculate the costs of identity fraud in Britain.

Will ID cards help to combat ID fraud?

Identity fraud can have a devastating impact on the victim, whether the victim be the true 'owner' of the identity or someone who suffers as a result of relying on the credentials of a person proffering a fake identity. However, the government's 2002 estimate of £1.3bn has been called into question repeatedly A 2004 conference organised by the Law Society[286] heard that the Cabinet Office report was rather more reticent on the issue of ID cards. The Cabinet Office also admitted that the oft-quoted figure of £1.3bn was derived from a "best guess". When the data is more closely analysed, the conclusions are less certain.

The accounting for the £1.3bn figure resulted from a canvassing of 18 organisations. The Cabinet Office estimated financial losses by quantifying results from only seven.

Table 2 - The Cabinet Office total estimates for Identity Theft, from 2002 report.

Organisation		Costs (£m)	Notes
HM Customs & Excise	VAT	215	Total MTIC fraud £1.7 – £2.6bn (midpoint £2.15bn). Assumes ID fraud is 10% of this.
	Money laundering	395	Based on £490m over 18 months; consistent with £200m in c. London
DH	Health Authorities	0.75	Study done in 2 HAs only – no broader extrapolation permitted 2816 multiple registrations
DWP	Instrument of Payment		No figures
	CSA		No figures
	Child Benefit		No figures
	Pensions & overseas		No figures
	Welfare fraud	35	C 1% of all welfare fraud (£2-5bn)
Home Office	Immigration	36	@ 50 pcm (Heathrow) x 10; £6000 per clandestine entrant
APACS	Credit cards	370	Includes use of counterfeit, lost/stolen cards and card not present fraud – 2001 estimate
Insurance companies		250	Based on £1bn total; 50% pre-meditated; 50% of this being direct ID fraud
CIFAS		62.5	Value of false ID/victim of impersonation fraud (by number of frauds reported)
Total		**£1,364m**	

We analyse these figures in detail below.

[286] Law Society conference 'Identity Cards: benefit or burden', London, March 22, 2004. Report available at http://www.lawsociety.org.uk/

HM Customs & Excise

Two separate figures are given in the Cabinet Office report. The first relates to Missing Trader Intra Community (MTIC) fraud, which essentially involves VAT fraud perpetrated by chains of traders operating within the EU. The Cabinet Office report states that:

> "MTIC fraudsters often operate using false identities or by using front people. It is often difficult to establish the identities of the true directors and identify those committing the fraud. HMCE estimate total losses due to this at between £1.7bn and £2.6bn pa. It is impossible to say how much is directly attributable to identity fraud, but even allowing for just 10% would give a figure of between £170m and £260m pa."[287]

In calculating the loss of £215 million due to identity-related VAT fraud, the report takes the mid-point of the *estimated* total losses, and then *assumes* that 10% of these losses will involve false identities. We are not given the basis of the HMCE total estimates and there is no reasoning backing up the assumption that 10% is identity-related. This is remarkable since the US studies show that in general, identity fraud is less than 3% of all forms of fraud.

Several points of concern arise from these numbers:

- Given that these frauds are perpetrated by EU traders, many, if not most, of these will not be UK citizens and a UK identity card scheme will not touch the majority of the fraudsters causing these losses.[288]
- The actual losses due to MTIC fraud which also involve identity fraud on the part of UK citizens will likely be a fraction of the £215 million claimed in the report.
- Even this amount of loss will not be avoided unless ID cards are demanded *and verified* at the point of transaction. This is not likely to occur since this would require verification against the national identity database and such access is unlikely to be granted to ordinary traders.

The second figure given by HMCE relates to money laundering, with estimates of £395 million being laundered each year. There remain a number of concerns with these figures as well:

- The connection with identity fraud is not established here. It is perfectly possible to lauder money using a genuine identity and the claim that all £395 million is somehow laundered using a false identity remains unproven.
- Although financial institutions are required to know their customer, it is not routine for customers to be asked to prove their identity with each transaction. Unless financial institutions are going to be required to do this and are also given the technological equipment to allow them to cross-check with the national

[287] Cabinet Office, Identity Fraud: a study, July 2002, http://www.homeoffice.gov.uk/docs/id_fraud-report.pdf, p73.
[288] It is also interesting to note that many of the countries referred to within the Cabinet Office report are countries with existing identity card schemes.

identity database, the introduction of UK identity cards will have a smaller impact on money laundering than the government envisions. There are also serious questions of practicality, given that so many transactions are now carried out online.

- To the extent that identification information is required by financial institutions, fraudsters will still be able to launder money based on the use of forged or stolen identity cards from a foreign country. Once again, UK identity cards may have little impact on these figures.

Department of Health

The Cabinet Office registers a loss of £750,000 for the Department of Health, yet it is entirely unclear from the report what this figure relates to. The report admits that there are no reliable figures for avoiding NHS payments or accessing NHS services by non-entitled people using the identities of entitled people. A recent report by the Directorate of Counter-fraud Services is cited, which found incidence of false identities at around the 0.2% mark, yet there is no indication of whether this figure was due to fraud or simple human error.

The Cabinet Office report further claims that a:

> "major problem … is where contractors … claim costs for treating patients who do not exist or who are no longer registered at that practice."

Yet there are no figures, or even estimates, available for this type of fraud. Once again, there is plenty of room for human error, rather than fraud, for example a clerical error in omitting to clear a patient's records once he has moved or is deceased. And while 2816 patients are known to have attempted to register with more than one GP to obtain multiple prescriptions, there is no suggestion of identity fraud in these figures. Rather this involves patients attempting to register more than once, most likely under a real name.

Department for Work and Pensions

No figures are presented for most types of benefit fraud, but the report estimates overall welfare fraud at between £2bn and £5bn. This is an extremely wide estimate, suggesting that little credence can be given to these figures. The report then takes the mid-point, £3.5bn, as the base estimate for overall welfare fraud and then arbitrarily selects a figure of 1% as an estimate for the level of identity fraud associated with general welfare fraud. There is no justification given for this figure of 1%, other than that it seems 'reasonable'. This leads the authors of the report to give a figure of £35 million for identity-related welfare fraud.

Once again, the underlying figures are questionable. Nevertheless, it is likely that some amount of welfare fraud is committed on the basis of a false identity.[289] In evidence 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

[289] A report by John Lettice 'UK ID scheme rides again, as biggest ID fraud of them all' 25 May 2005 comes to the same conclusion. Available at www.theregister.co.uk/2005/05/25/id_bill_mk2_fraud_con/html

fraction of the benefit fraud problem, but calculated that £50 million came from people not being who they said they were when making a claim. In 2002 David Blunkett advised Parliament "benefit fraud is only a tiny part of the problem in the benefit system".[290]

It is certainly credible that an identity card scheme would assist with this type of fraud, since the DWP is a government department and therefore likely to have access to the equipment necessary to cross-check an identity card with the national identity database.

Immigration and Nationality Department – Home Office

The Home Office estimates for immigration costs due to fraudulent documents need to be made a little more explicit. The figures given are:

Table 3 - Home Office Accounting of Identity Theft

Number of fraudulent documents found each month at Heathrow Terminal 3	50
Estimate of detection rate	10%
Estimate of actual number of entrants with fraudulent documents passing through T3 each month	50 x 10 = 500
Estimate of actual number of entrants with fraudulent documents passing through T3 each year	500 x 12 = 6000
Estimate potential cost of each clandestine entrant	£6000
Estimate total cost of clandestine entrants passing through T3 each year	£6000 x 6000 = £36 million

We have no explanation of the Home Office's estimate of £6000 per clandestine entrant, nor for the estimate of a 10% detection rate, but they appear reasonable. To what extent is the introduction of a UK identity card going to solve these immigration problems?

- Almost by definition, these clandestine entrants will be foreign nationals who would not be carrying UK identity card.
- A foreign national wanting to gain access to the UK with fraudulent documents could easily do so by using a fraudulent identity document from another EU country. As an 'EU national', he would be granted entry into the UK and also accorded the normal rights of any EU citizen in another EU country, including access to many government services.

The UK identity card can have little or no impact here.

Association of Payment Clearing Services

According to the Cabinet Office report, in 2001, "losses due to counterfeit cards, lost and stolen cards, and card not present fraud cost the card issuers around £370m." We will leave aside for now the issue of whether credit card amounts to identity fraud or is really simple theft. When discussing identity fraud or theft, credit card fraud is what

[290] 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.

most members of the public most readily think of. It is dubious whether the introduction of UK identity cards will assist with the problem:

- Identity cards could only assist if demanded at the point of transaction, but this almost never happens in the UK (and rarely in any other country for that matter).
- Even if an identity card scheme was introduced and card was demanded at point of transaction, verification would be impossible without the technological equipment giving access to the national identity register. It is highly unlikely that ordinary traders would be granted such access, leaving them vulnerable to fake identity cards in the same was as they are now vulnerable to fake credit cards.
- There are severe practical difficulties in checking identity with every commercial transaction taking place in the UK today. Transaction times may well become unacceptably slow, leading vendors to shun identity checking.
- Increasing numbers of transactions are now take place online and it is not possible for identity cards to be checked in these cases.

For ordinary transactions, the identity card would have little or no impact for the practical reasons just described. For extraordinary transactions, such as large purchases, it is already common practice for financial institutions to check with the genuine card holder in case of credit card theft.

Insurance industry

The Cabinet Office report claims that up to a quarter of all personal insurance fraud is a direct result of identity fraud, giving a figure of up to £250 million. The report admits that this estimate is difficult, so the figure used is already problematic and at the top end of the estimated range. Leaving the figure aside, the report does not make clear the likely effect of an identity card on these losses.

- To have any effect at all, identity cards would have to be required, not only at the time of the proposal, but also with each subsequent claim. Identity is not currently required, the insured being subject in any event to a duty of *uberrimae fidei*.
- UK identity cards would have no effect on that portion of insurance fraud committed by foreign nationals.
- The insurance industry would need access to the national identity database for verification purposes and this is not currently planned.
- The vast majority of insurance business is conducted at arm's length, for example over the Internet, thus precluding any opportunity to examine identity cards. The identity card serial number could be required and then cross-checked, but this would be open to abuse in much the same way as are credit card numbers. It is unlikely the insurance industry will change its business sourcing practices simply to examine an identity card. Its business is risk, and the amounts lost through fraud would be insignificant in comparison to the amounts of lost business due to a requirement of face-to-face transactions and production of identity cards, with its attendant inconvenience.

On balance, for practical reasons the identity card is unlikely to have an effect on the amount of losses due to insurance fraud.

CIFAS, the UK Fraud Prevention Service

CIFAS reports that false identity or victim impersonation fraud accounted for £62.5 million of losses during 2000/1. However, one analysis[291] notes that identity cards have no relevance to much of this type of fraud:

- 'Dumpster diving' forms a significant part of this problem, where personal data contained in papers which have been thrown away are stolen from dustbins outside homes and offices. Such personal data can then be used by the thief to gain goods and services. As justification for the introduction of identity cards, the Home Office points out in its most recent briefing that "A few items stolen from a rubbish bin such as utility bills and credit card statements can lead to huge financial losses as well as distress and inconvenience for victims in putting their records straight."[292] However, identity cards have no relevance here, unless they are checked at the point of a transaction based on stolen documents which, as argued above, is unlikely to happen. The Home Office's own justification is confusing.
- A related problem is theft of mail, particularly invitations from credit card companies, from communal entrance halls. The thief can then apply for the credit card using the details contained in the mail shot. For the same reasons as above, identity cards would not assist with this problem.
- Any fraudulent transaction which takes place at arm's length, for example over the Internet, will not be scotched by an identity card.
- Although some of the quoted £62.5 million of losses may be addressed by identity cards, it is likely that the majority of it will not because it is not feasible for identity cards to be demanded and then verified with each commercial transaction.

In summary, the only category of identity fraud cited by the Cabinet Office report on which identity cards may have a significant impact is the welfare fraud estimated to cost the Department of Work and Pensions £35 million a year. However, in the "Government's Reply to the Fourth Report from the Home Affairs Committee"[293] the government states that the DWP already has robust identity procedures in place and identity cards would be used "to maintain or even enhance that level of security". This suggests that identity cards are hardly even necessary here. When compared to the Government's claims of £1.3 billion, all this questions the Government's strategy for relying on identity fraud as the basis for identity cards. The identity cards scheme is projected to cost billions, and it does not appear to be a proportionate response when careful consideration is given to the limited ways in which it might assist.

[291] 'UK ID scheme rides again, as biggest ID fraud of them all', John Lettice, 25 May 2005 www.theregister.co.uk/2005/05/25/id_bill_mk2_fraud_con/html
[292] Home Office Identity Cards Briefing, May 2005 http://www.homeoffice.gov.uk/docs4/Id_Cards_Briefing.pdf
[293] October 2004, Session 2003-4 HC 130

Will identity cards facilitate identity fraud?

Quite apart from the overall cost to the taxpayer of initiating a national identity card scheme, recent estimates of the cost to individuals of buying an identity card run to £93 per person.[294] This is, quite simply, beyond the means of many citizens and may constitute a further incentive for criminals to invest in pioneering identity card forgery. Perhaps an easier route than forgery is persuading an insider in the identity card issuing centre to issue a false identity, either with money, through blackmail or through collaboration. The deterrents intended to stop this type of activity which are contained in the Bill would only be effective if there was a significant fear of apprehension. Yet insider fraud is endemic to organisations of all forms.

Another possibility is that the guardians of the database themselves make a security error, opening up the records of many ordinary citizens to an unscrupulous few. There is plenty of form for this sort of thing from the biggest of businesses, such as Choicepoint and Bank of America.[295] Given the fact that government websites are premium targets for malicious hackers, it is reasonable to assume that, sooner or later, the database's security will be breached, probably on multiple occasions. This opens up the possibility of existing details being stolen or changed, either accidentally or otherwise, and it is possible that someone might find a way to create new records. The Prime Minister's Official Spokesman has said that:

> "The national register of information would be protected and people had that assurance."[296]

In guaranteeing that the national identity database will be secure, the government is ignoring precedent. No database's security can be guaranteed, particularly one that contains this amount of information, which will likely be accessed millions of times every day, with data changed on thousands of individuals every day, and particularly when this information is so valuable.

One of the worries of a centralised database which is supposedly secure is that, if for some reason an ordinary citizen's identity information is changed and becomes inaccurate, he may not know it for a considerable time. The studies in the US indicate that many forms of fraud remain unknown to the victim for a number of years.[297] Once he does find that his record is inaccurate, it may be too late if he has already suffered some detriment. If the cultural perception is that the database is 'secure' there may be an effective reversal of the burden of proof such that the victim of the inaccurate record must effectively prove that it is inaccurate. Section 12 of the Identity Cards Bill (notification of changes affecting accuracy of Register) does nothing to assuage these fears, requiring the individual to provide proof that the entry in the register is inaccurate and that the information he is putting forward is accurate. In our extensive experience with information systems across many organisations, we have never found a database free of errors and inaccuracies; limiting these problems is one of the key purposes of data protection law.

---

[294] Home Office Identity Cards Briefing, May 2005 http://www.homeoffice.gov.uk/docs4/Id_Cards_Briefing.pdf
[295] http://www.securityfocus.com/columnists/305
[296] Morning press briefing 1100 BST from 25 May 2005 http://www.number-10.gov.uk/output/Page7548.asp
[297] FTC report.

Another strategy involves the increased monitoring of stolen documents. The Cabinet Office notes the case of the Netherlands, which at the time of writing the report, did not have a national identity card.

> The Netherlands has no unique identifier for its 16 million citizens, probably because of a widespread antipathy towards identity cards resulting from historical resonance from World War II occupation. But it does have well developed systems for keeping track of stolen and lost documents: the Verification of Identity System (VIS).[298]

Details of around six million documents are held in the central database. This database can also be accessed by private sector organisations. This is a far more proportionate solution: monitoring the minority of documents for a minority of citizens based on the fact that a crime has occurred, rather than monitoring the general population in the eventuality of a crime. It is also technologically feasible.

The Home Office Identity Fraud Standing Committee has an excellent website, www.identity-theft.org.uk, detailing common sense advice, on how to prevent and recover from identity fraud. If all citizens followed this advice, there would be a much reduced need for alternative solutions, such as the government's proposed identity cards and a national identity database. Promoting the contents of this website would be a much cheaper, safer and more proportionate solution to the problem. And until appropriate research is conducted on the nature of the threat of 'identity theft', it would be hazardous to create a massive 'solution' to a poorly understood problem.

[298] Cabinet Office report, page 40.

9

Policing and ID

> "It is obvious that the police now, as a matter of routine, demand the production of national registration identity cards whenever they stop or interrogate a motorist for whatever cause. Of course, if they are looking for a stolen car or have reason to believe that a particular motorist is engaged in committing a crime, that is one thing, but to demand a national registration identity card from all and sundry, for instance, from a lady who may leave her car outside a shop longer than she should, or some trivial matter of that sort, is wholly unreasonable. This Act was passed for security purposes, and not for the purposes for which, apparently, it is now sought to be used. To use Acts of Parliament, passed for particular purposes during war, in times when the war is past, except that technically a state of war exists, tends to turn law-abiding subjects into lawbreakers, which is a most undesirable state of affairs. Further, in this country we have always prided ourselves on the good feeling that exists between the police and the public and such action tends to make the people resentful of the acts of the police and inclines them to obstruct the police instead of to assist them ..."
>
> - Lord Goddard, *Willcock v. Muckle*, June 26 1951

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

As Lord Goddard noted, identity cards will necessarily have an influence over the relationship between the public and the police. It is vital that we understand potential changes to this relationship. There are other important effects that we must also understand, including what will happen to the police themselves when ID cards are introduced.

Proponents of identity cards frequently argue that the UK is one of the few countries within Europe yet to institute ID cards. They imply that identity cards do not lead necessarily to illiberal governance. Opponents of identity cards point out instead that it is rare for common law jurisdictions to implement ID cards. This group implies that there is something alien – perhaps "un-British" - about identity cards.

At a meeting at the Law Society in 2004, Stephen Harrison, the policy head of the Identity Cards team at the Home Office, was asked whether ID cards are alien to our culture and our traditions. Mr Harrison conceded that they may have been at the turn of the century, but the Government believes that times are changing and that people should change with them.[299] This debate is not likely to lead to a consensual solution.

It is more important, and more relevant, to understand the form of changes being introduced to Britain's methods of policing. As ID cards are promoted for use in combating fraud and illegal immigration, and to permit the police to gain access to the national identity register, we must consider the effects of these powers and measures on the practice of law enforcement.

This section questions the effects that the cards, as with other technologies, have on policing in the United Kingdom. It is not necessarily the case that advances in technology always lead to an advance in the efficiency of the UK's law enforcement agencies.

Demands from the Police

Assertions that identity cards would be a useful tool 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 damage good relations with the public.

According to police organisations, most economically developed countries find that 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 reduce the incidence of crime, or enhance 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, although 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 in some way being observed. Sometimes, cards are proposed as a means of reducing the opportunity for crime. In 1989, the UK government moved to introduce machine-readable ID cards to combat problems of violence and hooliganism at football grounds. The premise was that cards would authorise the bearer to enter certain grounds and certain locations, but not others. The card could also be cancelled if the bearer was involved in any trouble at a ground or related area. The proposal was scrapped following a report by the Lord Chief Justice that claimed that such a scheme could increase the danger of disorder and loss of life in the event of a catastrophe at a ground.

[299] 'IDENTITY CARDS: BENEFIT OR BURDEN?', The Law Society, Monday 22 March 2004, Report of the Debate.

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 bankcards are available as blanks in such countries as Singapore for several pounds. Within two months of the issue of new Commonwealth Bank high security hologram cards in Australia, near-perfect forgeries were already in circulation.

Even the police agree with this assessment and recognise the potential for forgery and fraud within an ID system. According to ACPO:

> "It should be recognised that whatever scheme is introduced a criminal somewhere will try to find a way around, or through, it. Therefore there will have to be a system of continual monitoring and review to adapt and change procedures where necessary."[300]

This conundrum has been debated throughout the world. It is based on the simple logic that the higher an ID card's value, the more it will be used. The more an ID card is used, the greater the value placed upon it and, consequently, the higher its value to criminal elements.

The potential for forgery and fraud is one of the most persuasive arguments against identity cards in the United States. There is considerable concern over the problem of identity theft, but many observers believe that the centralization of personal information would increase the risk of identity theft, fraud and the use of personal data by organised crime.

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 draw certain inferences by assessing crime trends across Europe.

[300] ACPO memorandum to the House of Commons - Home Affairs - Written Evidence, April 2004, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we02.htm

Country	Recorded Crime	Drug - Trafficking	Homicides	Terrorist Incidents[301]	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[302]	- 10	- 6	1.45	165 uk[303]	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

Table 4 - Crime Recorded by Police in EU Countries, 1995 - 1999[304]

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.

In recent years the UK police have been active in their support for ID cards. It is understandable that Ministers continually point to the support from the police. In general the police see many benefits:

> "In principle ACPO believes that the introduction of a national ID card scheme could deliver considerable benefits. Many areas of policing would benefit, not least the ability of the police to better protect and serve the public. As with many of our partners we have never seen ID cards as a panacea—but we do believe they could be a

[301] Incidents from MIPT Terrorism Knowledge Base, source: www.tkb.org/Home.jsp.
[302] England and Wales.
[303] N. Ireland had 618 incidents.
[304] International comparisons of criminal justice; 1999 spreadsheet RDS website issue 6/01 Gordon Barclay et al., May 2001, source: www.homeoffice.gov.uk/rds/.

> key part of broader strategic solutions to a range of community safety issues."[305]

The Police Federation also picked up on the dangers of seeing ID cards as a panacea:

> "Identity cards should be kept in perspective. They are not a panacea. Nonetheless they could be part of a broader solution and would make a police officer's job on the street easier".[306]

The police generally see benefits in the use of biometrics, though ACPO believes in the potential use of DNA in the identity card system:

> "Technological developments provide opportunities for the exploration of new uses for biometric identification. ACPO sees benefit in the use of fingerprint, iris or DNA identification. [...] The biometric data stored on the ID card should [...]
>
> - Create minimal bureaucracy for the applicant and for the authorities managing and having access to the data.
> - Be readily, quickly, accurately available to the authorities requiring access to the information—this element is particularly important to operational police officers.
>
> "ACPO is currently contributing to the interdepartmental work on the development of reliable and robust biometric identifiers. The police are involved in the trailing of portable identification technology through Project Lantern. ACPO is aware that the issue of the numbers and cost of portable readers required to ensure that the scheme is efficient and effective is significant."[307]

This appears to be part of a general belief that "[t]he more information you have, the wider the benefits can be." The police associations envisage that this information will be available on the streets for use with stop and search powers, and describe the promise of stop-and search and ID cards as follows:

> "Repeat stops of individuals could become a thing of the past if "mobile readers" were able to identify individuals who had been stopped previously.
>
> "On-street identification would also assist with (people) engaging in anti-social behaviour. For example, immediate identification of individuals in breach of Anti-Social Behaviour Orders (ASBOs), or Football Banning Orders, would accelerate the administration of justice and support legislation in this area. Similarly the ability to immediately identify and help those suffering from mental illness or

[305] 'Memorandum submitted by the Association of Chief Police Officers', submitted to House of Commons - Home Affairs - Written Evidence, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we02.htm
[306] 'Memorandum submitted by the Police Federation of England and Wales', The Police Federation, House of Commons - Home Affairs - Written Evidence, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we45.htm
[307] 'Memorandum submitted by the Association of Chief Police Officers', submitted to House of Commons - Home Affairs - Written Evidence, http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we02.htm

> medical problems would be of great benefit to the individual and the emergency services.
>
> "Public Disorder: The ability to quickly verify personal identity at public order or critical incidents would be invaluable. Quick validation of the details of witnesses and suspects would again lead to significant service improvements to those involved in police enquiries and those carrying out investigations.
>
> "Bureaucracy: As can be seen from the above examples the potential for reducing policing bureaucracy are significant. "Portable readers" of the biometric information contained on ID cards would undoubtedly save time and cost for the public and police officers."[308]

Similarly, the Police Federation claims that

> "Stop and Search procedures would be greatly improved following the introduction of identity cards. Firstly, police officers would be able to identify individuals beyond doubt. Secondly, curtailing the time taken to conduct stop and searches would enhance an individual's liberty. Thirdly, this time saving would also greatly benefit the police, allowing officers to spend more time policing the streets. If identity cards were compatible with a system of police smart card readers, officers would simply be able to check if and when they or their colleagues had stopped an individual before. This would ensure that the same individuals are not repeatedly searched within a given time-period."[309]

The police therefore envisage some form of tracking capability to monitor who has been stopped and searched.

It is important to recall at this point that the police are calling for compulsory ID cards, with a consequent compulsion to carry them:

> "Our views on compulsion to carry ID cards remain unchanged. The overwhelming view within ACPO is that the ID card scheme should operate on a "compulsory" and "universal" basis. Whilst we understand the rationale behind the proposed incremental approach we believe there are benefits to be accrued if individuals were required to carry or produce the card upon request to an appropriate authority. Those engaged in criminal activity will not be deterred if the scheme is not robust."[310]

ID Cards would also make the enforcement of ASBOs "far easier".[311]

---

[308] Ibid.
[309] Police Federation to the HAC.
[310] ACPO to the HAC.
[311] Police Federation to the HAC.

However, due to recent legislative changes compulsion to carry identity cards is becoming a redundant polemic: the police now have powers to take fingerprints - even at the roadside - when the technology is available.[312]

Effects on the Police: Will Increased Technology Help the Police?

According to ACPO:

> "We have long argued for greater investment in technology and the case and custody system being developed to allow the police, courts and the CPS to communicate electronically will have a major impact on efficiency and saving the time of front line police officers. It will also fundamentally improve the quality of service to the public."[313]

There is a false presumption that more technology (and more spending) means better police performance.[314] Indeed, technology may transform policing. However, according to research, increases in technology budgets tend to result in a waste of funds because the technologies are not used effectively. On occasion, the results are even hazardous to policing culture.

Technology is commonly seen as the holy grail of policing and, as such, the drive of current mainstream research and policy is to see how to pump more technology into police work. Numerous studies have argued that the increased use of technology leads naturally to better efficiency, faster response times, better resourcing and organisation of policing, and improved community safety. Such studies lead us to believe that the way forward is to increase the capacity and number of technologies, but this view ignores the complexity of both the police mandate and of technology. Other studies have pointed to the alienation of police officers, the invasion of privacy, excessive social control and excessive mechanization of the process of policing that results from an over-enthusiastic application of new technology.

The use of technology can and does alter police interaction with people and environments. If a new technology is to have significant effects on the police and their mandate, then comprehensive and far-sighted research is required before it is introduced. An uncontrolled change of mandate would be dangerous for society because it would distort the commonly agreed balance between freedom and social control.

Policing in Britain

The primary mandate of the police in Britain is to uphold order in society. Any discussion of the application of advanced technologies must be seen in the light of how they might unbalance the role police have in upholding this order. This is quite unique to the United Kingdom.

[312] ACPO News, http://www.acpo.police.uk/news/2004/q3/Police_powers.html.
[313] 'ACPO RESPONSE TO HOME AFFAIRS SELECT COMMITTEE REPORT', Association of Chief Police Officers, March 10, 2005.
[314] 'Law Enforcement Information Technology: A Managerial, Operational, and Practitioner Guide', Jim Chu, CRC Press, 2001.

Internationally the mandate of police is primarily seen as the enforcement of order, where 'order' refers to law enforcement. However, this definition is not appropriate for the mandate of the police in the United Kingdom. The mandate of UK police is instead the implementation of order through the act of peacekeeping, where peacekeeping is the maintaining of order within agreed social principles. Peacekeeping relies on the discretion of police officers and on their common sense, much like the work of social workers. Thus the essence of police work is contained in common sense, discretion and a situational understanding which acknowledges the unwritten norms of a community.

In the UK, these agreed social principles are reflected in common and statutory law. More importantly, they are reflected in a non-codified, relatively fast changing system of localized socially accepted norms of behaviour.[315] These socially acceptable norms of behaviour influence police work as much as common and statutory law.

What makes peacekeeping different from law enforcement is the flexibility provided by the extra consensus reached between the community and the police. Seen in this light, the police are not anti-crime machines but priority seekers. Therefore, the accepted norms of the community are the benchmark from which they deal with a community.

According to field studies documenting police activities, police officers exercise their mandate through talking to individuals (both giving suggestions to victims and threatening arrest for an inappropriate behaviour), finding solutions or mediations amongst parties, withholding people with dangerous behaviours, and providing a sense of presence.

Technology and the Police Mandate

It would be easier to assess the value of technology strategy in police work if we were able to define more precisely the ends to which the technology would be applied and in what ways it could be expected to work.[316]

Whilst the police mandate is inherently flexible it is not necessarily wise to have that flexibility dictated by the characteristics of the technology that the police employ. Technology may provide a subtle shift in the role of the British police sufficient to displace them as peacekeepers and transform them into a law enforcement machine. This would create a significant change in the policing of Britain.

The potential of technology to improve the effectiveness of crime control, as well as to enhance the professional status and organisational legitimacy of the police, has created a longstanding affinity between technology and police work.[317] The image and practice of the police is shaped by information technologies.[318]

[315] Manwaring-White, S. (1983). The policing revolution : police technology, democracy and liberty in Britain. Brighton, Harvester.
[316] Manning, P. K. (1997). Police work : the social organization of policing. Prospect Heights, Ill., Waveland Press.
[317] Manning, P. K. (2003). Policing contingencies. Chicago, University of Chicago Press.; Ericson, R. V. and K. D. Haggerty (1997). Policing the risk society. Toronto ; Buffalo, University of Toronto Press.
[318] Manning, P. K. (2003). Policing contingencies. Chicago, University of Chicago Press.

In operational terms, police forces in Britain are at the forefront of the use of information technology to support all aspects of their service delivery.[319] This development has been labelled *e-policing* and is strongly supported by the government. E-policing provides information to officers through mobile computing. In police terms, this means immediate access to police databases through multiple technologies, and is arguably an efficient use of resources.

To better understand the implications of technology upon British policing we can refer to a key study from Canada.[320] The information technology supported auditing, monitoring, and managing risk.[321] However, the reporting system curbed individual officers' discretion while supervision of their activities intensified. The study concluded that the use of information and communication technologies changed the structural aspects of policing by limiting individual discretion, levelling hierarchies and questioning traditional divisions of labour. Traditional police command and control structures were replaced by mechanisms that – through surveillance - regulated police conduct.[322]

Apart from issues relating to the transformation of police culture and operations, we should also consider the fact that technologies may fail. When this happens in the policing environment, the consequences are hazardous and expensive. A study of the use of technology in the 1970s and 1980s reported disappointing results of various technological innovations such as computer-aided dispatch systems, attempts to reduce response time, car locator and tracking systems, crime mapping techniques, and management information systems, all of which failed to reach expectations and in some ways exacerbated original problems. The study concluded that new technologies have less positive effects on police practices than their proponents predict.[323]

It is fair to say that information technologies are employed not only because of their functions, but also because of the image that the police seek to transmit. Such an approach can result in costly endeavours that inhibit both cost recovery and the achievement of stated objectives.

Toward the End of Discretion

The strength of the police mandate is contingent upon the relationship officers have with a community. Technology can become a burden that endangers the essence of policing by framing a one-dimensional view of the world. It is possible that police work does not have the close affinity with technology that one might imagine.

The administration of order is an act of peacekeeping that depends chiefly on discretion and common sense; these attributes open up a range of possibilities for the administration of order.[324] Notable exceptions aside, the British police have a tradition of restraint in the act of maintaining public order – a fundamental characteristic that the

[319] Povey, K. (2001). Open All Hours. London, HMIC**:** 193.
[320] Ericson, R. V. and K. D. Haggerty (1997). Policing the risk society. Toronto ; Buffalo, University of Toronto Press.
[321] Ibid.
[322] Ibid.
[323] Manning, P. K. (1997). Police work : the social organization of policing. Prospect Heights, Ill., Waveland Press.
[324] Davis, K. (1969). Discretionary Justice. Baton Rouge, Louisiana State University Press.

first police commissioner explicitly articulated in connection with the issue of authority. The principles of policing in Britain are based upon flexibility – or discretion – in the execution of the law, giving primacy to common rather than statutory law. Great reliance is placed on professional competence within police forces.

Mobile technologies may give officers exceptional coordinating and documenting power whilst promoting an internal accountability through the surveillance of police action. But they also displace the rules of engagement with society and promote a mechanistic, administration-oriented form of law enforcement, dwarfing the essential – and subtle – peacekeeping function that communities seek.[325]

Social control is a property of states of social relations and not a thing imposed from the outside. Thus:

> "the police ultimately depend on the voluntary compliance of most citizens with their authority…the combination of strength and restraint became the foundation of the London Bobby's public image."[326]

Although it might be argued that mobile technologies have not entirely removed discretion, it is precisely because of the symbolic value of these technologies that discretion might be at risk. As argued by many researchers[327], police officers tend to act in a different way when they feel they are being observed – be it by fellow officers, other citizens or the media. Usually their behaviour, when under surveillance, tends towards a standardised imposition of order. This may lead to mechanistically stopping and demanding fingerprints or iris scans merely because the technology is available and the law appears to encourage such conduct.

By comparison, the American system, from which most technological innovations in policing are borrowed, has always been action oriented and predicated upon perceptions of the public as a dangerous adversary.[328] It is not a leap of imagination to assume that we are slowly transforming our own police toward the American system, particularly as we adopt American techniques and technologies. We are driven by the spectre of fear through the narrative of dangerous stories.[329] It is common to think of police work in terms of the most extreme incidents they attend; however, these represent a small part of the work of a police officer, and such scenarios should not form the basis upon which technologies are designed and built.

This is not to suggest that police should do away with mobile – or other – technologies that may facilitate the act of peacekeeping. However, it is within the use, or envisaged use, that the problems of particular technologies lay. There may be some essential parts of the police function where the use of technology should not be encouraged.

While a technological attitude on an abstract level may makes perfect sense in a police bureaucracy, the perception that all use of technology is good tends to obscure the

[325] Goldstein, H. (1964). 'Police Discretion: The Ideal vs. the Real.' Public Administration Review(23): 140-148. Goldstein, H. (1990). Problem-oriented policing. Philadelphia, Temple University Press.
[326] Newburn T (2004) Policing: Key readings. London, Willan Publishing page 32 .
[327] Manning, P. K. (2003). Policing contingencies. Chicago, University of Chicago Press
[328] Manning, P. K. (1997). Police work : the social organization of policing. Prospect Heights, Ill., Waveland Press.
[329] e.g. Glassner B (2000) The Culture of Fear. Basic Books.

uncertain and contradictory role of police officers in a democratic society and to portray them as functionaries with a standardized task that relies on documentation and coordination.[330]

There is also the risk of leaving decisions about the practical administration of justice to system designers who know little about operational realities. A leading expert[331] states that there are four modes of policing conduct implicit in the design of technology that do not reflect the practice of policing:

> "the primary objective of the police is crime control, police activity is one of the primary determinants of crime levels, the police are organized and operate as a rational bureaucracy and police strategies are primarily those of deterrence".[332]

Accordingly if technologies are not properly viewed, managed and used they can shift police attention to inappropriate measures, raise misleading public expectations, and impose restrictions on police operations.[333]

Our own fears are leading us to encourage the police to adopt technologies that they believe they need. But by doing so we are transforming the police and facilitating the end of discretion, a key component of British policing culture. According to one leading expert,

> "The good cops were street-corner politicians who controlled their beats in the common interest by selectively enforcing the rules, sometimes letting off people for behaviour for which others were arrested. The not-so-good cops were those who either retreated from the confusion and dangers of the street altogether or mechanically applied every rule as the law required."[334]

Although one might not agree with this particular definition of the *good cop*, the concept of the *not-so-good cop* resonates in light of the previous discussion. It further suggests that the current drive towards optimisation, standardisation and surveillance might not produce the most attractive environment in terms of citizens-police relations. This is supported by the most notable difference between continental and British police systems: the surveillance of the civilian population.[335] Thus, historically, the British police have been concerned with preserving the liberties of the population, not only in actual terms, but also symbolic terms.

The implementation of ID cards and the national register is likely to involve substantial implications for policing in Britain. Often it is assumed that the increased use of technology will aid policing, but this ignores the fact that the use of technology

[330] Goldstein, H. (1990). Problem-oriented policing. Philadelphia, Temple University Press.
[331] Hough, M. (1980). 'Managing with Less Technology: The Impact of Information Technology on Police Management.' British Journal of Criminology 20(4): 344-57.
[332] Ibid, p. 351-52.
[333] Sparrow, M. (1991). 'Information Systems: A Help or Hindrance in the Evolution of Policing?' The Police Chief 58(4): 26-44.
[334] Wilson, J. Q. (1989). Bureaucracy. New York, Basic Books, p344.
[335] Chapman, B. (1970). Police State. London, Pall Mall.; Tobias, J. (1972). 'Police and Public in the United Kingdom.' Journal of Contemporary History **7**(1): 201-19.

transforms the relationship between the police and the public. It also minimizes discretion, a cornerstone of British policing. Finally, it may provide access to vast data stores, exacerbating the public's already problematic perception of 'stop and search' powers.

10

Race, Discrimination, Immigration and Policing

The relationship between Identity Cards and ethnic profiling is strong, yet poorly studied. Governments are keen to ensure that their new policies do not discriminate unfairly against minority groups. This is particularly the case with the Identity Cards Bill. Throughout the world, identity cards are associated with discrimination. In almost every country with identity cards, individuals may be compelled to produce those cards upon demand by the police. In every country that grants this power to their police, questions inevitably arise as to whether this power is used more, and perhaps disproportionately, against immigrants, minorities, or other selected groups. To avoid the appearance of establishing a similar system in the UK, despite all the rhetoric of harmonising with other countries' practices, the Identity Card Bill does not grant police the power to compel production.

Any position opposed to the introduction of the Identity Cards Bill on grounds of discrimination will inevitably be countered by those in favour of the scheme with the argument that police powers will not be extended, and that it is not mandatory for individuals to carry the card on a day-to-day basis.

This gives rise to two significant inconsistencies with the Government's approach. Firstly, the bill fails to satisfy the demands of the constituency of the police sector, even though the Government claims to be representing the demands of the police. Secondly, the Government claims that the card will combat illegal immigration, when the bill as it stands will do little to combat illegal immigration unless it requires compulsory identification and production powers. The first point will be dealt with under function creep, and the second will be discussed in its own right.

Function Creep towards Production

Despite the Government's claims that the Identity Card Bill has been designed to satisfy the demands of police, it is carefully designed to prevent the police from getting what they have asked for. This may be the intention at present in order to satisfy critics, but it ignores both history and legislative intention.

Many identity cards start out at first without a power to compel production. The card used in the Second World War was originally designed to administer national service, security and rationing. The police did not have the right to demand that individuals

carry ID, though when stopped they could be asked to produce it at a police station within two days. In the case of *Willcock v Muckle*, Mr Willcock refused to go to the police station with his ID card. By the time of Willcock's refusal to comply, the purposes for the scheme had extended from the original 3 to 39, including the prevention of bigamous marriages.[336]

The Government has made frequent claims that the reason for implementing identity cards in the UK is that the police have requested it. The Police Federation informed the Home Affairs Committee that in calling for identity cards, the police are also asking for the power to compel production:

> "Stop and Search procedures will be greatly improved following the introduction of identity cards."

Similarly, if the aim of the card is to combat illegal immigration, it must be combined with a stop and search component if it is to be effective. It must also be compulsory to have the card in order to allow for immigration checks at work. If the Government is truly aiming to combat illegal immigration, then it will eventually have to introduce production powers. In order to meet its legislative goals, the law will have to be changed, 'ramped up', to a compulsory regime.

During the House of Commons Debates on Monday 20th December 2004 on the topic of the Identity Cards Bill, the Home Secretary was questioned by the Conservative MP, Francis Maude, on this exact issue.

> "Mr. Maude: The suspicion that many of us have and the reason why we feel that the police are so enthusiastic about this is that it is an incremental process. First, there will be a voluntary scheme. Gradually, as the money will have been spent on it, it can then be argued that the only way of getting value for that money is by introducing compulsion, which will then mean carrying the card at all times. It is a salami-slicing process, which is why so many people are very suspicious about it. "
>
> "Mr. Clarke: I have no sympathy with the "thin end of the wedge" argument. People may have argued when national registration of births was introduced in 1837 that they would at some time arrive in a society in which everybody operated in a "1984" type of world. That is nonsense; it simply has no substance."[337]

There is some substance to Mr Maude's argument: Studies demonstrate that 'compulsion by stealth' is a likely consequence.[338] Concerns regarding function creep

[336] 'Supplementary memorandum by the Information Commissioner (VOT 23(b))', submitted to the Select Committee on Constitutional Affairs, http://www.publications.parliament.uk/pa/cm200405/cmselect/cmodpm/243/243we28.htm

[337] Hansard, House of Commons debate, December 20, 2004.

[338] 'POLICING THE COMMUNITY: The Impact of National Identity Cards in the European Union', Adrian Beck and Kate Broadhurst (Scarman Centre for the Study of Public Order), 1998, published in the *Journal of European Migration Studies*.

are understandable, particularly in light of Government reliance on secondary legislation.

During the same debate, the Liberal Democrat Spokesperson on Home Affairs pointed out the Government's intention, expressed in their regulatory impact assessment, that service providers should only ask certain groups for proof of identification will not merely create cultural problems, but also serious legal problems. He stated:

> "Linking illegal working to ID cards will lead – bluntly – to people who do not look British being stopped".

Douglas Hogg (Conservative MP) also reiterated these concerns:

> "Bearing it in mind that the stated purposes of the scheme are to combat terrorism and illegal immigration, we can also be sure that those powers will be used most vigorously against ethnic minorities".

Jeremy Corbyn (Labour MP) picked up on the same theme, voicing fears of "the profiling of individuals to decide whether they should be stopped and searched" and that "various agencies will decide to check whether people with certain ethnic attributes have a card". David Curry (Conservative MP) echoed their concerns about the difficulties that could be caused by too great a focus upon members of minority ethnic communities.

The Current Environment of Race and Police Powers

For several years, the possible existence of a subculture of 'institutional racism' in the operations of the UK police force was investigated through a number of inquiries. These studies, most notably the 'The Stephen Lawrence Inquiry Report', attempted to prescribe a number of remedies. The issue of 'stop and search' by the police is most often identified as a concrete manifestation of such racism. Annual figures point to the disproportionate exercise of these powers towards ethnic minority groups. In this section we will primarily deal with the main powers used to stop and search individuals and then proceed to examine the predicted impact that the introduction of identity cards will exert on race relations.

The most common power used to conduct a stop and search is provided by s1 of the Police and Criminal Evidence Act 1984 (PACE). This allows a police officer to search an individual if he has *reasonable grounds* to suspect that he will find stolen or prohibited articles. A further power to stop and search is provided by s60 of the Criminal Justice and Public Order Act 1994. If a police officer, of or above the rank of Inspector, *reasonably believes* that incidents involving serious violence may take place or that persons are carrying dangerous instruments or weapons without good reason, he may give an authorisation for a period of up to 24 hours, in any locality in his police area, that police constables may stop and search any individual or vehicle for offensive weapons or dangerous instruments, whether or not he has any grounds for suspecting that the individual is carrying articles of the kind mentioned.

The third important power to stop and search is provided by s44 of the Terrorism Act 2000. This grants police officers the power to stop and search for articles that could be

used for terrorism, although an officer *does not need grounds for suspecting* the presence of such articles to use the powers. Prior authorisation to exercise the power within a given area must be sought by the relevant officer of rank for up to a period of 28 days. However, the authorisation may be renewed. A prime example of this can be seen in London, which has been continuously designated as such a zone since February 2001.[339]

Criminal Stop and Search

The above powers to stop and search are generally governed by Code A of the Codes of Practice that were released in accordance with PACE. The Codes have been particularly important in informing both the police and the public as to the proper exercise of police power. A breach of the Codes does not automatically render police action unlawful as this depends upon the severity of the breach. Nor does it necessarily render any evidence obtained from the improper actions of the police inadmissible in a subsequent trial. A breach of the codes should at least initiate some form of disciplinary action against the offending police constable and, most importantly, clarify the standards that all officers should adhere to.

Code A specifically covers the exercise by police officers of statutory powers to stop and search. The Code is too lengthy for detailed examination in this report; [340] however, the most relevant provisions are outlined below:

- Rule 1.1 states that the powers to stop and search must be used without unlawful discrimination and emphasises that the Race Relations (Amendment) Act 2000 makes it unlawful to discriminate on the grounds of race, colour, ethnic origins, nationality or national origins when using these powers.
- Rule 3.8 states that prior to the commencement of any search the police officer must inform the individual of his name and the police station to which he is attached, the legal search power which is being exercised, the purpose of the search and where relevant, the grounds for the search (the latter is not applicable for searches under s44 of the Terrorism Act 2000).
- Rule 4.1 states that an officer who has carried out a search must make a note of it at the time, unless there are exceptional circumstances that would make this wholly impracticable. If a record is not made at the time, the officer must do so as soon as possible afterwards.
- Rule 4.2 states that a copy of the record must be given immediately to the person. The officer may ask for the name, address and date of birth of the person searched although there is no obligation on a person to provide these details and no power of detention if the person is unwilling to do so.
- Rule 4.3 states that the record of the search must contain the name of the person searched or if this is withheld a description; the person's ethnic background; the date, time and place that the person was first detained and the date, time and place that the person was searched; the purpose of the search; the ground for making it (or the authorization); the outcome and the identity of the police officer making the search.

[339] 'The Queen on the Application of Gillan and Anr v The Commissioner of Police for the Metropolis and Anr', Court of Appeal (Civil Division), 29th July 2004. Paragraph 13.
[340] The Code is available in full at http://www.homeoffice.gov.uk/docs3/pacecode_a.pdf.

Despite the supplementary provisions of PACE to stop and search powers, controversy frequently surrounds the exercise of these statutory powers due to the disproportionate number of people from ethnic minorities being subject to stops. Figures released by the Home Office[341] and subsequent comparisons, reveal that between 2001/2002 and 2002/2003 the number of recorded stop and searches rose by 17% for white people, but by 36% for Asian people and 38% for black people. However, the largest increase was for 'Other' minority ethnic groups at 47%. Such figures do not clearly demonstrate the disproportionate increases that have been experienced since September 11th 2001, but an analysis from the organisation 'Statewatch'[342] highlights the following:

- Since 2001/2002, stop and searches have increased by 66% for black people and by 75% for Asians compared to less than 4% for white people. Of further importance is the observation that the largest increases have been experienced by those who are classified by the police as 'Other' (90%) or 'Not Known' (126%).
- In 2003/2004, 14 individuals per 1,000 of the white population were subject to stop and searches as compared to 93 per 1,000 of the black population and 29 per 1,000 of the Asian population.
- Following the Metropolitan Police Authority's (MPA) Stop and Search Scrutiny, the MPA was forced to conclude that 'stop and search practices continue to be influenced by racial bias'[343].
- Between 2001/2002 and 2002/2003, police stop and searches under terrorism legislation rose by 302% for Asian people, by 230% for black people and by 118% for white people.[344]

The Home Office has attempted to address this issue with the creation of the 'Stop and Search Action Team' (SSAT) whose aim is to ensure that police forces use their stop and search powers as 'fairly and effectively as possible to prevent and detect crime' and 'to increase the confidence that the black and minority ethnic community have in the way the police use this power'[345]. The SSAT strategy 2004/2005[346] brought together views from various sources, including 'The Stephen Lawrence Inquiry Report' and the 'National Criminal Justice Board', in an attempt to influence the exercise of stop and search powers and their effect upon community relations.

The SSAT strategy envisaged, amongst other things, that by 1st April 2005, all forces should be recording stops (in addition to stop and searches) and a revised Code A would also encompass 'stops' in its guidance. The strategy revealed that the 'Home Office Research, Development and Statistics Directorate' (RDS) carried out an evaluation of recording stops, and asserted that it had encouraged officers to be more appreciative of issues surrounding ethnic origin. Simultaneously, however, the RDS revealed that there

[341] 'Statistics on Race and the Criminal Justice System – 2003', A Home Office Publication under section 95 of the Criminal Justice Act 1991. www.homeoffice.gov.uk/rds/index.htm
[342] 'Statewatch Special Report: Ethnic Injustice continues unabated. Statewatch News Online, April 2005. Statewatch article: RefNo# 26437, http://database.statewatch.org/unprotected/article.asp?aid=26437
[343] 'MPA Stop and Search Scrutiny – Far reaching report published', 38/04, Metropolitan Police Authority, May 20 2004, available at www.mpa.gov.uk/news/press/2004/04-038.htm
[344] 'Terror Searches of Asians up threefold, Daily Telegraph, July 2, 2004.
[345] 'Stop And Search Action Team: Interim Guidance', Home Office, available at www.homeoffice.gov.uk/docs3/Guidance26July.pdf.
[346] available on the Home Office website: www.homeoffice.gov.uk/docs3/SSATPolicydoc.pdf

was evidence of under-recording: there had been a mixed or negative police response to the extra paperwork and even when openly observed by Home Office researchers, some police officers failed to record stops. While this initiative by the SSAT, and similar initiatives, exudes good intentions, the importations of such practices into police activities will evidently continue to encounter resistance, be it deliberate or otherwise.

Terrorism Stop and Search

Despite assurances made in the Home Office's Race Equality Impact Assessment that the issue of racial discrimination will continue to be monitored, and the emphasis placed upon an assertion that the majority of participants are in favour of ID cards, the topic still raises concerns in many quarters. This is principally in the light of increasing evidence of problematic use of police powers, in particular the disputed use of the power to stop and search under s44 of the Terrorism Act 2000.

S44 came under intense scrutiny in the latter half of 2004 as a result of stops and searches by police at an arms exhibition in the Docklands area of London during July of the same year. Several protesters were stopped by police in the locality of the arms fair and searched for 'articles connected with terrorism'. Liberty, the civil liberties organisation, brought a claim against the Metropolitan Police Commissioner on behalf of two affected individuals for judicial review of the powers exercised under s44 on the grounds that they were being used unlawfully to deter people from protesting. Liberty alleged breaches of Article 5 (liberty), 8 (family and private life), 9 (freedom of thought, conscience and religion), 10 (freedom of expression) and 11 (freedom of peaceful assembly and association).

Although it lost its case and the subsequent appeal, Liberty have been granted permission to be heard in the House of Lords; the case will be heard by the Appellate Committee in October 2005. This case continues to highlight the dangers posed by the use and abuse of the s44 stop and search powers, particularly because there is no need to suspect that an individual is actually carrying articles to be used in the commission of terrorism offences.

Of particular interest during this period were the contradictory statements that were made. Notably, as the Guardian reported[347], Scotland Yard initially denied use of the (Terrorism Act) legislation, but later admitted that it had been used on some occasions. Judicial comment made during the appeal case indicated that disclosure on the part of the Metropolitan Police had not been forthcoming. In its conclusions, the Court stated that it was:

> "important that if the police are given exceptional powers….because of the threats of the safety to the public, they are prepared to demonstrate they are being used with appropriate circumspection."[348]

Nonetheless, the lack of sufficient disclosure clearly did not sway the court to consider more rigorous judicial review of the potentially *ultra vires* exercise of these powers.

[347] 'Police can use terror powers on protesters', Rebecca Allison, The Guardian, November 1, 2003.
[348] 'The Queen on the Application of Gillan and Anr v The Commissioner of Police for the Metropolis and Anr', Court of Appeal (Civil Division), 29th July 2004, paragraph 54.

This episode, while bearing little direct relevance to the issue of racial discrimination, serves to demonstrate the capacity of the police to stretch the boundaries of what is considered 'proper' police practice in the exercise of their powers to stop and search, especially where the omnipresent threat of terrorism is allowed to influence matters.

Immigration Checks

On the issue of immigration checks, figures are more difficult to obtain. There are reports that immigration officials have apprehended individuals on public transport in order to ascertain their immigration status. Although this practice began in London, it is spreading nationwide. In September 2004, The Guardian revealed that in the previous 15 months, 235 operations had been conducted, and went on to say:

> "The figures showed that those arrested included 717 failed asylum seekers but thousands more people have been stopped and questioned by immigration staff using powers which the police are banned from using."[349]

The article also quoted the immigration minister, Des Browne, who defended the operations and said that although immigration officers do not have the same powers as police to stop and search, they can legitimately question people to determine their immigration status where there is a *reasonable suspicion* that a person is an immigration offender.

A later article published in the New Statesman[350] in November 2004 revealed that such stops are usually initiated under the guise of ticket inspections, but once apprehended, a suspect is subjected to questioning by immigration officials. Official policy on this practice is difficult to locate, although each of these stops should be fully recorded. Immigration officials are not subject to the same reporting procedures as police officers, and the Home Office has stated that: "the data is not collated centrally because it is impractical and expensive".

Such "street operations", as the Home Office has named them, are joint police and immigration operations. According to one ticket inspector, the officials target ethnic minorities, notably Asian people or those of Eastern European origin. This has caused an understandable degree of unease amongst employees of the transport system. The New Statesman article reveals that many Underground workers have complained about the operations, particularly one that was conducted outside Whitechapel tube station, targeting Bangladeshi people. The nature of the spot checks seems to be highly intrusive and individuals have been detained for 'up to forty minutes' in public, while their details are checked and their fingerprints taken on the new portable scanners. As the article in the New Statesman highlighted, white Australians, New Zealanders or South Africans are not affected by these "street operations", which gives a clear indication of the racial bias.

[349] '1,000 Illegal migrants arrested in Swoops', Alan Travis, Home Affairs Editor, September 15, 2004, http://www.guardian.co.uk/uk_news/story/0,,1304719,00.html
[350] 'Police State', Tom Wall, New Statesman, November 22, 2004.

In response to the disquiet amongst transport staff, the RMT transport union carried out its repeated threats to take action if its members were not withdrawn from such operations. On the 15th February 2005, The Evening Standard reported that: "random immigration checks on Tube passengers have been banned by Underground chiefs".[351] A protocol was being drawn up between the British Transport Police and Transport for London that would eliminate all random checks, but potentially allows for intelligence-led premeditated operations.

Stop and Search and Identity Cards

In light of the above, it is easy to recognise why there is increasing opposition to national ID cards; it appears to be inevitable that they will be employed as further grounds upon which to base racial prejudice. As a result, reports and inquiries into the introduction of ID cards have been punctuated by recurrent mention of the discriminatory effect of ID cards.

The Home Office produced a Race Equality Impact Assessment alongside the introduction of the Identity Cards Bill to the House of Commons on 25th May 2005, which summarised the views of individuals and organisations. Below is an outline of some of the observations made by the report.

- The report acknowledged that there were fears "that the police will interpret the legislation around identity cards in a way that will discriminate against minority ethnic groups, with a strongly held view that the police will stop a disproportionately high number of black and Asian people and demand sight of the identity card even though the draft Bill provides no such powers," particularly where there was a reliance on discretion.
- The report states that concerns expressed by members of the black and ethnic minority communities largely mirrored those of the white population and "concerns over the potential discriminatory effects of the Bill were secondary." With regard to fears of discrimination, black respondents retained the highest levels of concern, with 77% predicting that they would be requested to produce an ID card more frequently and 72% predicting that they would be singled out on ethnic minority grounds.
- The Commission for Racial Equality (CRE) commented that the introduction of a national compulsory identity card would not be racially discriminatory as it would be issued to all residents, but acknowledged the widespread perception that they could provide a source of discrimination particularly in the operation of the system.
- The CRE further expressed concern for people who had been working illegally in the UK for many years and feared the creation of an underclass.
- The CRE mentioned four areas where ID cards could have potential for indirect discrimination, notably (1) police stop and searches, (2) service provision and employment, (3) provision of information without consent and (4) gypsies and travellers.

[351] 'Immigration Checks on Tube Passengers banned', Ben Leapman, Evening Standard, February 15, 2005.

- The Citizens Advice Bureau (CAB) stated that 'a universal mechanism of identification would be "a welcome step forward in improving access to services"', however it also mentioned that the requirement for foreign nationals to register first would place heavy burdens on individuals.
- The Home Affairs Select Committee, which published a report on identity cards on 30th July 2004, accepted the useful role that ID cards may maintain with regard to access to services; however, in considering the effect of identity cards on minorities, particularly the socially excluded and ethnic minorities, concluded that they would be asked more frequently by the police to produce the identity card and this would have an adverse effect on race relations.
- The Government accepts that a compulsory scheme would be less discriminatory.
- Overall, the majority of participants were in favour of the Identity Card scheme.

This last finding is the more surprising when one considers the findings of the UK Passport Services study: it noted that 55% of the BME subgroups considered biometrics as an infringement of civil liberties, as did 53% of those who were designated as 'other religion'. Similarly, 42% of the 18-34 subgroup saw biometrics as an infringement of civil liberties.

ID and Illegal Immigration and Work

Complaints concerning the discriminatory and draconian nature of the immigration stop checks have led to some compromise in the way operations are conducted, as demonstrated by the withdrawal of support from the London Underground. If the police, working with immigration officials, can already stop a person at random on the grounds that they reasonably suspect him of being an "immigration offender", and demand to verify his immigration/citizenship status, the National Identity Register and the ID card fits into these plans perfectly. The Bill, in this context, is therefore integral to the creation of an increasingly police-orientated state. If a person of Asian origin has the option of carrying an ID card or being subject to 40 minute 'verifications', then the description 'voluntary' becomes meaningless. The introduction of identity cards, whether mandatory to carry at all times or not, will enshrine and condone random, racially based stop-checking.

On the issue of illegal working, the situation is similarly confusing. The Bill creates a situation where employers are not obliged to verify identity cards, but the fact that they have done so will qualify as a defence if they are accused of employing a person with no right to work in the UK. The Government already has in place many safeguards for controlling illegal working in the UK: indeed, the legislation in this area was updated in May 2004. Changes to the Asylum and Immigration Act 1998 were introduced to:

- Make it harder for people who do not have permission to work in the United Kingdom to obtain work by using forged or false documents;
- Make it easier for companies to ensure that they employ people who are legally permitted to work in the United Kingdom;

- Strengthen the Government's controls on tackling illegal working by making it easier for the United Kingdom Immigration Service to take action against employers who deliberately use illegal labour.[352]

Under section 8 of the Act, it is a criminal offence to employ someone who has no right to work in the UK. Employers are given a statutory defence against conviction for employing if they check and copy "certain original documents belonging to your employee". The penalty for failing to comply is £5000 for each illegal employee.

If this current system is not working well, simply adding ID cards to the list of approved identity documents is not likely to improve matters. The only measures that could change the situation are a compulsion on all individuals to carry ID cards in order to permit spot-checks by the Home Office, a requirement on all employers to report, and a requirement to verify the data against the national register. The Regulatory Impact Assessment for the Bill acknowledges this when it states that:

> "The scheme will have greatest impact on illegal immigration and illegal working if it became compulsory to register with the scheme."[353]

Even if there is a requirement to register, it is not clear what is likely to happen in a situation where a biometric ID card does not match the details of the potential employee. At present, the Government's advice on finding out whether a person is eligible to work in the UK states that the employer is entitled to refuse employment and "may want to call the Employers hotline".[354] Presumably an ID card will oblige employers to play a more significant role.

This points to the likelihood that internal checkpoints could be constructed across British society. Some professional bodies have already expressed concern about taking on the role of policing identity. The British Medical Association has stated that it is:

> "concerned about the possibility that doctors would themselves be asked to police access to health services. A doctor's primary professional duty is to promote the wellbeing of his or her patients, and to provide health services on the basis of clinical need. Such a responsibility would create a conflict of professional interest for doctors."[355]

Similarly, when the current Home Secretary, Mr Clarke, was Secretary of State for Education, he said that there were no plans for schools "to check on the immigration status of children joining a school to see if they were entitled to free education."[356]
The obvious concerns in the Health and Education services about the principle of implementing such checks are likely to be shared by employers throughout the UK.

---

[352] 'Changes to the law on preventing illegal working: short guidance for United Kingdom employers', Amendments to document checks under section 8 of the Asylum and Immigration Act 1996, The Home Office, April 2004, available at http://www.workingintheuk.gov.uk/ind/en/home/0/preventing_illegal.html.
[353] Bill RIA, Paragraph 38.
[354] Ibid, page 6.
[355] 'BMA raises questions about ID cards and access to healthcare UK', Medical News Today, July 23, 2004.
[356] 'Schools rebuff Blunkett's ID scheme', Alan Travis, The Guardian, April 28, 2004.

Experiences in Other Countries

Predictions of the likely abuse of police powers are substantiated by evidence of the implementation of ID card schemes in other European countries. A report produced in 1997, 'Policing the Community: The impact of National Identity Cards in the European Union'[357], provides a comprehensive guide to the legislation that assists the particular ID card scheme and the actual police practices that have evolved in a variety of European Countries.

Most importantly, the report reveals that the 'voluntary' schemes employed in many European countries are voluntary in semantics only, and 'administrative' detention of an individual, and/or penal fines for non-disclosure, are commonplace in countries where either voluntary or compulsory schemes exist. Case studies of the respective methods of implementation in Germany, France and the Netherlands do little to allay fears of likely racial prejudices.

In Germany, police responses to questions on the identity card checks revealed an awareness of racial discrimination laws. The police argued that minorities are also white, and consequently discrimination in ID checks was rare. German civil rights groups begged to differ, asserting that, despite many migrants being white, there were visible differences between them and the native German population. The report's authors accompanied the police in Germany for a period of time and observed that the German police were stopping higher numbers of people from ethnic minorities. The officers explained that this was a necessary measure to combat illegal immigration.

Similar patterns affecting ethnic minorities emerged in studies conducted in the Netherlands. Although the system was voluntary at the time, strong links to the identity card's role in combating illegal immigration created 'obvious' potential for abuse, and during observations by the authors, a tip-off concerning a factory was investigated on the basis that the employees were 'foreign looking'.

In France, the study reported similar levels of prejudice, although tensions between ethnic minorities and the police seemed more heightened. The Institute for Advanced Studies in Internal Security (IHESI) drew attention to the link between the cards and tightening immigration law adding that: "although the card itself provided no threat to civil liberties, the police powers to check ID provided an ever growing intrusion." According to Mouloud Aounit, the secretary general of the French anti-racism group MRAP:

> "They aren't in themselves a force for repression, but in the current climate of security hysteria they facilitate it... Young people of Algerian or Moroccan descent are being checked six times a day."[358]

[357] 'Policing the Community: The Impact of National Identity Cards in the European Union' by Adrian Beck and Kate Broadhurst (Scarman Centre for the Study of Public Order), *Journal of European Migration Studies*, 1998.
[358] 'ID cards may cut queues but learn lessons of history, warn Europeans', Amelia Gentleman, The Guardian, November 15, 2003.

Michel Tubiana, the president of the human rights federation FIDH, stated:

> "A system which allows ID checks encourages discrimination."[359]

In the UK, the 1997 report of the Scarman Centre concluded that there were difficulties in ascertaining whether the research findings and higher rates of offending amongst some ethnic minority groups are a result of disproportionate crime involvement or of disproportionate crime control directed at them. The study considers it likely that the two are linked, and that discrimination against minorities, particularly black minorities, interrelates with high rates of offending. Finally, the report suggested that:

> "even if a voluntary card was introduced (in the UK) with no additional powers for police to check an individual's identity, evidence from other EU countries would suggest that through a process of compulsion by stealth, officers may be increasingly suspicious of those who did not have a card, and this in itself could cause tension when performing a stop and search."

However, despite the fact that this finding is based on both qualitative and quantitative research, it is one that, several years later, we are being asked to ignore.

As Part of the Larger Legislative Landscape: SOCPA

Aside from the immigration and money laundering regulations that have created opportunities for identification measures, the Serious Organised Crime and Police Act of 2005 also contains serious measures that must be noted. Together these laws show that an ID card is part of a much larger collection of laws and policies put forward by the Government to transform policing.

Making all Offences Arrestable and Searchable

The power to stop and search requires reasonable grounds for suspecting that the search will find stolen goods or prohibited articles. Similarly for road checks, the police can stop a car if the vehicle is carrying someone who has committed, or is intending to commit, an offence, is a prisoner or a witness. Traditionally, offences are divided into *arrestable* and *non-arrestable*. Arrestable offences are those where the sentence is fixed by law, punishable by 5 years of imprisonment, or specified offences included in definition by statute.

The difference in law is that someone can be arrested by a constable if the officer has reasonable grounds for suspecting that the individual is committing, or has committed, an arrestable offence; or anyone about whom he has reasonable grounds for suspicion that they are guilty of an arrestable offence. For non-arrestable offences, a constable may arrest anyone about whom he has reasonable grounds for suspicion if he is satisfied:

- that the identity of the relevant person is not known, cannot be readily ascertained or is in doubt as to whether it is his real name;

[359] Ibid.

- that the relevant person has not furnished a satisfactory address for service of a summons, or there are reasonable grounds for doubting that address;
- where the constable has reasonable grounds for believing that arrest is necessary to prevent the relevant person
    - causing injury to himself or another
    - suffering injury
    - causing loss of or damage to property
    - committing an offence against public decency
    - causing an unlawful obstruction of the highway;
- where the constable has reasonable grounds for believing that arrest is necessary to protect a child or other vulnerable person from the relevant person.[360]

Where a person has been convicted of a recordable offence, has not been in detention in a police station and has not had his fingerprints taken, he can be required by the police to attend at a police station to give his fingerprints.

There are provisions yet to be brought into force in the Criminal Justice Act 2003 that will enable people arrested in the street to be bailed to a police station. It is believed that these powers await the availability of mobile fingerprinting facilities that will be carried in police cars. Sections 116 and 117 Serious and Organised Crime and Police Act 2005, when brought into force, will enable the police to take photographs and fingerprints of arrested persons at places other than at a police station.

It would appear that there exists no power to take a non-intimate sample (e.g. of DNA) without consent other than at a police station. However, with consent, it can be taken anywhere, as can photographs or fingerprints.

The present policy seems to be that all who come into contact with the police should be photographed, fingerprinted and swabbed for DNA (and tested for drugs). Fingerprints and DNA are subjected to speculative searches to see if they have been found at scenes of unsolved crimes.

Section 4 Criminal Justice Act 2003 introduces a new section 30A, which empowers a police officer to release on bail any person arrested or taken into custody before he arrives at a police station (s30A(1) and (2)). No conditions can be imposed on bail granted in this way (s30A(4)) save that the person must be required to attend at a any police station (s30A(3) and (5)).

The Bail Act 1976 does not apply to street bail (s30C(3)) but a constable may arrest without warrant anyone who fails to attend at a police station as required (s30D(1)). Such failure to attend is not in itself an offence (although for the purposes of s30 and s31 PACE 1984 it is to be treated as an arrest for an offence simply to permit it to be integrated into the procedure at police stations).

Section 9 Criminal Justice Act 2003 extends s61 PACE 1984 to permit the taking of fingerprints without consent if a suspect is detained at a police station in consequence of

[360] Section 25, PACE 1984.

his arrest for a recordable offence. Section 10 extends the same power to the taking of non-intimate samples.

Section 110 SOCPA 2005 when brought into force will remove the distinction between arrestable and non-arrestable offences; there will be a power of arrest for all offences, no matter how petty. As a result, the regime within PACE for non-arrestable offences is rewritten, allowing constables to arrest without warrant anyone who is about to commit any offence, or whom he has reasonable grounds for suspecting to be about to commit an offence. It would appear that the new powers will extend to any offence, as 'offence' does not seem to be defined, and may therefore include bye-law offences. PACE is rewritten by s110(4) SOCPA, which provides that the new PACE arrest powers "are to have effect in relation to any offence whenever committed".

Thus there will be a power of arrest for a host of minor matters that hitherto would have been commenced by summons. Those committing motoring offences, such as speeding, failing to comply with a traffic sign, or parking on a yellow will be liable to arrest. A person seen in school time with their child, because they are not required to be in school, have leave of absence, have a medical appointment or are educated at home, is liable to arrest if a police officer does not accept the explanation and believes he has reasonable grounds to suspect that the offence of failing to secure regular attendance at school is being committed (s444 Education Act 1996).

Under PACE, fingerprints can be taken at any time with consent; before charge on the authority of a superintendent who has reasonable grounds for suspecting that a person is involved in a criminal offence; after charge with a recordable offence. Under SOCPA, fingerprints and photographs may be taken if the constable reasonably suspects that a person is committing, or attempting to commit, an offence, if the name of the person is unknown, or if the constable has reason to doubt the given name.

In summary, the new and pending legislation will permit police to conduct identity checks and fingerprinting for any offence, no matter how trivial, and to bail that person to appear at a police station. The existence of an identity card and national register is central to the execution of these new powers.

11

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. Until recently, opinion polls had 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 significantly high. Throughout 2003 and 2004 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 had been remarkably consistent.

An April 2004 Detica/MORI poll[361] 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.

[361] Detica/MORI poll, http://www.mori.com/polls/2004/detica.shtml.

Proposals to charge people directly for a card appear to be the key trigger for public concern. A recent poll (from Reform/ICM)[362] 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).

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[363] 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.

The most recent ICM poll, commissioned by the campaign group NO2ID, found that overall support for the government's proposals had dropped to 55%, with 43% believing the scheme was a "bad or very bad idea".

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

[362] Reform/ICM poll, http://www.reform.co.uk/filestore/pdf/041203%20id%20cards%20tables.pdf.
[363] Privacy International/YouGov poll, http://www.privacyinternational.org/issues/idcard/uk/idpollanalysis.pdf

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.

Entrenched hostility and non-co-operation

The Privacy International/YouGov poll indicated that opposition to the identity cards scheme, while still in the minority, was deeply hostile. As discussed elsewhere in this report, the non-co-operating population is likely to exact a high toll on the scheme.

The strength of feeling amongst opponents can be gauged by responses to a "competition" run by NO2ID. Visitors to the organisation's website were asked to consider how they could – within the law – disrupt the scheme. The following published examples are illuminating, and demonstrate that organised actions of resistance will create substantial cost and stress.

Refuse to comply / cooperate

"I have a simple answer to this. I will refuse to pay... if they take the money from my wages I will resign my job. If they take the money from my dole I will not claim benefit. I will then claim sanctuary at my local church (already been arranged). When eventually forced into court will close my defence with a quote from 'The Making of the English Working Class' the quote will be 700 pages long and I will read it out in court...very slowly. Should clog up the system a bit..."

"If you refused to let your hand actually make contact with the fingerprint scanner's surface and a Home Office employee physically pushed your hand onto it, that could be classed as common assault."

"For the finger prints it'll be heavy duty DIY - sanding something down with wet and dry, grouting the bathroom or being a bit clumsy with the superglue. An alternative approach would be to have two plastic bags containing wet flannels in my pockets so I can make my fingers prune like in time for my allotted scan."

"It's quite easy to remove your irises. Atropine is a very old drug and dilates your pupils so you have no irises. Its effect is temporary…"

Delaying tactics

"Turn up at the at 'Appointed time and place' very promptly and then demand that they take you details immediately. When they refuse because people are waiting, tell them to give you another appointment and walk out. You have complied with the law."

"Every time an appointment is made, claim to be away on holiday and unable to attend. Keep breaking appointments due to illness, bus broken down, etc. Push up the administrative costs as much as possible each step of the way."

"Forget accompanying information. Take wife's passport by mistake. Have some kind of fit in the foyer. Have some kind of fit during the eyeball scanning. Turn up roaring drunk. Smoke during the process. Vomit on the machines. Take your 'carer' along and demand they be allowed to accompany you during the process. Provide all information via your 'carer' and later dispute the accuracy of conversation."

Overload the system

"…organise 'Renew your passports' week or month. Time it so that everyone just beats the deadline where they'd be entered on the NIR. And we also swamp the Passport Office, which regularly has month-long backlogs just with normal renewals.

Think about what proportion of the population normally needs to interact with the Passport Office in a month. 0.3%? If we get that up to 6% (i.e. 200x more), they'll be sunk for at least a year."

"Give lots of not quite correct information, and then send a series of letters 'correcting' it item by item ("I had thought I lived at 2 Acacia Drive from 3 September 2005, but my aunt has reminded me that I moved in on the day she had her hip replacement, which was 4 September, not the 3rd", "I have now checked my birth certificate and discovered my middle name does have an 'e' in it after all"... etc)."

Payment

"…paying in amounts of less than £1 a time using multiple Girobank cheques, which, [at the time of the poll tax], cost the recipient at least 50p per cheque in bank charges to collect, but which were free to the payee.
- paying hundreds of pounds not merely in cash, but in small coins..."
"How can we register or pay fines, etc. if we haven't received the relevant letters? Still on letters, when they arrive, write "unsolicited junk mail, return to sender", on unopened envelopes and post them back."

"If it comes to it… pay with cheques from defunct accounts. Forget to sign them. Put the decimal point in the wrong place. Use a completely different signature. Don't put stamps to the full value on the envelope so the receiving office has to pay to get it. Get a certificate of posting from the post office (they're free) for everything you send, but make your handwriting on the envelope impossible to read so it can't be delivered."

Boycott

"Write to you bank, building society, insurance company, the supermarket you use regularly, and tell them that you will take your business elsewhere if they support the introduction of ID cards…"

"The weakest link in the chain, here, are telecoms companies. The Times has reported that the government is in talks with BT already - fine - if you use BT, tell them you're taking your business elsewhere if the bid for any contracts related to this system - hit them right where it going to hurt most, in their profit margins."

"I have a pension invested in an Ethical Fund - I was surprised to see one of the companies involved in the ID card/biometric passport scheme was in their list of 'ethical' companies. I am now demanding to know why my pension company includes this company in their fund when they are involved in unethical business."

Ridicule

"I intend to change my title from MR to MS, and my name from a male to a female name, and turn up wearing a wig and full make-up, whilst insisting that my sex is "male". My wife will do the reverse."

"Have a deeply moving religious experience on the morning of your visit to the processing centre and convert to a religion which requires your body to be fully covered by something like a burkha."

12

The Legal Environment

There are a number of legal implications to the introduction of identity cards in the United Kingdom. The Government's approach to identity cards gives rise to particular legal challenges. In the following sections we will review the existing legal environment, the implications for data protection laws, likely effects of the cards on freedom of movement within the EU, and an assessment of biometric passports under English law.

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[364] 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);
- 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.

[364] 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.

Data Protection Act

> "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 section will seek to identify some of the data protection and privacy concerns referred to by the Information Commissioner.

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 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 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-date. 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.[365] 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.[366]

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

[365] Information Commissioner's evidence to Select Committee on Home Affairs, 3rd February 2004.
[366] 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.[367] Compatibility therefore remains to be tested in the courts.

[367] 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.[368]

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.

[368] 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."[369]

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.

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

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.

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

Eligibility to enrol 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".[370] 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".[371] 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.

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".[372]

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

[370] Identity Cards Bill: Race Equality Impact Assessment, rev1, para.13.
[371] Ibid.
[372] Explanatory Notes to the Identity Cards Bill, rev1, para. 77.

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)[373] 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.

[373] 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.

Effects on EU Freedom of Movement

This section[374] describes certain of the issues associated with the United Kingdom's (UK) proposed Identity Cards Bill, introduced and published by the UK Government on 29th November 2004. A report issued by the Joint Committee on Human Rights on 2nd February 2005 already has examined the Bill for compliance with human rights legislation and principles, including notably the European Convention on Human Rights. This section 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 section 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.

EU Freedom of Movement Principle

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.[375] 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 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,

[374] This section was prepared for the London School of Economics and Political Science by Covington and Burling.

[375] "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.

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 30th 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."[376]

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.[377] 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.

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:

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

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

> "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."*[378] (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.[379]

Significantly, the Government appears to equate registering, as that term is understood under the Directive, with registering for purposes of the National Identity Register.[380] 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 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.[381]

---

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

[379] 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".

[380] 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.

[381] 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.

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.

Biometric Passports and English Law

A key component of the identity card scheme is that the UK Passport Service ("UKPS") intends to introduce a facial-recognition image biometric in the UK passport beginning in late 2005/ early 2006. The International Civil Aviation Organisation ("ICAO") has nominated facial-recognition as the primary biometric for travel documents, with iris pattern and fingerprint as secondary, but not mandatory, biometrics. In line with ICAO recommendations, the UKPS intends to deploy a chip in future UK passports to store the holder's facial image and at least one additional biometric identifier.

This section considers whether the introduction of biometric passports to the UK might violate the legal rights of UK citizens. A number of legal arguments have been put forward and conclusions are summarised below. However, in several cases these arguments may be countered by national security concerns raised by the Government. It is also arguable that such concerns do not merit the disproportionate measures the Government intends to adopt and many of these concerns may be unfounded, possibly doing little to bolster national security and rather inconveniencing the UK general public.

The principal arguments are as follows:

- **The fundamental notion of a passport will be changed.** The passport is a travel document securing safe conduct through foreign States. Introducing additional personal data to the passport alters its concept to nothing less than an ID card. The additional measures are arguably surplus to requirements and disproportionate to safety concerns, doing little to make passports more secure. Rather than facilitating freedom of movement, the changes may impose further restrictions and offer unnecessary additional controls to Government.
- **The measures may violate the common law right to exit and re-enter the UK.** This common law right of each UK citizen is now enshrined in the Immigration Act, which does provide for exceptions. However, if a right to leave the UK exists and a passport is a prerequisite, then a right to a passport must exist also, subject to those exceptions. That right would likely be hindered if new biometrics were introduced. The Act's exceptions are aimed in spirit at immigration control of foreign nationals, not control of UK citizens leaving the country.
- **Collecting and processing biometric data may infringe UK data protection laws.** UK data protection legislation may be violated, particularly with respect to clarity of purpose for use, excess data collection, data storage duration and possibly data security. However, data protection legislation provides for exceptions to processing personal data when in the interests of national security or for preventing crime.
- **EU rights of non-discrimination and free movement may be violated.** The measures may discriminate against UK citizens within the EU if other EU citizens are not required to provide biometric data when entering or leaving the UK. The measures may restrict the freedom of movement of UK citizens within the EU and restrictions to this right must only consider the conduct of individuals and not apply more broadly. Additionally, the measures may restrict

the free movement of workers, although exceptions may be applied in the interests of public security or public policy.

- **Human rights laws may be violated, especially a right to private life and non-discrimination.** The measures may violate the ECHR and restrict the right to private life of UK citizens. Restricting travel and requiring data to be stored on Government databases may violate the ECHR where it is unnecessary and exceed the legitimate public security interests. Likewise, the measures may be regarded as discriminatory against UK nationals.

Legal Evolution of the UK Passport and Royal Prerogative

UK passports are issued in the UK under the powers of the royal prerogative and of statute. The royal prerogative is a body of customary authority recognised in monarchic common law jurisdictions as belonging solely to the monarch. The royal prerogative is not subject to parliamentary scrutiny but individual prerogatives may be abolished by legislative enactment. The prerogative to issue passports remains in force today, giving the sovereign, now through the Secretary of State, the discretion to grant or refuse any application for a passport. This right has remained unchanged for hundreds of years and continues to govern the UKPS's authority for the issue of UK passports. Since no statute or English case law lays down the rules surrounding the power to issue passports in the UK or the nature of that passport, evolution of the document itself has been dictated by historical events. In the UK constitutional context, a passport remains today what it was some 500 years ago, namely a pass of safe conduct.[382]

The passport has undergone a number of physical changes since its introduction in the UK. Principally these have related to style and the details included in the document linking the holder with a given passport. A photograph of the holder became a requirement in 1914 as a security feature, together with a range of personal identifying data about the holder. This included details of the holder's facial and nasal shape, eyes and complexion. During the 1970s, security adaptations to passports became increasingly necessary in response to threats arising from stolen and falsified documents. New features were introduced to UK passports to help counter fraud.[383] By contrast, the need for additional personal identifying data was regarded as no longer necessary for the purposes of the document and these were removed.[384]

The move by the UKPS to introduce a chip holding biometric data arguably departs from the historical and constitutional notion of a passport. These measures effectively transform the passport from a travel document securing safe conduct, which citizens have a right to possess to exercise their right of movement (see below), to a form of ID card.[385] Additional biometric data provided and stored on Governmental databases

[382] In an Act of 1414, exists a reference to "safe conducts" (one of the first references to an early passport) by which British subjects were allowed to travel freely under the authority of the then King Henry V.

[383] For example, blue security paper incorporating a special water-mark was introduced to passport pages and photographs were laminated to prevent easy substitution. Eventually a security laminate overprint was introduced in the early 1980s.

[384] In 1972 a woman's maiden name was no longer shown on page 1 of the passport and the holder's eye colour was omitted. By 1985, the distinguishing marks and height were also removed from page 2 of the UK passport.

[385] In some countries, the passport is used as an official ID card and is necessary to carry out everyday administrative transactions, e.g., in Russia where it is needed for receipt of medical care, receiving mail and installation of a telephone line. Moreover, it is an administrative offence not to hold a passport in Russia.

would become a prerequisite for a UK citizen to leave the country. In essence, the Government would be using the passport as a means to gather data about its citizens disproportionate to the level of data needed to travel.[386]

Additionally, the trend in recent decades has been to strengthen the security features of the passport itself. To limit production of counterfeit passports or use of stolen passports, new features have been added to make copying or alteration of details more difficult. The introduction of a chip and a second biometric may do little to assist in passport security. A second biometric is surplus to requirements and reintroduces the outdated trend for passports to carry superfluous personal identifying details.

Common Law Right to Leave the Country

The right to leave the country is a fundamental legal right of each UK citizen. The right of travel is enshrined in Article 42 of the Magna Carta, which in 1215 granted a right to exit and re-enter the realm – a right that has been directly relied upon in the Indian courts.[387] In *DPP v. Bhagwan*,[388] Lord Diplock referred to the common law right of a British subject to come and go "*without let or hindrance*," and this common law right is embodied in Section 1 of the UK Immigration Act 1971.[389]

However, this right is clearly of little use without the possession of a passport, which is a mechanism by which the right to enter and exit the UK is made administratively feasible. Restricting that right to enter and exit by imparting onerous and disproportionate measures to obtain a passport is tantamount to curbing the freedom of every UK citizen. It has been stated in the UK that the issue of a passport is the "normal expectation of every citizen",[390] and indeed, taking the requirement of a passport together with the right embodied in Section 1 of the Immigration Act, there must be a concomitant right to a passport,[391] which can only be restricted in the limited circumstances to which that section applies.[392]

The Government must respect each UK citizen's right to enter and exit the country and avoid imposing disproportionate conditions to obtain a passport as to make that right

[386] There is no entry requirement at present in any country for UK citizens to possess biometric data other than a facial image on their passport. Note that the US has reversed its decision recently that biometric details must be introduced to EU passports by October 2005 to secure entry to the US.

[387] That right has been extended to a right to passport facilities in India, *see Sawhney v. Assistant Passport Officer, Government of India* (1967) Times, 15 April. Note that in the English case of *Secretary of State for the Home Department v. Lakdawalla* [1972] Imm AR 62, the courts queried whether there is a right to passport stating that the fact there is no Act, rule or regulation dealing with the issue of passports confirms that a passport is merely a privilege.

[388] [1972] AC 60.

[389] Note that the right in Section 1 is subject to the restrictions set out in that Act.

[390] *See R v. Secretary of State for Foreign and Commonwealth Affairs, ex parte Everett* [1989] QB 11 per Taylor LJ. However, note the House of Lords stated in 1958 that "*No British subject has a legal right to a passport. The grant of UK passport is a Royal Prerogative exercised through her Majesty's ministers and in particular the Foreign Secretary,*" *see* HL Official Report 209 (5th series) col 860 (Parliamentary Question).

[391] Note that the right to a passport has been held in the US to be a constitutional right, *see Kent v. Dulles* 357 US 116 (1958) at 125-126; and in France the *Cour de Cassation* has held there is a right to leave France and that refusal of a passport may be a restriction of that right, *see e.g., Cass.Civ*. 1re 28/11/1984 RFDA 1985.760 *concl. Sadon*.

[392] Section 3A of the Act permits the Secretary of State to impose conditions on entry, which could extend to passport format. However, where such conditions are so unreasonable as to make obtaining a passport undesirable, it is arguable that the right to enter and leave the UK has been curtailed.

barren. Citizens reluctant to have their biometric data accessible on a passport database effectively would be prevented from applying for a passport and so lose their freedom to leave the UK.[393]

Rights Under Data Protection Laws

The data protection implications of the Government's Scheme and the measures to be introduced to passports have already been considered above.[394] In short, the lack of clarity in respect of the purposes for which the biometric data are collected and the possibility that two biometrics are indeed excessive for passport issue could be incompatible with the data protection principles under the UK Data Protection Act.[395] Additionally, a central database of passport details necessarily will involve considerable security risks. It is arguable that the UKPS will be presented with an enormous task in meeting its technical and organisational obligations under the seventh data protection principle to prevent unauthorised or unlawful processing of the data held therein. Also, there may be concerns surrounding the length of time data are kept on the central Government database, which may fall foul of the fifth principle requiring data to be kept no longer than necessary for the purpose(s) specified.

The Act does exempt personal data from any of the provisions of the data protection principles if the data are required for the purpose of safeguarding national security[396] or from the first principle if the data are processed for the prevention or detection of crime.[397] It is not clear to what extent the Government may rely on national security concerns to justify introduction of biometric passports and central biometric databases and many of the counter arguments are addressed in the Interim Report referred to above.

Rights Under EC Treaty

Measures to be introduced by the UKPS include provision of two forms biometric data before a passport may be issued. This requirement may infringe a number of Articles of the EC Treaty.[398] These are the potential Articles implicated by the Scheme:

1. **Article 12 - Non-discrimination on grounds of nationality.** This Article prohibits discrimination of any EU citizen on the grounds of their national origin. The Article may be infringed if the measures introduced impose an unfair burden on UK nationals alone within the EU. If similar biometric passport requirements are not required of other EU nationals entering or leaving the UK, then UK citizens might arguably face direct discrimination, particularly if failure to provide the biometric data would restrict the right of travel outside the UK.

[393] Of interest is Article 5(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"), which states that "everyone has a right to liberty and security of person." However, this Article only covers actual detention and not restrictions on free movement. Article 2 Protocol No. 4 to the ECHR guarantees a right to freedom of movement, but the UK has not ratified that Protocol yet.
[394] The Identity Project - An Assessment of the UK Identity Cards Bill & its Implications, Interim Report, March 2005.
[395] Schedule 1, Data Protection Act 1998.
[396] Section 28 of the Act.
[397] Section 29 of the Act.
[398] Treaty Establishing the European Community, C 325/33, Rome, 25 March 1957.

2. **Article 18 - Free movement of persons.** Article 18 embodies the fundamental right to move and reside freely within the EU, subject to certain limitations and conditions laid down in the Treaty and measures adopted to give it effect. Free movement of persons within the EU is one of the basic pillars of the EU ideal.[399] The proposal to introduce biometric data to passports may breach this Article. The principles of Article 18 are expanded in additional EU legislation including Directive 2004/38 on the right of citizens to move and reside freely in the EU.[400]

Directive 2004/38, to be implemented in the UK by 30 April 2006, confers a right of entry and exit on EU citizens to other EU Member States with a valid ID card or passport.[401] No requirements are provided as to what format the passport should take other than it being valid "at least for all Member States and for countries through which the holder must pass when travelling between Member States."[402] However, Article 27 of the Directive imposes restrictions on the right of entry and exit on grounds of public policy and public security. It is specifically stated that measures taken on these grounds must comply with the principle of proportionality and shall be based exclusively on the conduct of the individual concerned:

> "[t]he 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."[403]

Arguably, the general, blanket nature of the measures as introduced by the UKPS may breach Article 27 of the Directive. The measures do not consider individual concerns, but rather treat all UK citizens as a potential threat to national security and so restrict the movement of all UK citizens entering and exiting the UK.

3. **Article 39 - Free movement of workers.** The Treaty sets out a general principle of freedom of movement of workers to be secured within the EU. This freedom abolishes discrimination based on nationality, but is restricted to limitations on grounds of public policy, public security or public health. However, this Article does not further consider how these restrictions should be interpreted. It is not clear whether an argument based on public security would justify the measures to be introduced.

Rights Under ECHR

Article 8 of the ECHR guarantees the right to respect for private and family life. The Convention prohibits interference by public authorities with that right except:

---

[399] It is also enshrined in the International Covenant on Civil and Political Rights, which entered into force 23 March 1976, which the UK ratified. Article 12(1) sets out a right to liberty of movement and freedom to choose residence. Article 12(4) states that "*No one shall be arbitrarily deprived of the right to enter his own country.*" The Convention allows for exceptions where necessary including to protect national security and public order.

[400] Directive 2004/38/EC of 29 April 2004, on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States.

[401] Articles 4 and 5.

[402] Article 4(4).

[403] Article 27(2).

> "…as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, the prevention of disorder or crime, the protection of health or morals or for the protection of the rights and freedoms of others."[404]

Requiring UK citizens to provide biometric data and permit processing of that data for uncertain purposes prior to travel may violate the principles of Article 8 in three ways.[405] First, the Government will make provision of this data compulsory before leaving the UK, which could fail to respect UK citizens' right to privacy in respect of that data. The storage and use of information concerning a person's private life in the files of the UKPS (and possibly other bodies) may amount to an interference with the right to respect for private life.[406]

Second, not everyone will be comfortable permitting access to such sensitive data as iris and finger print scans, particularly without adequate reassurances that the data will not be provided to third parties and used for uncertain purposes. Such measures therefore may be viewed as "hindrances" to the effective exercise of the Article 8 right as they will hinder the travel right of UK citizens. The European Court of Human Rights has held hindrances to be an interference even if they do not actually prevent the exercise of the right.[407] The Court has not offered an exhaustive definition of "private life." However, it is closely linked to the notion of personal autonomy and development and is more than a right to privacy. Thus, in line with the Court's broad view of what amounts to an interference with private life, restrictions on ease of travel may hinder autonomy and development of citizens and so violate Article 8.[408]

Third, the measures also may infringe Article 8 if they interfere with the family life of UK citizens. Restrictions on UK citizens who hold only UK passports may interfere with the family life of those citizens with respect to travel with other family members who do not need to provide biometric data (because they hold a passport from another State).

Arguably, the measures the Government seeks to impose would not be "necessary" and so unjustified under Article 8(2). Current identification measures associated with MRPs are viewed by many as adequate. Although the additional measures may assist in border security checks, the Government must weigh up the intrusion into citizens' rights when considering what is truly necessary. Likewise, it is hard to argue that the measures would be in the interests of national security, public safety or indeed prevent crime. If

---

[404] Article 8(2).

[405] *See also* UK Human Rights Act 1998, section 6(1): "*It is unlawful for a public authority to act in a way which is incompatible with a Convention right.*"

[406] *Leander v Sweden* (1987) 9 EHRR 433.

[407] *See Golder v UK* (1975) 1 EHRR 524, para 26.

[408] *See Botta v Italy* (1998) 26 EHRR 241 para 32, in which the Court took a broad view of private life and referred to a right of physical and psychological integrity - the right to development of personality of each individual in his relations with other human beings. *See also Brüggeman and Scheuten v Germany* (1981) 3 EHRR 244, in which the Court held that private life secured to the individual sphere within which a citizen can freely pursue the development and fulfilment of his/ her personality. More specifically on the issue of right to hold a passport *see Smirnova v Russia* (2003) ECHR 397 in which the Court held that depriving a Russian citizen of a passport amounted to continuing interference with the citizen's private life. Note, however, that in this case the passport had been confiscated following the citizen's arrest and that in Russia a passport was needed as proof of ID for everyday transactions.

only UK citizens are required to provide the additional data, it is hard to envisage how that will deter or prevent threats to the UK from foreign nationals. Furthermore, restricting the rights and freedoms of UK citizens runs contrary to the very wording of Article 8, which makes clear that measures must protect these same rights.

The measures may also infringe Article 14, which states that the enjoyment of rights under the ECHR shall be secured without discrimination on any ground, including national origin. The disproportionate nature of the data required to obtain a future UK passport arguably discriminates against UK citizens purely on the grounds of national origin. The applicability of Article 14 is not limited to cases in which there is an accompanying violation of another provision of the ECHR.[409] Thus, if the Government's measures are exempted under Article 8(2), it may still be possible that the measures infringe Article 14, as there remains a link to the enjoyment of rights under Article 8. Moreover, the Court has made clear that "very weighty reasons" will be needed to justify differences of treatment based solely on nationality.[410]

[409] *Belgian Linguistic case* (1968) 1 EHRR 252 at 283 para 9: "…*a measure which in itself is in conformity with the requirements of the Article enshrining the right or freedom in question may however infringe this Article when read in conjunction with Article 14 for the reason that it is of a discriminatory nature.*"
[410] *Gaygusuz v Austria* 23 EHRR 364.

13

Biometrics

Prosecutions for dealing with or creating false ID cards and high-level identity documents have been pursued in many countries, including Britain,[411] Hong Kong,[412] Pakistan,[413] Ireland,[414] Malaysia,[415] Yemen,[416] Czech Republic,[417] Venezuela,[418] India,[419] Italy,[420] and Sri Lanka[421] 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.[422]

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.

Faith in the Perfectibility of Technology

A biometric is a measure of identity based on a body part or behaviour of an individual. The most well known biometrics are fingerprints, iris scans, facial images, 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

[411] 'Passport scam uncovered', BBC News Online, December 3, 1999, http://news.bbc.co.uk/1/hi/uk/548559.stm.
[412] '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
[413] '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.
[414] Parliament of Ireland, April 1, 2003, http://www.irlgov.ie/debates-03/1Apr/Sect10.htm.
[415] http://www.mmail.com.my/Current_News/MM/Friday/National/20041210100244/Article/index_html
[416] 'Yemen confirms Cole suspects' trial', BBC News Online, December 6, 2000, http://news.bbc.co.uk/2/hi/middle_east/1058085.stm.
[417] 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.
[418] 'Some thoughts on identification', Asuntos Legales, http://www.analitica.com/archivo/vam1996.06/asleg1us.htm.
[419] 'Hill Kaka - A military or a political failure', Kashmir Sentinel, http://www.kashmirsentinel.com/june2003/18.html
[420] '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.
[421] '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.
[422] 'Sheetrit promises new smart ID card tender before 2005', Globes online, September 7, 2004, http://www.globes.co.il/DocsEn/did=834696.htm.

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).

It is a faith in biometrics that is driving the Identity Card Bill. In October 2004, Prime Minister Tony Blair announced that ID cards would be in the Queen's speech. On the topic of technological progress, he stated that

> "Overall, progress is very encouraging and I'm confident we can successfully develop a secure ID card for the whole country. (…) Computers and technology are so advanced now that forgery of passports and identity documents are easier than it's ever been. (…) A secure modern solution will give us much more protection than we have at the moment."[423]

The Government has repeatedly claimed that the use of biometrics will prevent any fraudulent use of the system. Often it is said that biometrics is the key enabler of the Government's bill, particularly since the very existence of the National Identity Register hinges on the verification of biometrics. A central register on a scale of 50 million records would need to contain very accurate biometrics, and the verification process would have to involve high-integrity devices. To operate at a national scale, as envisioned by the Government, the technology would have to be close to perfect. Failure of the biometrics and the register can not be an option.

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[424] while researchers in Germany have established[425] that iris recognition is vulnerable to simple forgery.[426]

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

[423] 'PM Press Conference', Number 10 Downing Street, October 25, 2004.
[424] 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
[425] 'Body Check', Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, CT Magazine, November 2002, http://www.heise.de/ct/english/02/11/114/.
[426] Liveness Detection in Biometric Systems, http://www.biometricsinfo.org/whitepaper1.htm.

> of application-dependent evaluations, their potential susceptibility to deception, the lack of standards, and questions of users' acceptance.[427]

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.

The Government has been previously warned of all these problems. According to Written Evidence submitted to the Home Affairs Committee from BT, these biometrics require further testing.

> "Fingerprint recognition is in use in a number of applications and is a relative success. Issues with fingerprint recognition include the high rate of false non-match results and social inclusion given that in the current UK population approximately one in a thousand people are unable to provide the required four suitable fingerprints. Another potential problem area is the public perception of the process of taking fingerprints and its link with the criminal justice process.
>
> Iris recognition is as yet unproven in large-scale biometric applications. Issues include the physical size of the each individual datum and for a population in excess of 50 million, the need for an image of both irises to ensure uniqueness. Around one in ten thousand people do not have a suitable iris for recognition.
>
> Facial recognition is not currently sufficiently reliable for the identification of each member of the population and recent trials have shown relatively poor identification performance."[428]

[427] U.S. General Accounting Office, Using Biometrics for Border Security, Washington D.C., November 2002 http://www.gao.gov/new.items/d03174.pdf.

[428] 'Memorandum submitted by British Telecommunications plc', submitted to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we04.htm.

Similarly, QinetiQ advised the Government on the challenges of perfecting authentication, and re-emphasised usability and user acceptance as a factor.

> "Fingerprints have been in existence for many years and fitted the analogue authentication processes well. In today's digital domain fingerprints suffer from high false acceptance rates and a social stigma in some cultures, notably UK ("only criminals have their fingerprints taken, don't they?"). A biometric has to have high fidelity and be least intrusive to the individual. It must also be low cost and impact on the existing infrastructure as little as possible. Any society that adopts a biometric for authentication must also allow for technology improvement.
>
> (…) Its fidelity must be such that the probability of a correct authentication is what is known as the five 9s—99.999% probability. This figure is taken from telecommunication availability statistics for the domestic customer before they complain about lack of service. The science and research into biometrics is only really beginning and systems that adopt authentication biometrics must accommodate the future."[429]

The advice provided to the Government was that there are many components to the decision to implement biometrics. A belief in the technology working, or that it can be made to work is dangerously simplistic. Rather it is essential to understand the dynamics of the technology, the specific details of its effectiveness, the challenges to deployment, and its usability, amongst many other dynamics.

The Government has conducted a number of studies on the use of biometrics to better understand some of these dynamics, though the results have been conflicting. The first was commissioned by Communications Electronics Security Group (CESG), and conducted by researchers at the Centre for Mathematics and Scientific Computing at the National Physical Laboratory.[430] This research was conducted well before the Government articulated its plans for a national ID system based on biometrics. It studied a number of systems (face, finger, hand, iris, vein and voice-biometrics) to test performance, feasibility, and to encourage more testing.

This first NPL report was careful to note that system performance is dependent on the application, environment and population. This study involved only 200 users. The study looked at the metrics that show the usefulness of each biometric system.

- Often more than two attempts would be required to obtain an enrolment;
- There are frequent errors in data collection, e.g. the use of the wrong biometric, user interaction problems, and input errors;
- The 'failure to enrol rate' measures the mere generation of a template of value to the system. Face, Hand, Vein, and Voice achieved a 0% failure rate, iris achieved a 0.5% failure rate, and fingerprinting varied from 1% to 2%;

[429] 'Memorandum submitted by QinetiQ'.
[430] 'Biometric Product Testing Final Report', Issue 1.0, Tony Mansfield, Gavin Kelly, David Chandler, Jan Kane, March 19, 2001.

- The 'failure to acquire rate' measures the proportion of attempts for which the system is unable to capture or locate an image of sufficient quality. While the failure rate for face, hand, and vein remained at 0%, fingerprinting rose to 2.8%, and voice went up to 2.5%. Iris failure rate was 0%;
- The 'false match rate' vs. 'false non-match rate' studies the comparison of a capture biometric against an enrolment template. By adjusting the decision criteria there can be a trade-off between false match and false non-match errors. The iris system had a pre-determined threshold, and had no false matches in over 2 million cross-comparisons. Otherwise, matching failures arose due to poor quality images;
- The 'false acceptance rate' vs. 'false rejection rate' measures the decision errors for the whole system;
- The 'multiple attempt error rates' studied the effectiveness of repeated attempts to use the system.

A second study was conducted by one of the researchers at the NPL and another from BTexact Technologies. This study was commissioned by the UK Passport Service, the Driver and Vehicle Licensing Agency, and the Home Office.[431] This time the research was geared towards the Government's policy at the time, that of entitlement cards. The biometrics selected were fingerprints, iris and face image recognition. It measured the ability to detect fraud in double-applications for a card, and the ability to verify in order to confirm the use of the card by the correct individual.

The purpose of the study was to test the feasibility and risks of the use of biometrics for a national identity scheme. Therefore biometrics that could not be stored in a central database for a one-to-many verification were not considered. That is, while hand geometry systems are less invasive and useful for verification with a template on a chip, it is not as relatively unique amongst a population of 50 million. Biometrics were selected on the grounds that they could be used to ensure a unique identity against all other registrants, verifying biometrics on the card against the card holder, and checking the identity on the card against a watch-list of images.

The main findings of the study were that:

- "in principle, fingerprint or iris recognition can provide the identification performance required for unique identification over the entire UK adult population. This would require, however, the enrolment and registration of at least four fingers, or both irises. However, the practicalities of deploying either iris or fingerprint recognition in such a scheme are far from straightforward";
- Such a system would be a groundbreaking deployment for this kind of biometric application. "Not only would it be one of the largest deployments to date, but aspects of its performance would be far more demanding than those of similarly sized systems; such existing systems are either not applied in the civil sector, or operate in countries where public acceptability issues are less prominent";
- Current biometric systems are not designed for this type of deployment;
- Implementation by 2007 to limit identity fraud appears feasible, provided work commences in early 2003;

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

- The use of biometrics adds to the cost of the card system. The most significant cost is the time and effort to enrol individuals and collect biometric data;
- Ultimately the choice of biometric, or to not use biometrics at all, may be based on total system costs.

The report is very clear that 100% certainty in authentication can never be guaranteed, particularly on the scale foreseen by the Government. The study was conducted on the assumptions that the Government's scheme would involve:

- Approximately 50 million people;
- Daily throughput between 10,000 and 50,000 enrolments in the roll-out phase of 10 years;
- Daily throughput of 3000 enrolments after the roll-out phase, due to new 16-year olds and foreign residents;
- Approximately 2000 local offices for processing (at UKPS and DVLA local offices and by High Street Partners);

The report also highlights the factors essential to successful use of biometrics for authentication:

- Extent to which the system operates without human intervention;
- Degree of 'uniqueness' of the biometric;
- Technical factors (e.g. security, robustness, cost, scalability);
- Social factors (e.g. acceptability, trust in the operators of the system).

The report makes some conclusions regarding the specific biometrics. While fingerprint biometrics are the most likely to be implemented on a large scale, the comparison times can be very slow. Iris scan results are compared at a much faster rate, but the technology is not yet tested for wide deployment. Face recognition is a long way from achieving the necessary accuracy for what the Government envisions, and 'recent trials of the technology have shown relatively poor identification performance for even quite small populations', though it works well for one-to-one verification. While the combination of biometrics does allow for an improved performance, "the performance improvement is unlikely to be commensurate with the increased costs, and collection of the additional biometric images might be seen as unnecessarily intrusive by the public."

The report goes on to call for pilot implementations of the technologies to obtain good estimates of performance. The UK Passport Service was set to do such a study, but in the end, it undertook only a user acceptability test.

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 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 a national ID card) are unable to enrol fingerprints or iris images. Ability to recognise both characteristics is known to decline with age (fingerprints wear down, some eye conditions increasing with age cloud the eye), 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.

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. A UK Passport Service trial funded by the Home Office had a representative sub-sample of the whole population, with 10,016 involved, but a quota sample of 2,000 only. 750 disabled participants were involved, though this was 250 short of the target number.

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 Qantas air 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, as well as 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 biometric 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 fingerprint 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) 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

According to the NPL/BTexact study, there are still significant fears about the use of fingerprinting.

> "One senior UK fingerprint examiner with many years of experience in the front line of police activities mentioned that many householders who had been burgled refused to be fingerprinted to eliminate their own prints from those of a burglar – in spite of assurances about the destruction of their data after use. In a deployment in the USA, however, we were told that assurances of limitation of use were sufficient to gain the trust of the participants."[432]

The sense of criminalisation is one of the larger obstacles to the wide-spread use of fingerprints, particularly on the scale envisioned by the UK Government involving a national registry that can be used by the police for watch-listing.

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 universal applicability of 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[433] 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.

---

[432] 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', for UKPS, DVLA, and the Home Office, by Tony Mansfield and Marek Rejman-Greene, February 2003, p. 27.

[433] Fingerprint Verification Competition 2004, Open Category Results: Average results over all databases, Preliminary results, http://bias.csr.unibo.it/fvc2004/results.asp.

According to one expert, our understanding of fingerprints "is dangerously flawed and risks causing miscarriages of justice".[434] 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 11th 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 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."[435]

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.[436] 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").[437] 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

[434] 'The Achilles' Heel of Fingerprints', J.L. Mnookin, Washington Post, May 29, 2004.
[435] Ibid.
[436] 'FBI Faulted in Arrest of Ore. Lawyer', B. Harden, Washington Post, November 16, 2004.
[437] See references to this term, for example, in http://www.speechtechmag.com/issues/3_3/cover/442-1.html

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 elsewhere 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.[438] 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.

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."[439]

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."[440]

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."[441]

A report for the European Commission observes:

---

[438] U.S. General Accounting Office, Using Biometrics for Border Security, Washington DC, 2002, http://www.gao.gov/new.items/d03174.pdf.
[439] ibid p.73.
[440] 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.
[441] Penny Khaw, Iris recognition technology for improved authentication, SANS Institute, 2002 http://www.sans.org/rr/papers/6/132.pdf.

> "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."[442]

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."[443]

While the European Telecommunications Standards Institute (ETSI) acknowledges:

> "Iris recognition may fail in the case of a blind eye."[444]

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".[445] 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.[446]

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."[447]

---

[442] 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.
[443] 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.
[444] 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.
[445] Industry presentation by Iris Australia & Iridium, http://www.sensory7.com/presentations/DSD.ppt.
[446] emedicine.com, http://www.emedicine.com/OPH/topic43.htm
[447] Roberto Roizenblatt et al., Iris recognition as a biometric method after cataract surgery, *BioMedical Engineering OnLine* 2004, 3:2.

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.[448]

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."[449]

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.

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

> "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."[450]

Dr 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."[451]

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:

---

[448] Cited in EuroTimes, published by the European Association of Cataract and refractive surgeons, http://www.escrs.org/eurotimes/archive/nov_dec2000/ukopthamologists.asp.
[449] John Daugman, Iris Recognition, available at http://www.icdri.org/biometrics/iris_biometrics.htm.
[450] Ibid.
[451] Argus technology website http://www.argus-solutions.com/about_overview.htm

> "While blind people can be difficult to enrol, there are instances where blind people have used iris recognition successfully."[452]

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.[453] 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."[454]

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. 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.

The above data 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. This 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, rights 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

[452] Website information http://www.lgiris.com/iris/index.html
[453] 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.
[454] 'Technical glitches do not bode well for ID cards, experts warn', Computer Weekly, May 7, 2004.

organisational 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 is 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 Significance of the UK Passport Service Trial

These other studies provide an insight into the results of the UKPS trial. After many delays, the report of the trials was released in May 2005.[455] Despite the need for a trial of the actual biometrics and their use, the UKPS Biometric Enrolment Trial was more of a customer response test:

> ”The goal of the UKPS Biometrics Enrolment Trial was to test the processes and record customer experience and attitude during the recording and verification of facial, iris and fingerprint biometrics, rather than test or develop the biometric technology itself – it was not a technology trial.”[456]

While this is a disappointment considering the time and effort that went into the trial, a number of conclusions can still be drawn from the report.

The trial involved 10,016 individuals from a variety of sample groups including a quota group of 2000 and 750 disabled participants. The trial databases were pre-loaded with 118,000 irises and 1 million fingerprints.

Enrolment Success

While the report claims that ‘the majority of participants in all sample groups successfully enrolled’, there are significant gaps:

- On facial recognition, success rate for the non-disabled was 100%, though 98% for disabled participants. Ten percent of all disabled participants could not be registered on the first try, while the average for all other participants was 4%. Black paricipants suffered the highest failure rate.

[455] ‘UK Passport Service Biometrics Enrolment Trial’, Atos Origin, May 2005.
[456] Ibid., p.6.

- On iris registration, only 90% of non-disabled participants could enrol, though the results were 61% for disabled participants. Asian and White participants had higher success rates than Black participants. A divergence also occurred between participants aged under 60 who had a higher success rate than participants aged over 60.
- On fingerprint enrolment, nearly 100% of non-disabled participants could enrol, but only 96% of disabled participants. Reasons for failing to enrol included a 'false match' with fingerprints obtained earlier in the Trial. Surprising results included that 2% of all Black participants could not be fingerprinted, while 45% of Black participants required multiple attempts at enrolment (while 30% on average required multiple attempts).

In total, this means that 0.62% of the disabled participants could not be registered at all. This translated into over 850,000 UK citizens who would be excluded from an identification system based on these results.

Verification Results

When individuals' biometrics were verified against the database, the results were much more problematic.

- On face recognition, the verification rate was 69% for the non-disabled, and 48% for disabled participants. Participants under the age of 60 had a better verification rate than those over 60. Changes in appearance caused failures, as did lighting problems. Black participants encountered more difficulties in registration: at one location 78% of Black participants failed to verify, while at another the error rate was 26%.
- On iris verification, the verification rate was 96% for non-disabled, though for disabled participants it was 91%. This again worked better for younger participants than for older ones, as older individuals were almost five times more likely to fail than those aged 18-24 (5.37% compared to 1.19%).
- On fingerprint verification, 81% of non-disabled participants were verified, while the rate was 80% for disabled participants. Again, younger users were more successful than older users, with sometimes severe differences. It was found that frequently the devices did not record sufficient detail from the fingers.

The problems here are many and complex. The report concludes only that the readers were insufficient and the lighting problematic.

Attitudes Towards Biometrics

On the usability issue, iris-scanning comes off worst for time taken, positioning, and the overall experience. Many felt criminalised by the taking of fingerprints, and some thought it was overly intrusive.[457]

Prior to the trial subgroups '18-34yr olds', 'Black and Minority Ethnic', 'Other Religion' showed much more concern compared with the average scores. The general

[457] Ibid, p.106.

disabled participant group also indicated more concern prior to the trial, in particular of the iris biometric.[458] Though the concern fell after the enrolment, these same groups continued to show the greatest levels of concern.

The polling on the results also showed dramatic differences in opinion between groups. When asked whether biometrics are an infringement of civil liberties, 55% within the BME subgroup tended to agree or agreed strongly, as did 53% of those designated as 'other religion', and 42% within the 18-34 subgroup.

Concluding Remarks on the Trial

In summary, this trial was a wasted opportunity to perform what the NPL reports had called for: a wide-scale trial of the technology. The performance of biometrics from this trial, however, was very disappointing. This reduces the likelihood for the potential mass deployment of biometrics for a national identity scheme. Any scheme deployed on a large scale would have to have very small error rate. This is what the Home Affairs Committee was told by numerous vendors and specialists.

The results from this trial show that the enrolment of the biometrics was non-trivial. After a number of attempts, though, only 862,000 individuals would be likely to be excluded entirely from the systems. That is, 862,000 disabled citizens would not be able to participate in the scheme. The results on verification show that the average citizen is likely to encounter a number of rejections while using the system. Even for supposedly perfect technologies such as iris scans, the failure to verify was still very high.

Yet the Government has already hailed the results of this trial as evidence that the technology is fine. Home Office Minister Tony McNulty announced that, based on the UKPS trial:

> "Once we get onto the procurement process and delivery neither the government nor the IT sector will be found wanting."[459]

He continued,

> "I'm confident of the robustness of the technology within the time scales we are talking about. We are not starting from a zero knowledge base. (…) The UKPS trial did teach us things that will be filtered into the process. I would be confident that the technology is in place as and when we need it."[460]

The UKPS trial report claims that the use of multiple biometrics would be ideal because of the problems with each specific biometric. But the NPL/BTexact study had already shown that such a scheme would be overly complex and costly, unlikely to be worth the effort and resources required. Implementing such a system involving these biometrics like this across the United Kingdom for use by 50 million individuals could bring the country to a stand-still. At best, it will be a tremendous waste of resources.

---

[458] Ibid., p.119
[459] 'ID Cards on Trial: Minister defends "robust" biometrics', Andy McCue, Silicon.com, June 7, 2005.
[460] 'Minister says ID technology is robust', Kable's Government Computing, June 6, 2005, available at http://www.kablenet.com/kd.nsf/Frontpage/9D2499D2C05F6E2A80257018004BBEF8?OpenDocument.

Conclusions: Remarks on the Perfectibility of Technology

It is important not to perceive technology as a panacea for social troubles. It is also important to understand that there is no perfectibility of technology: technology can be improved, but the notion of achieving perfection is at best misguided, at worst dangerous. Technology may be scientific, but once outside of the laboratory, it involves engineering. A great deal of engineering is about making the best decisions with the available limitations. It is thus important to remember that we are still able to, and must, make decisions about what are the appropriate technologies to implement.

We conclude this section with a statement from one of the world's leading experts on technology and privacy, the Italian Privacy Commissioner, Stefano Rodota. In a speech in which he warns against 'technological anasthesia', he argues that:

> "The public is overrating biometrics by thinking that technological development will go hand in hand with hi-tech protection against terrorism. [He concedes that a rejection of biometrics] "would be unthinkable, as in many cases it can help to make people's lives easier. What should be avoided is encouraging unjustified use of this kind of technology, which should only be used when a person needs to be identified at all cost. Furthermore, we need to ensure that all personal data be dealt with accurately and not made public. We also need to enforce all rules aiming at safeguarding personal privacy. Research has proven that the advantage of having centralized databases is questionable, as these are difficult to manage. And if a criminal organization manages to access them, they turn from safety tools into potentially criminal tools. Therefore evaluations must be made on the basis of each single case. The value of democracy must be a priority. We cannot afford to resort to controlling citizens as totalitarian regimes did. In the end, they lost their battle against democracy."[461]

Technology can not be perfected so expectations must be kept in check. These expectations should then inform future decisions. Nothing about technology is inevitable, and this is a fact that merely empowers us to make decisions.

It is not just so simple as to say that the technology will one day improve. The factors that go into this consideration are numerous and complex. The balancing act regarding such technology involves hundreds of factors including user perceptions, lighting, facilities-spacing, training of staff, age of devices, age of users, race, abilities to enrol compared to abilities to verify, the acceptable rate of error in contrast to the acceptable rigour. We must consider all of these factors as we decide what kind of infrastructure we would like to build, and what kind of society we are constructing.

[461] 'Privacy watchdog warns against 'technological anesthesia'', AGI, April 28, 2005.

14

Security, Safety and the National Identity Register

From a security perspective, the approach to identity verification outlined in the Identity Cards Bill is substantially – perhaps fatally – flawed. This section of the report outlines why we have concluded that, in consequence, the National Identity Register poses a far larger risk to the safety and security of UK citizens than any of the problems that it purports to solve.

The proposed National Identity Register (NIR) that forms part of the UK government's Identity Card programme will involve:

- A database holding records for 50 – 60 million people;
- Dozens – or even hundreds – of enrolment centres spread across the UK;
- A nationwide organisation involving several thousand staff;
- 5 million or more enrolment operations per year;
- Possibly 1 billion or more identity verifications and queries per year;
- Possibly 1 billion or more audit records per year.

This is already a large requirement, but there are greater challenges:

- The system has to be highly secure to protect the data it holds from unauthorised access or modification and to protect the privacy, safety and security of the millions of citizens identified in its records;
- The integrity of the system and the data held will be critical and will require extensive protection against data loss or corruption;
- The system as a whole will have to be extremely reliable because any extended service failures will prevent dependent organisations from carrying out their functions;
- Data in the National Identity Register will be an attractive target for both internal and external attacks; the system will have to cope with attacks designed to prevent it supplying its services effectively (known as ‘denial of service’ attacks);
- Every action and transaction, however small, will have to be recorded for auditing in order to detect and prosecute criminal abuse by those with access to the system;

- The system will have to accept and respond to hundreds or even thousands of identity enrolment and verification requests each minute; enrolment requests will involve a large processing load and a proportion will require costly and time consuming manual intervention;
- All personnel involved with the system will need to be security vetted to prevent criminal infiltration of NIR operations or 'insider' attacks.

Most experienced systems designers will immediately recognise that this combination of requirements poses an extreme challenge even without the security requirements. Even if the security requirements are undertaken the system becomes infeasible unless substantial pruning and simplification is undertaken.

The following sections will consider security and safety aspects of the proposal and some of the dilemmas that will be faced if a system of this scale and complexity is pursued.

Secure Information Systems

Since many governments have recognised the need for secure computer systems, internationally recognised criteria have been created to describe the 'security quality' achieved by computer systems. In the UK, the Communications Electronic Security Group (CESG) administers the UK's contribution to this field.[462]

The basic principle used is that if a computer system faces higher security risks, it will need to be of higher security quality in order to counter them (the technical term used to describe security quality is 'security assurance'). Typical factors that increase the risks, and hence the security assurance needed, are:

1. the scale and the complexity of the system
2. the number of users
3. the security sensitivity of data held on the system
4. whether it has connections to other computer systems, especially untrusted ones
5. whether it is connected to the Internet
6. whether it is likely to be an attractive target for attack

The security assurance levels used for assessing computer systems range from EAL 0, which is 'inadequate assurance', to EAL 7, which is the highest assurance that is considered to be practical (which can only be achieved in small, simple systems).[463]

Systems of the character of the National Identity Register are large, complex systems that hold considerable quantities of sensitive data. Such systems also face high levels of security risk because of their connections to other computers, and even to the Internet. The general view is that such systems require the highest levels of security assurance at EAL 6 or higher, but there are no systems of this character on the market that are higher than EAL 4. For example, the UK certified products list[464] contains no operating systems and no databases with security qualities above EAL 4, which is two or more

[462] http://www.cesg.gov.uk/site/iacs/
[463] http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=13
[464] http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=151

quality levels below that needed to implement the NIR. This is the case even for special "secure" versions of software, such as the Open INGRES/Enhanced Security database and the Sun Solaris 2.6SE operating system.

The NIR is an example of a class of computer systems requiring 'Mandatory Access Control', which means that the security policy cannot be overridden by the users. The most common systems of this type are described as 'multi-level secure'. These are systems that defence and intelligence agencies have been seeking to build for more than two decades. Although they are technically feasible on a small scale, experience shows that their development is extremely costly, their performance is very often disappointing and their maintenance and support costs are prohibitively high.

The problem is well summarised by Dr Rick Smith, a US computer security expert, who says:

> "Multilevel security (MLS) has posed a challenge to the computer security community since the 1960s. MLS sounds like a mundane problem in access control: allow information to flow freely between recipients in a computing system who have appropriate security clearances while preventing leaks to unauthorized recipients. However, MLS systems incorporate two essential features: first, the system must enforce these restrictions regardless of the actions of system users or administrators, and second, MLS systems strive to enforce these restrictions with incredibly high reliability. This has led developers to implement specialized security mechanisms and to apply sophisticated techniques to review, analyze, and test those mechanisms for correct and reliable behaviour.
>
> "Despite this, MLS systems have rarely provided the degree of security desired by their most demanding customers in the military services, intelligence organizations, and related agencies. The high costs associated with developing MLS products, combined with the limited size of the user community, have also prevented MLS capabilities from appearing in commercial products."[465]

Since the National Identity Register will require a mandatory access control system, the scale, complexity and assurance of which is a long way beyond anything ever previously contemplated, the programme is certain to face technical problems of a kind that are known to lead to development difficulties, and very often to uncontrolled cost growth during development.

There is thus very good evidence to suggest that it will not be feasible to build a computer system capable of operating the National Identity Register with effective security provisions. An attempt to build such a system is likely to be extremely expensive and at high risk of failure.

[465] http://www.cs.stthomas.edu/faculty/resmith/r/mls/index.html

Enrolment

The enrolment stage, in which people's biometrics are recorded and their details entered into the National Identity Register, is critical if the authenticity of each identity record is to be ensured. The immediate problem is that of balancing convenience of enrolment against the necessary quality of the result.

For example, to make enrolment easy, there will need to be many locations where enrolment is possible. But if there are many locations, the staff costs will be very large and the ability of systems managers to maintain control over the integrity of operations will be degraded. Since enrolment is critical to the integrity of the whole system, it will be important that staff members are well trained, with at least two people present at any time so that no single person acting alone can subvert an enrolment operation. Since there have to be more staff to cover leave and sickness, the usual assumption for a secure system is that three staff members are needed for every individual role that needs to be performed. This figure increases when management and backroom staff needs are taken into account.

The integrity of the National Identity Register will be compromised even if only a small number of these thousands of staff act improperly. With smaller centres, in particular, it will become feasible for those who see value in attacking the system to plan an infiltration strategy based on subverting a single enrolment centre. This will add to the requirements for vetting, auditing and other measures designed to ensure that such strategies cannot succeed. This will further increase both the initial and the operating costs.

If four staff members are needed per enrolment line, then with ten-minute enrolment interviews it is unlikely that more than ten interviews can be conducted per staff-day, or 2000 interviews per staff-year. With proper interviews and careful checks of foundation documents, productivity is likely to be even lower. 5,000,000 enrolments per year would thus require an establishment of several thousand staff. This is certainly what will be needed to maintain the quality of enrolment processes, but experience suggests that it will soon be seen as an unacceptably low throughput and will thus provoke ‘corner cutting’ to achieve savings, leading to the compromises that so often undermine security in the real world.

It also seems likely that such pressures will promote other enrolment strategies involving fewer centres. However, this is unlikely to make significant cost savings since it will simply shift costs onto those who now have to travel some distance in order to enrol. This will also make enrolment much less convenient, adding significantly to the difficulties faced by those who have to register for ID cards. We may expect particular problems for the elderly, for people with physical and mental disabilities, and for people living in remote communities.

Another issue is that of how citizens will be able to have confidence in enrolment centres and those who work in them.

Multiple Registrations

A key aspect of government claims about ID cards is the assertion that it will not be possible for the same person to register more than once with different details, since biometrics will expose attempts to achieve this. However, this assertion should be treated cautiously because it depends on several assumptions that have yet to be proven.

Firstly, this assumes a perfect biometric system, whereas it is far from clear that biometrics can meet this challenge for a population of over 50 million people. Secondly, this also assumes that the system as a whole is perfect and will not contain security weaknesses that can be exploited to create multiple registrations containing the same biometrics.

Of course, this might not be seen as a major problem, as anyone seeking to make multiple registrations with the same biometrics would presumably have to be lucky to find themselves with biometrics that are problematic. However, it is possible that ways of creating such situations will be discovered. We can expect technical attacks, whereby people try to create false identities using rubber finger covers, printed contact lenses and so on. But it is not 'normal cases' that are the source of most problems in secure systems; rather, it is usually one of the many 'special cases' that is exploited to subvert security.

There will, for example, be people whose biometrics are not fully satisfactory, and for whom the National Identity Register will have to make special provisions, such as holding data on known false matches. There are certain to be many such special cases, all of which have to be very carefully considered and implemented in a way that prevents their exploitation. The problem with this situation is that those who are seeking to defend the system only succeed if they find and eliminate all vulnerabilities, whereas an attacker succeeds if he can find just one that has been overlooked. In practice, this imbalance greatly increases the cost of maintaining security, because each minor change to the system has to be extensively analysed in order to ensure that it does not inadvertently introduce any exploitable security weaknesses. This is one of the reasons why maintenance and support costs for secure systems are enormous when compared with those of their insecure counterparts.

Of course, insiders will quickly get to know the 'special cases' and will be sufficiently resourceful to recognise how they can be exploited. It is inevitable that this sort of information will filter out to those who want to subvert the system.

Banks go to enormous lengths to protect the privacy of their customers' account details, but they face exactly this dilemma in that the banking system can only operate effectively if there is widespread sharing of account data. It is thus inevitable that, no matter how much the banks spend on security, it will still be possible for outsiders to obtain unauthorised access to account details.

The basic problem here is easy to understand: the greater the number of people who know a secret, the less secret it is. A system such as the National Identity Register, involving thousands of staff, stands little chance of being highly secure.

Identity Verification

If ID cards are to be more reliable than 'photo ID' cards, it is essential that their biometric features are widely used with frequent checks against the National Identity Register. Additionally, since the government proposes to hold identity-related data in the National Identity Register, on-line identity checks will be essential in key circumstances when access to this data is needed.

This puts the National Identity Register at the heart of the system, which in turn makes the security of National Identity Register data and control of access to it absolutely critical for the safety and security of all who are identified in its records.

Subject Consent for Access by Verifier to Data Held in the National Identity Register

In recent months, Government Ministers, including the Prime Minister, have claimed that data held in the National Identity Register will be safe and secure, and yet the Identity Cards Bill contains no explicit security requirements that provide a basis for such assurances.

Clauses 14(1)(a) and 14(1)(b) provide for verifier access with the consent of the subject but offer no indication of how this consent will be obtained nor how it will be authenticated.

Clauses 14(5) and 14(6) indicate that the Secretary of State **may** impose conditions on how consent is given, but it contains no **obligation** to do this in a way that provides a high level of confidence that the identity of the person seeking access (or giving consent for access by another party) matches the identity of the person whose National Identity Register record is being requested.

It is particularly puzzling that the government should seek to introduce a supposedly high-quality system for verifying people's identity, and yet fail to invoke explicitly this mechanism for authenticating subject access and subject access consent.

At very least, a new provision is needed to the effect that:

> The Secretary of State **shall** ensure that access under clauses 14(1)(a) and 14(1)(b) will only be granted if both the identity of the subject and their consent have been fully authenticated in a way that does not rely on a presumption that the subject trusts the person seeking to obtain such access.

The Bill should also make it an explicit requirement that access to data held in an National Identity Register record, other than the biometrics, is conditional on confirmation that the biometrics of the person purporting to give consent match the biometrics held in the National Identity Register record to which access is being sought. It would be hypocritical to advocate such services for use by others, yet fail to mandate their use in controlling access to the National Identity Register.

Although the Secretary of State **may** accredit those who seek to verify the identity of others using the National Identity Register, he is again under no **obligation** to do so. Given the safety and security risks of allowing unidentified individuals to access data held in the National Identity Register, it is again important to make access conditional on National Identity Register based identity checks upon those who are seeking to verify the identity of others.

Although the National Identity Register contains biometric data for verifying a person's identity, it also contains alternative provisions based on passwords and security questions. It appears that this mechanism has been included to cover situations in which biometrics cannot be recorded, measured, or used for a particular reason.

The circumstances in which this alternative means of identity verification can be employed are not specified. In particular it is not clear whether it can only be used when an entry in the National Identity Register does not contain biometric data, or when a subject is consenting to access by telephone or via the Internet. In consequence, it might be possible for those seeking access to the National Identity Register to use this low quality means of identification instead of high quality biometrics and thereby gain access to data in the entry without a strong check on the identity of the person giving consent.

Although it seems that clause 14(2) contains a provision that prevents security-critical data such as passwords and the answers to security questions being revealed, in practice this is not a significant constraint: a verifier can infer this information after a successful identity check because he is told if the values he supplies match those in the National Identity Register. This is an example of a well-known class of attacks known as 'inference attacks', in which an attacker can deduce information that he is not authorised to obtain from other information that he is given.

After one successful access request, a verifier will know the password and other security answers and can subsequently use this information to gain access to the National Identity Register without seeking further consent from the subject. Moreover, there is nothing in this Bill that imposes constraints or sanctions on verifiers who misuse data or even reveal it to others (we will return to this issue later). In addition, there appears to be no provision whereby a subject can give consent for access only to a subset of the identity-related data held in the National Identity Register. The recent spate of online "phishing" attacks (where hackers gain access to banking customers' passwords) shows how easily these security mechanisms can be abused, and how difficult it can be for the police to prevent such activities and track down the perpetrators.

A worrying aspect of this legislation is that the minimal security provision that it does contain – passwords and security answers – is seriously flawed, since it has been known for many years that information of this character should never be handled in the way that the Bill proposes. When such obvious errors are made in elementary aspects of security provision, there is no basis for confidence in the overall security of the National Identity Register.

These weaknesses in the proposed system undermine the Government's claim that data held in the National Identity Register will be safe and secure.

Conditions for Access to Data Held in the National Identity Register

In the operation of Identity Cards, there are three parties to an identity verification attempt:

1. the subject – the person whose identity is to be verified
2. the verifier – the person who is seeking to verify the identity of the subject
3. the Secretary of State – the person who proposes to offer confirmation of identity and offer identity-related data to the verifier

and there are three potential sources of biometric data

1. biometric data held in the National Identity Register
2. biometric data held on Identity Cards
3. biometric data derived from actual biometric measurements

This triplication of biometric data means that many different situations arise in any identity check, ranging from complete unavailability of biometrics to a situation in which all three sources of biometric data are available. Further complexity arises because there can be no presumption of the extent to which each of the three parties to an identity verification trust each of the other two parties. This includes, for example, the potential for 'two against one' collusion between any two of the three parties to undermine the interests of the third party.

Such situations need a very carefully constructed technical and legal framework if they are to be properly managed. A comparable problem arose in the Nuclear Test Ban Treaty[466] where the US and the Soviet Union each wanted to place seismic detection equipment on each other's territory in a situation in which (a) neither party trusted the other not to interfere with the equipment or the communications involved, and (b) neither party trusted that the only purpose of the equipment so installed was the detection of illegal nuclear tests.

Solving such problems requires a substantial research investment, covering both the technical and the legal aspects of the way in which these requirements can be met that is satisfactory to the interests and concerns of both parties. In the case of the National Identity Register, the situation is more complex because there are in fact three parties involved and three sources of biometric data.

Although it would be unrealistic to expect that the Identity Cards Bill should specify the complex technical details that are necessary to perform an identity verification in such a situation, it must necessarily establish a framework for them that is capable of coping successfully with the challenges that a complex three-party verification process will generate. There is little evidence to suggest that the Bill has been drafted in a way that indicates a capacity to deal with these complexities.

[466] 'How to Insure That Data Acquired to Verify Treaty Compliance Are Trustworthy', by Gustavus. J. Simmons, Chapter 13, Contemporary Cryptology: the Science of Information Integrity, IEEE Press, 1991.

This analysis suggests that the provisions in Section 14 of this Bill are inadequate in security terms, and fail to establish a sound basis for the security of data held in the National Identity Register.

Access to Data Held in the National Identity Register without Subject Consent

There are also worrying security deficiencies in Sections 19 to 23, that cover access to data in the National Identity Register held without the consent of the subject (this will subsequently be referred to as 'covert access').

Inadequate Controls Covering Access without Consent

A large number of organisations can gain covert access to National Identity Register data, the only constraint imposed on them being a requirement to show that the data cannot reasonably be obtained in another way. In practice, this constraint is so weak as to be virtually useless.

There is, for example, no requirement that such requests should be subject specific, which means that organisations with covert access rights can undertake 'fishing expeditions' in the National Identity Register.

Whereas a person who is seeking to verify an identity would have to nominate a subject, the police and others appear to be free to make requests that are not subject specific. This will mean, for example, that requests such as: 'supply fingerprint and address records for all who live in Worcester', or: 'provide the identity records of all those whose fingerprints might be a partial match for those attached', are permissible. It therefore appears that those with covert access will be able to interrogate the National Identity Register using full database search and extraction capabilities.

The ability to make such access requests without nominating a subject has serious safety and security implications. Although it might help in fighting crime, it will also create new risks for honest citizens. For example, those whose fingerprints are innocently found at crime scenes could have to account for their presence to the police, who would have the ability to identify them using the National Identity Register.

Although the size of any consequential risk is unknown, it is clearly present if largely unconstrained police access to the National Identity Register is allowed. In consequence it is far from certain that benefits in fighting crime will be sufficient to offset *new* risks for law-abiding citizens.

The Ability of Government Agencies to Impersonate UK Citizens

One bizarre provision within this part of the Bill is that organisations that have rights to covert access can obtain the passwords and security answers that are supposed to verify subject access and subject consent for third party access. Since the only possible use of this data is to impersonate the subject in respect of the giving of consent, it has to be concluded that the Government is inadvertently making provision to allow the police and other agencies to impersonate the subject in this regard. A likely consequence is

that the police, the intelligence agencies, and any criminal organisations who have managed to penetrate or infiltrate the National Identity Register, will be able to impersonate not just subjects but also verifiers (assuming they are also identified using the National Identity Register mechanisms).

These National Identity Register 'insiders' will be able to frame citizens – and also to create alibis for crooks – by making people appear to have undergone identity checks in locations that they never in fact visited (verifiers may also be crooked, and try to create false identification records using rubber finger impressions or photographs of irises: current biometric equipment mostly assumes honest attendants, rather than operators trying to deceive it). It is perhaps fortunate, therefore, that what the Bill actually specifies is inept in security terms, in that it needlessly exposes these items and thereby undermines their evidential value for authenticating the person identified by the NIR record in question. Ministers should recall the thinking behind the Electronic Communications Act of 2000, which rightly prohibited the mandatory escrow of signature keys, as this would have undermined the evidential value of signatures made with them.

Lack of Constraints on the Use of NIR derived Data Once Obtained

Although those operating the National Identity Register face criminal sanctions if they misuse or reveal National Identity Register data without authorisation, the Identity Cards Bill imposes no such sanctions on those who obtain data from the National Identity Register. Hence it seems that the police and intelligence agencies, and even those who do no more than use the National Identity Register for identity verification, do not face any meaningful penalties for data misuse.

Although those who access and subsequently misuse National Identity Register data face penalties under the Data Protection Act, in practice these sanctions are weak in their impact as they are limited to a fine. A specific and serious criminal offence might generate more confidence.

The lack of constraints on the misuse of National Identity Register-derived data once it has been obtained has serious implications. As long as the National Identity Register operates alongside the traditional means of identity verification, anyone who obtains National Identity Register data is in an ideal position to produce false documents that can then be used as a starting point for 'identity theft'. Far from undermining identity-based crime, the National Identity Register could easily facilitate it.

Weak National Identity Register access controls could also have a devastating impact on those who have good reasons for avoiding the existence of easy means of identification. This would include, for example, those in senior government or military positions who may be terrorist targets, those who might be subject to harassment or attack from 'animal rights' activists or from other extremist groups. Those who wish to hide from stalkers or from those who wish to harm them will also be at increased risk. Terrorist groups, in particular, would have an ideal starting point for identifying and locating their targets if they are able to gain easy access to data held in the National Identity Register.

In the light of these examples of the high risks that the availability of identity data will bring to some, it is worth reflecting on a statement made by David Blunkett, speaking in a debate on the earlier Identity Cards Bill:

> "Let me make it clear: no one has anything to fear from being correctly identified …"[467]

It is our view that those who understand the nature of identity would never pursue the type of centralised approach embodied in the National Identity Register because many of the security risks identified here are inherent in such an approach.

Insider Attacks and Auditing

One of the most difficult and challenging aspects of secure systems design and implementation is that of providing effective auditing that is capable of detecting and revealing malign behaviour on the part of system operators or users.

The difficulties inherent in the audit requirement can be illustrated by considering the audit load that will be generated by the National Identity Register. The system will have to handle (depending on the time of day or hour) up to 100 transactions per second continuously, each of which has to be recorded for audit. This will generate around 1 Gigabyte of data per day.

Although auditing can generate large quantities of data, the real problem is not the volume as such, but rather the 'needle in a haystack' problem of analysing this data to detect suspicious behaviour by users or system operators. Proactive audit analysis is important for the early detection and removal of subverted users and operators, but the volume of data forces the use of some form of automated or semi-automated audit analysis, or the random or targeted analysis of the audit records for specific users and operators.

However, although automated audit analysis will often catch 'amateur' insider attacks, long term subverted insiders will go to considerable lengths to ensure that their actions appear unremarkable. As a result, they are only likely to be discovered by manual audit analysis, meaning that that they can operate as subverted insiders for a considerable time without fear of detection, unless a high proportion of operators are subject to regular manual audits.

The regular manual audit of a high proportion of system operators for a system as large as the National Identity Register will be an extremely expensive process. Again, it is likely that corner-cutting to reduce costs will curtail effective auditing and exacerbate the risks of security compromises in the operation of the National Identity Register.

[467] Commons Hansard, Identity Cards, November 11, 2003.

Data Integrity and Database Pollution

Even small databases can quickly become outdated as the real world situations they record change. It seems inevitable, for example, that the 'place of residence' data in the National Identity Register for a significant proportion of National Identity Register records will become outdated quite quickly, since it will be seen as a tedious and intrusive requirement to report such changes, especially for those such as students and young professionals who are highly mobile. It is not clear that a fine will be a meaningful deterrent if a significant proportion of the population ignores this requirement.

Although addresses are an obvious example of data items that are subject to progressive pollution, other National Identity Register records, and even recorded biometrics, may suffer from such problems.

The progressive, slow degradation of the accuracy of data items in databases is a very common problem and one that often proves extremely difficult to control. It creates difficulties in databases even when users and operators have strong interests in maintaining good database integrity. In the case of the National Identity Register, the problem could be much more serious since a proportion of those registered will be opposed to the Register's existence and will see pollution of the National Identity Register as a benefit. In consequence, relying on subject change reports to ensure the integrity of National Identity Register data is unrealistic.

Database pollution is a serious problem because small amounts of data pollution can lead to a disproportionate drop in confidence in the integrity of the database as a whole, and thus undermine its effectiveness. Even in quite small databases, it is not uncommon to find that confidence in the accuracy of data items becomes so poor that the database has to be abandoned, and a new version built from scratch because this is a cheaper solution than an attempt to 'clean' the existing one.

The scale of the pollution problem for the National Identity Register is hard to predict, but in such a huge database it is likely to be difficult and costly to control, especially if a significant proportion of subjects actively work against the integrity objective. This could result in significant operating costs because tracking down and correcting errors in such a large database will be a very difficult task.

Conclusions

Security analysis of the Identity Cards Bill and the National Identity Register shows that:

1. The scale and complexity of the National Identity Register make it infeasible to build a computer system that can provide the level of security assurance necessary to protect the safety and privacy of those who are identified by its records. An attempt to build such a system is likely to be extremely expensive and at high risk of failure.
2. There is no obligation on the Secretary of State to protect this data or to properly authenticate a person's consent to accesses to data in their National Identity Register records.

3. The police and many other organisations will have almost unconstrained access to data held in the NIR, thereby creating serious new risks for honest UK citizens and significant new opportunities for criminals.
4. Parties who are able to access the National Identity Register will be able to discover the subject's passwords and related security details and will thus be able to impersonate them in situations where these items are intended to provide evidence of the subject's consent to access.
5. The Bill fails to establish a sound basis for identity verification that is capable of satisfying the essential interests of the three parties involved (the subject, the verifier and the state).
6. The lack of any explicit obligation to ensure the security of data held in the NIR, and the weak controls on access to this data, will facilitate 'identity theft' and will lead to serious increases in the risks faced by those who need to restrict access to identity data in order to ensure their safety or security .
7. In particular, these serious deficiencies will facilitate the operations of terrorists, animal rights activists and others who wish to identify suitable targets for their illegal activities.
8. It seems likely that the scale and complexity of the National Identity Register will make it impossible to maintain the integrity of the data that it holds; decline in its integrity over time seems inevitable and will undermine its value, thus having a negative impact on all services that become dependent on it.
9. Most importantly, it is possible that the centralisation of a massive amount of identity related data in a single database such as the National Identity Register creates an inherent and serious security risk.

15

The IT Environment in the UK

The United Kingdom is often a world leader in government IT projects. We have a rich experience in outsourcing projects, development projects, and the implementation of new systems. These projects and systems have not always achieved their stated goals.

Before embarking on a system as large as the one proposed in the Government's policy, it is important to understand the risks and challenges that we are likely to face. Then we can better understand the technological feasibility of the programme, and the likely cost ramifications.

Government Statements on Costs

Since the inception of the National Identity scheme, the Government has published very little information about anticipated costs. This has cast doubt over the few cost statements released by the Home Office, since there is no common framework to compare their different estimates with each other, or with independent estimates.

The confusion has been catalysed by an apparent blurring of the boundaries between identity cards and passports: the legal mandate, administrative process and common functionality have led to public uncertainty about which parts of the Government's stated costs relate to the National Identity scheme, and which to the Passport Service.

The results of Government studies into the technologies and processes that will support the National Identity scheme have not resolved these problems, and the Government's refusal to share information about the Gateway Reviews, feasibility studies and project management process leads us to conclude that the scheme may be vulnerable to functional errors or cost-overruns.

Current Government Costing

In November 2003, then Home Secretary David Blunkett announced cost estimates on the identity card.

> "To avoid accusations of underestimating the cost, we have chosen to build in a substantial contingency. We estimate that the basic cost, over a ten-year period, would be £35. All but a very small amount of that would be necessary in introducing biometrics in any case. The addition would be in the region of around £4, spread over the ten-year period. We will ensure that the basic cost of a card could be paid for

> by individuals in a variety of ways. Some people could choose to pay incrementally, through mechanisms such as saving stamps and credits."[468]

The cost of the larger system was then described as:

> "We have estimated total set-up costs and revenue over the first three years at around £36 million, £60 million and £90 million, respectively… The charge under debate will be met by each person who receives a card for a service from which he or she will benefit."[469]

However, the system involves more than just paying for the card, the biometric collection, and the set-up costs: issues such as system integration, data management and audit need to be considered. When the Identity Cards Bill was introduced for second reading in December 2004 the Government was less willing to discuss costs in detail. According to then Home Office Minister Des Browne,

> "The functionality of an identity system, as we debated in great detail in the context of the identity card for the electoral system in Northern Ireland, depends on a number of layers, and can be used in different ways. Of course there will need to be readers, and if we are to use cards for access to public services that will need readers too, but each decision will need to be made on a case-by-case basis for the purposes of those public services, according to a cost-benefit analysis of what investment we need to put in to get the best benefit out—[Interruption.] That is the proper answer, and the hon. Gentleman knows fine well that it is."[470]

This statement underlines the uncertainty of the costs associated with the Bill. These costs are likely to rise as the project develops, and one of the key reasons for this is the ongoing work by the Home Office to consider the potential design. According to the director of security solutions at QinetiQ,

> "The Home Office wants matching online because it wants to keep an eye on the bad guys and keep an audit trail. But that means talking over the internet to the central database. We are saying it is a step too far."[471]

In January 2004, BT warned the Home Affairs Committee that the database would have to be designed with care. BT stated that the storage and interrogation of data in the National Identity Register would be "heavily reliant" on the architecture, and this would

[468] Hansard, November 11, 2003: Column 173.
[469] Hansard, November 11, 2003 : Column 178.
[470] Hansard, December 20, 2004.
[471] 'ID card plans are too complex and too expensive, government is told', Bill Godwin, Computer Weekly, February 15, 2005.

require "a high performance system".[472] Northrop Grumman calls for the database to contain "a limited choice of biometric" to ease the implementation.[473]

It is likely that the costs will rise further as more users are added to the system. Uncertainty will also probably increase because of the prevalence of biometrics. The Government has already suggested the need for readers in every hospital and doctor's surgery. According to then Home Office minister Hazel Blears,

> "We also want to make sure that only the people who're entitled to use our public services like the National Health Service, making sure that people who contribute to it can use it and those who don't, can't. So, where it is necessary, then we will have to have the technology in place to read the cards."[474]

According to a Home Office statement, the estimated total cost will be £3.1 billion.[475] A detailed statement of this estimate was not provided to Parliament. It is hard to substantiate or justify this cost based on the published information. The Government has not, for example, stated which elements of the scheme this cost will cover, or the process used to derive those costs.

When the Bill was reintroduced, the Government announced a new partial costs estimate. In the Regulatory Impact Assessment, the Government announced that:

> "The current best estimate is that the total average annual running costs for issuing passports and ID cards to UK nationals is estimated at £584m. Some set-up costs will be incurred after the first ID cards/biometric passports are issued as it will be more cost effective to build parts of the infrastructure incrementally."[476]

The new price rise was due to "allowances for contingency, optimism bias and non-recoverable VAT."[477]

The Government identified the running costs of the scheme as

1. the issuing of passports and ID cards;
2. the maintenance of passports and ID cards – e.g. to issue replacements for lost documents; and
3. the verification service – e.g. through charges to accredited organisations.

The Government's best estimate for the costs was set at an "indicative unit cost" £93 per card, for a card that is valid for 10 years.

---

[472] 'Memorandum submitted by British Telecommunications plc' to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we04.htm.
[473] 'Memorandum submitted by Northrop Grumman', submitted to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we40.htm.
[474] 'U.K. to Put Biometric Readers in all Hospitals, Blears Says', Bloomberg, September 29, 2004.
[475] 'ID trials: What is involved?' BBC Online, April 24, 2004.
[476] 'Regulatory Impact Assessment', released by the Home Office for the Identity Cards Bill, Introduced to the House of Commons on May 25, 2005, available at http://www.homeoffice.gov.uk/docs4/Identity_cards_bill_regulatory_impact.pdf.
[477] Ibid.

> "The actual amount charged to a person will depend on future policy decisions on charging within the scope allowed by the Identity Cards Bill …."[478]

It has been suggested that organisations wishing to perform on-line verification would have to pay for the link and for the card readers. The readers were estimated at £250-£750, depending on their level of sophistication.

These numbers are surprising in view of a biometrics report commissioned by the Government, written by the National Physical Laboratory, which predicted costs as below.

Item	Unit Cost	Number	Item Cost
Licence fees for biometric components, software, etc.	£1 per person	50,000,000 people	£50 million
Biometric hardware at front office	£5000 per front office	2000 offices	£10 million
Biometric hardware for remote enrolment	£2000 per front office	2000 offices	£4 million
Hardware at back office, networks, etc.			£10 million
Marketing and publicity	£1 per person	50,000,000 people	£50 million
Enrolment (allowing 10 minutes per person)	Staff costs £40 per hour	50,000,000*10/60 hours	£330 million

Table 5 - Costs of 2003 Proposed Scheme, from 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', for UKPS, DVLA and the Home Office, page 29.

While this outlined merely the 'Entitlement Card' scheme of 2003, biometric hardware was already estimated at £5000 per office.

The Importance of Scope

One consistent problem with the Government's statements on the estimated cost of the National Identity scheme has been the absence of any scope statement to define how the costs have been calculated. The various figures cannot be compared when there is no common baseline against which to evaluate them; nor can an independent assessment be compared directly with Government figures.

What is clear is that the cost of the National Identity Cards scheme has been bound into that of passport reform, since these two areas share many common functions and issues.

Confusing Passports and ID Costs

The Government has stated its intention to absorb the costs of the National Identity scheme by increasing the cost of passports. However, this has lead to confusion between identity cards and passports, and a blurring of the boundaries of functionality and cost. In an article published on his first day as Home Secretary, Charles Clarke commented in the Times:

[478] Ibid.

> "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."

As we have pointed out elsewhere in this report, the biometric passport and the identity card are quite separate instruments. Below we show how the accounting for these projects seems to blur the boundaries.

Mr Des Browne concluded the second reading of the Bill with a roundup responding to questions of costs and passports.

> "Among other memorable moments was the admission by the hon. Member for Winchester (Mr. Oaten) that we need to spend money to put biometrics into passports. We now have the Liberal Democrats' support for that. Will he therefore now explain why he and his colleagues have been making an arithmetical calculation that takes all that money out—[Interruption.] He says from a sedentary position that his calculation is on top of that. I can do the arithmetic as well as he can. The Liberal Democrats took the £450 million, which he now says must be spent on passports, added to that the £85 million, and the £50 million for verification, multiplied it by 10, and have gone around television and radio studios saying that the proposal will cost £5 billion, plus, in some cases, the £85 for each individual. Perhaps now we shall hear some honesty about the arithmetic of that policy from the Liberal Democrats, so that we can have a proper debate."
>
> ...
>
> "The cost of biometric passports is estimated to be £415 million per annum by 2008–09. Reusing passport infrastructure for ID cards saves money on issuing both separately. The cost of introducing ID cards for UK citizens on top of passport cost is £85 million. We estimate an additional £50 million per annum to provide verification services. In addition, as we set out in November 2003, we estimate set-up costs in the first three years to be £186 million. There will be some additional costs beyond this period. We are continuing to work on these estimates and will inform the House when we are in a position to provide updated figures." [479]

In March 2005 the Passport Office released its assessment of the likely rises in costs for passports. As argued elsewhere in this report, the Government has confused the international passport requirements with the proposals for a national ID card. This confusion has a substantial influence on costings.

The Government intends to transform the Passport Office into a new department that is responsible for Identity. According to the Home Office Minister:

[479] Hansard, December 20, 2004.

> "These changes will also lay the foundations for the Government's proposed national identity cards scheme – which would help tackle identity fraud, organised crime, illegal immigration, and terrorism, as well as making it easier for UK citizens to travel and to carry out everyday transactions securely and conveniently. The UKPS would be a key part of the new Home Office agency that would be established to run the scheme."[480]

Yet in March 2005 the Passport Services made clear that it intended to include only digital photographs in all passports beginning in 2006.[481] While this is ideal for passports, digital photographs are not the biometric foundations of the identity card. The form of verification that the Government foresees for identity cards requires additional and more accurate biometrics such as fingerprinting of multiple fingers.

Even without the use of additional biometrics in the immediate term, the costs of the passport are increasingly disproportionate. For example, the Passport Service intends to require interviews for all first-time applicants. Such a process is relatively unnecessary for the issuance of passports, and our research could not find any other country that intends to implement a similar process. The US, for example, only requires that documentation be included in all first-time applications (e.g. birth certificate), but does not require this documentation for renewals. The interview process is appropriate only if the Passport Service is intent on collecting biometrics that require face-to-face meetings, involving the collection of fingerprints and iris scans. Digital photographs are not dependent on such interviews.

The Passport Service is also implementing a central database, containing data relating to every passport holder. According to the Passport Service, "current research has identified that there could be significant benefits in storing the data on a person-by-person rather than a passport-by-passport basis." By introducing interviews and a central database the Passport Service is developing the infrastructure for the identity card. This is likely to cost more than if it was merely developing the infrastructure for a standardised biometric passport.

Consequently, all these additional programmes and services force the Passport Services to raise the costs of delivering biometric passports. According to the Passport Service,[482] the cost of passports, in their current form with a single digital photo, is set to increase by 91%.

	2004/2005	2005/2006	2006/2007
Passport Output ('000s)	6386	6910	6853
Average Unit cost per passport	£35.60	£42.36	£67.93

Table 6 - Unit costs per passport, UK Passport Service Corporate and Business Plan, 2005, p.30.

This is a remarkable increase, and it is important to note that this does not even include the costs of issuing the identity card with additional biometrics.

[480] 'UK Passport Service: Improving Passport Security and Tackling ID Fraud', Reference: UKPS001/2005 - Date: 24 Mar 2005, available at http://www.homeoffice.gov.uk/n_story.asp?item_id=1282.
[481] 'UK Passport Service, Corporate and Business Plans 2005-2010', UKPS, available at http://www.passport.gov.uk/downloads/UKPS_CBP_2005-10.pdf.
[482] 'UK Passport Service, Corporate and Business Plans 2005-2010', figure 4.1 on page 30.

The rise in costs cannot be entirely explained by the costs of meeting international obligations. Other countries are implementing biometric passports without similar price increases. For example, the US Government has proposed a maximum cost increase of 20% for new passports. The German Government advertised their new passport costs of 59 euros by emphasising that it will cost almost half as much as those in the UK.[483]

This situation arises because of the blurring of the boundary between passports and identity cards, and the resulting administrative costs. According to UKPS,

> "The large increase in the average unit cost per passport in 2006/07 is based on a number of our improvement initiatives, in particular Authentication by Interview (AbI), the Personal Identification Project (PIP) and facial biometric chips (ePassports) being implemented completely. As explained throughout this Plan, these steps are essential if we are better to safeguard our customers' identities."

The reality is that these initiatives are only required to support ID cards. The Government is a victim of confused thinking if it believes the increased costs of passports cannot be attributed to international obligations.

The figures suggest that the costs of passports are rising to meet the national ID register at a notional half-way point, and then will rise again to finally incorporate additional costs of the national ID infrastructure. The quality of the debate on these matters will not improve without a clear understanding of the ICAO standards and the US obligations, along with a comparative study of what other countries are planning.

Improvements in Government Cost Assessments

Arguably the Government has made a number of positive steps to better understand the challenges of IT projects, and in particular, to understand the challenges of implementing the ID card programme. One step is a set of reports and studies that were commissioned to better understand the technology that may be used in the project; another was the use of 'Gateway Process' reviews to ensure that programmes are on course and are feasible.

Unfortunately in both cases the Government has not been sufficiently open and transparent on the outcomes of these studies and their assessment of the costing and feasibility of the ID Card programme. The reasons for this are explained below.

Sparse Studies

This bill represents a substantial increase in Government IT expenditure, creating what will be one of the largest single IT projects in the world. It is surprising that so little is known even at this advanced stage of planning. As mentioned above, this uncertainty will only increase costs, and could possibly lead to the failure of the project.

[483] 'Biometric passports are to cost 59 euros', heise online, June 2, 2005, available at http://www.heise.de/english/newsticker/news/60204.

The deliberative process on this bill has already suffered from a lack of open discussion on projected costs. The Home Affairs Committee was warned by a variety of experts that detailed specifications were required in order for costs to be reigned in, and without adequate research, the specification would remain ambiguous. For instance, the UK Computing Research Committee argued that a number of questions remain unanswered:

- "How long could this process be permitted to take (mean, median and maximum) before the delays became unacceptable in the most time-critical of the required functions?
- What level of false positive matches (fraudulent use not detected) is acceptable for the most demanding function for which the card would be required?
- What level of false negative matches (legitimate use rejected by the system) is acceptable for the most demanding function for which the card would be required?
- What level of failure to obtain any matches (biometric not able to be read) is acceptable for the most demanding function for which the card would be required?
- Would all necessary data about the cardholder be contained on the card itself, or would there need to be interrogation of one or more databases?
- How would the authenticity of the data on the card (or in any associated databases) be established initially? What is the acceptable error rate in this data?
- How sensitive (private/secret) is the data on the card or on any associated database? (This will influence the necessary security mechanisms).
- Will any databases be accessible from public terminals or connected to the Internet?
- How many people/locations will need to be able to read the data on any databases?
- How many people/locations will need to be able to alter the data on any databases?
- What mechanisms are required to allow the cardholder to have access to, or to modify, any or all of the data held about them?"[484]

These questions cannot be answered without detailed studies into the use of biometrics, detailed consideration on the content of the cards, trials of cross-country implementation, and clear operational guidelines.

Particular reference should be made to one study on the feasibility of biometrics conducted by the National Physical Laboratory and BTexact (hereafter referred to as 'the NPL report') conducted in 2003 (see section on Biometrics). The UK Computing Research Committee found this study to be 'competent' and supported the conclusions, although with the caveat:

[484] 'Memorandum submitted by the UK Computing Research Committee', submitted to the Select Committee on Home Affairs, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we52.htm.

> "that the analysis of error rates for the only biometric that appears to be feasible for the envisaged system (iris scanning) have been drawn from two sources of limited dependability. The first is a study of only 200 volunteers, a sample unrepresentative of the general population.[485] The other is a study by the company that holds the patents for the technology and which would be a major beneficiary of any widespread introduction of iris scanning systems."[486]

The NPL report concluded that the choice of biometrics should be made once additional information became available, through further studies and consultation. The Computing Research Committee concluded similarly:

> "We believe that a well-controlled, independent, large-scale study should be undertaken before any decision is made to commit to a particular biometric technology, to ensure that the necessary low error rates can be achieved for a population of 60 million people, and that no minority group is unacceptably disadvantaged by the chosen biometric."

Subsequent studies that were conducted were of some value; though the results were delivered too late to inform debate on the first occasion that the Bill went through Parliament. In the Spring and Summer of 2004 the Home Office promoted a trial-run of the biometric systems envisioned for the new passports and identity cards. The trial was conducted by the Passport Service in London, together with three other centres around Britain and was led by Atos Origin.

The trial involved 10,000 volunteers. At an early stage of the work the Home Office argued that:

> "The trial is about testing the effectiveness of the technology. We will want to know if we need to have the three biometric details. For example someone may have an eye problem so the iris scan may not work properly. Another person may have a disability which prevents us taking fingerprints. We are just trying to establish the practical aspects of incorporating the information into the biometric database. We will use the exceptional cases to test the robustness of the system. [...] We are confident that we are using cutting edge technology and we also need to be aware of the risks of fraud. This is the best technology available so we need to make sure we are recording information in the right way."[487]

Shortly afterwards it became known that the trial had been delayed by three months because of difficulties with the hardware and software[488] even though the equipment had been fully tested by the contractor. In acknowledging the delay, the Home Secretary David Blunkett argued that "it is important to get it right rather than get it quickly."[489]

---

[485] http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf.
[486] 'Memorandum submitted by the UK Computing Research Committee'.
[487] 'ID Trials: What is involved? BBC Online', April 24, 2004
[488] 'ID card trials put back by technical glitches', Richard Ford, The Times, May 5 2004
[489] Ibid.

In October 2004 the Prime Minister expressed his own participation in the programme.

> "This morning also I took part in the trial testing of the new biometric technology for identity cards. It is important we get this technology right and ensure it will be user-friendly for the public. That is of course the purpose of the trial. Overall progress is very encouraging and I am confident we can successfully develop a secure biometric ID card for the whole country, and I think ID cards have an important role to play in fighting serious crime and terrorism and tackling illegal immigration."[490]

The programme was due to be completed in three months, however. In November the trial was extended to address concerns expressed by disabled people.[491]

The final report was due to be released in September 2004 but publication was again delayed to May 2005, at which time it was released in conjunction with the Bill.

The report's findings, which provided a disappointing result for the accuracy of biometric technologies, are considered in more detail elsewhere in this report.

However, when the issue of technological effectiveness was raised in Parliamentary debates, the Government was adamant that the technology functioned well. In the Second Reading in the House of Lords, Baroness Scotland stated:

> "Biometrics are a new concept and some have asked us the obvious question: will it work? I can reassure noble Lords that the National Physical Laboratory carried out a study in 2003 and published a report which concluded that:
>
> > 'In principle, fingerprint or iris recognition can provide the identification performance required for unique identification over the entire UK adult population.'
>
> Not only that, but the United Kingdom Passport Service has also carried out a trial of biometric enrolment of a sample of some 10,000 individuals to test the practicalities of enrolling biometrics. This has included using a mobile enrolment unit that could travel to rural areas as well as to offshore islands."[492]

The report was not ready in time for the consideration of Parliament when the Bill was first presented.

The Home Office Science and Technology Reference Group is also due to publish a report on the Identity Cards Programme. In response to a parliamentary question in December 2004, the then Home Office Minister Des Browne said:

---

[490] PM Press Conference, October 25, 2005.
[491] 'Cost of ID card and passport rises to £85', Alan Travis, The Guardian, November 3, 2004.
[492] Hansard, March 20, 2005.

> "The Home Office Science and Technology Reference group has not reached any conclusions about the Identity Cards Programme. The Group recognises there are a number of scientific and technical challenges that the programme will be tackling and it will be following up its initial discussion of the Identity Cards Programme at a later date. This is in addition to the follow-up discussions already held between some members of the Science and Technology Reference Group and Identity Card Programme staff. The Government's Chief Scientific Adviser will also be chairing an external panel to provide systematic peer review of the scientific and technical advice provided to the Identity Cards Programme."[493]

One of these reports was referred to in a later statement in Hansard. According to the Home Secretary:

> "An assessment is under way on the different forms of biometrics that could be used, such as fingerprints, iris examinations and photographs. I am confident that, as in many countries throughout the world, the biometric regime that we establish will provide the security that people rightly look for. The Bill has been given proper scrutiny. Indeed, in preparation for the legislation, we started a six-month public consultation exercise in 2002."[494]

This report has not been released.

Gateway Reviews

All these issues led to the development of Gateway Reviews by the Office of Government Commerce in 2000. The OGC was to work with departments to improve the management of IT-enabled projects. One of the key requirements from the OGC on all departments is that "no government initiative (including legislation) dependent on new IT to be announced before analysis of risks and implementation options has been undertaken".[495]

The 'gateway review process' is promised to provide "an independent assessment of the status of IT-enabled and other projects at various stages of the procurement lifecycle."[496] Its goal is to examine a "project at critical stages in its lifecycle to provide assurance that it can progress successfully to the next stage; the process is based on well-proven techniques that lead to more effective delivery of benefits together with more predictable costs and outcomes."[497]

The review process involves six 'key gates'.

---

[493] Hansard, December 20, 2004, Column 1501W.
[494] Hansard, Debate on Clause 31, February 10, 2005.
[495] 'Improving IT procurement: The impact of the Office of Government Commerce's initiatives on departments and suppliers in the delivery of major IT-enabled projects', a Report by the Comptroller and Auditor General, National Audit Office, HC 877 Session 2003-2004, November 2004, p.3.
[496] Ibid., p.6.
[497] 'The OGC Gateway Process – designed for your success', Office of Government Commerce, available at http://www.ogc.gov.uk/index.asp?id=377.

> "There are five OGC Gateway Reviews during the lifecycle of a project, three before contract award and two looking at service implementation and confirmation of the operational benefits. In addition there is a repeatable Gate 0 for programmes, designed to confirm the feasibility and viability of the initiative when set against other corporate priorities and objectives. Further Gate 0 reviews later in the life of the Programme can revisit and confirm the business case, the management of programme risks, the management of the portfolio of the projects, and the delivery of benefits."[498]

These stages are as follows:

Gateway Stage	Purpose	Description
Gateway Review 0 Strategic assessment	**Establish business need for programme**	Asks how the proposed programme meets the business need that lies behind it. Assesses the capability of those who are responsible for the programme and the support of users and stakeholders.
Gateway Review 1 Business justification	**Develop business case**	Asks whether the end project is feasible, affordable, and likely to achieve value for money. Also whether the high-level plans for establishing it are clear and realistic.
Gateway Review 2 Procurement strategy	**Develop procurement strategy**	Asks whether the tendering strategy sufficiently reflects business requirements, awareness of the market, good practice in procurement, and changes to business need. Asks whether funding is available for the whole project, and with adequate financial controls in place.
Gateway Review 3 Investment decision	**Competitive procurement**	Asks whether the tendering process has met its objectives and followed good practice, and whether the prospective contractor is likely to deliver on time, within budget and achieve value for money. Assesses readiness of the business to implement the contract.
Gateway Review 4 Readiness for service	**Award and implement contract**	Assesses whether project plans are up to date, and adapted to working successfully with the contractor. Asks whether implementation of the project is going to plan, with any lessons for the future being recorded.
Gateway Review 5 Benefits evaluation (repeated as required)	**Closure**	Assesses whether expected benefits are being delivered, and what is being done to pursue continued improvements. Asks what contingency plans there are for future changes.

Table 7 Gateway Stages and the Product Lifecycle, taken from NAO report "Improving IT procurement", 2004, p.15.

The Home Office has undertaken most reviews of its systems to date.[499] The NAO conducted a study on the OGC's activities and found that some progress was being made in government projects, but much remains to be done.

It is important to note that the Gateway process was applied to the Criminal Records Bureau case. The OGC raised questions about the readiness of the project to go live, but accepted there was 'no turning back' and let the system launch regardless.[500] The output of the Gateway review process on the Identity Cards projects should be scrutinised closely – and publicly – before the project is permitted to proceed.

[498] 'Improving IT procurement: The impact of the Office of Government Commerce's initiatives on departments and suppliers in the delivery of major IT-enabled projects', p.7.
[499] 'Improving IT procurement', p.18.
[500] 'Criminal Records Bureau: Delivering Safer Recruitment?', Report by the Comptroller and Auditor General, HC 266 Session 2003-2004, February 2004, p.3.

Identity Cards Programme Gateway Reviews

The Identity Cards Programme has been subject to Gateway reviews by the OGC. The first such review was completed in January 2004.[501] The Home Affairs Committee was informed that the OGC had also conducted prior reviews.[502] The Home Office has, however, been reluctant to release the results of the reviews. The Government was asked about this on January 31st 2005,

> "Mr. Oaten: To ask the Chancellor of the Exchequer if he will publish (a) the Office of Government Commerce's (OGC's) Gateway Zero review into the identity cards scheme and (b) all other OGC reviews of the scheme. [208284]
>
> Mr. Boateng: I am currently reviewing whether there is any Gateway Review or other OGC review which should be published regarding the identity cards scheme and I will write to the hon. Member as soon as these considerations are complete."[503]

A Freedom of Information Request was filed to gain access to the pre-Stage Zero and the Stage Zero reviews. The OGC responded that the information was exempt from the Freedom of Information Act.

> "s.3391(b) and 92) of the Freedom of Information Act 200 (the Act) as OGC is a public authority with functions in relation to the examination of the economy, efficiency and effectiveness with which other public authorities use their resources in discharging their functions, and disclosures of the requested information would, or would be likely to, prejudice the discharge of those functions.
>
> The OGC gateway Review process depends for its efficacy and promptness on 9a) the candour of interviewees and (b) the reasonable reliance then placed on reports by the particular individuals to whom reports are solely addressed (usually Senior Responsible Owners or SROs), the confidence of interviewees and the SRO in the integrity of the OGC Gateway process is thereby central to the success of the Gateway Review process in the ID cards programme."[504]

These exemptions are subject to the 'balance of the public interest', and required a further fifteen days to complete that balancing exercise. The Home Office responded with a similar letter shortly afterwards.[505]

---

[501] House of Commons Hansard Written Answers for December 9, 2004, pt25.
[502] Home Affairs Committee Minutes of Evidence – Volume II (HC 130-II), statement of Katherine Courtney to the Committee under Question 36, posed on December 11, 2003.
[503] House of Commons Hansard Written Answers for January 31, 2005 (pt 11), available at http://www.publications.parliament.uk/pa/cm200405/cmhansrd/cm050131/text/50131w11.htm
[504] Response under the Freedom of Information Act Request Reference no.92247, February 1, 2005, archived at http://www.spy.org.uk/foia/archives/foia_requests_in_progress/ogc_gateway_reviews_of_the_identity_cards_programme/index.html.
[505] Response under the Freedom of Information Act Request from the Information Policy Team of the Home office, February 1, 2005.

Fifteen days later the Home Office "concluded that the balance is in favour of non-disclosure".[506] The Home Office did release some "background information contained within the two Gateway 0 Reviews". The background documentation on the Gateway Zero review from 2003 merely repeated Home Office policy on the need for an identity card. The background documentation for the Gateway Zero review of 2004 held additional information that eventually became part of the draft Bill of April 2004, merely updating the Home Office existing public policy statements.

While appeals were being filed with the OGC for an internal review, a further parliamentary question was posed.

> "Mark Oaten (Winchester, LDem): To ask the Chancellor of the Exchequer what traffic light status was awarded to the identity cards scheme by the Office of Government Commerce at the Gateway Review 1 stage."
>
> "Paul Boateng (Brent South, Lab): The ID Cards programme has not yet undergone a Gate 1 Review. It has, however, undergone two OGC Gate 0 Reviews, in June 2003 and January 2004 respectively. The traffic light status awarded by these reviews is exempt from disclosure under the Freedom of Information Act 2000 as disclosure would be likely to prejudice both the ability of OGC to examine the effectiveness, efficiency and economy with which other Government Departments exercise their functions and also the formulation and development of Government policy. I believe the public interest in disclosure of such information is outweighed by the public interest in non-disclosure."[507]

The Home Office did not respond to a request for Internal Review. As a result, to this date we are unable to ascertain the details of the Gateway reviews, and we consequentially cannot fully ascertain the levels of knowledge, appreciation, and concern within the Home Office regarding the risks and costs involved in taking the Identity Cards programme forward.

The purpose of this section was to review the reasons for past failures in government IT projects. These failures have led to serious problems with sometimes dangerous repercussions. A system on the scale of the Identity Cards programme will have similar problems and repercussions, particularly because of the architecture selected by the Home Office. Some innovations have been introduced into the Government IT procurement process, but because the Home Office is unwilling to disclose either its process of consultation with industry organisations or the details of the risk management process under the OGC, we are unable to ascertain whether these innovations were of any benefit to the Identity Cards Programme.

This leads us to conclude that there is a risk the Government is not adequately protecting this project from the fate that lay in store for its other large and complex

[506] Response to Freedom of Information request, From the Information Policy Team of the Home Office, February 22, 2005.
[507] House of Commons Hansard Written Answers for March 16, 2005.

systems. The UK Computing Review Committee is sceptical of the feasibility of the programme, even with the OGC process:

> "We are aware of the improvements made through the OGC Gateway process, but we see nothing in that process which would deal with the engineering complexities of this (or any similar) project, and enable the procurement to proceed at reasonable levels of risk."[508]

This situation is also hurting the deliberative process. Parliament is being asked to approve a bill that will involve significant costs, but Parliament is not being informed of these costs. When the Home Affairs Committee reported this concern, the Home Secretary responded:

> "I do not accept that it is appropriate to release detailed, market-sensitive information about the financial and contractual aspects of the scheme at this stage. I understand the desire for more information, but we need to balance this with our duty to ensure we get the best value for money for the taxpayer."[509]

We believe, in view of the Government's track record, that the balance should veer more towards disclosure.

The Challenges of UK Government IT Projects

To better understand the likely implementation challenges – and associated costs – of the National Identity scheme we need to look at the dynamics of the use of information technology by the UK Government. In many ways the UK Government IT environment is unique, and the dynamics of this environment will influence the level of success of the identity card proposals.

We will draw lessons from some of the challenges faced by other government IT programmes. One significant factor in public sector procurement is that in recent years the UK Government has tended to make substantial amendments to projects once they have commenced. This binds the Government to the existing contractors, and raises costs.

In light of the problems that have arisen in the NHS programme for IT, we recommend that Parliament wait for the results of outstanding research reports before approving a project of the size and complexity of the national ID system.

We also recommend against the UK model of 'enabling legislation' and instead move toward developing a clearly defined project with specific guidelines based on primary legislation.

[508] 'Memorandum submitted by the UK Computing Research Committee'.
[509] 'Response to Home Affairs Select Committee Report on Identity Cards', Home Office press release issued July 30, 2004, available at http://www.homeoffice.gov.uk/n_story.asp?item_id=1047.

In Context: Government IT

The UK Government has a long history of creating large-scale IT projects such as a national ID infrastructure. In fact, the Government leads the world on very large and very long-term IT outsourcing contracts (e.g. the Inland Revenue project). Unfortunately these contracts are typified by large contract prices and few safeguards.[510]

Common Project Challenges

In 2002 it was reported that central civil government departments had around 100 major IT projects in their initial stages of procurement with a total value of £10bn.[511] In 2003 the Government's expenditure on information technology was estimated at £2.3bn.[512] Ten departments accounted for three-quarters of the total expenditure, and five suppliers won 60 percent of contracts.[513] The Home Office ranks third amongst all government departments for IT expenditure.[514]

However, these projects all too frequently end in failure or substantial cost increases or delays. The delays in implementing new technology can put service delivery at substantial risk. The NAO cites the Home Office project to improve handling of immigration, asylum and citizenship cases, giving the assessment that the project suffered because of late delivery of computer systems.[515] This resulted in recommendations from the NAO that called on departments to consider whether a project may be "too ambitious" and to agree details early in the process.[516] Some of the common problems and associated causes are identified in the table below.

[510] 'Government IT Performance and the Power of the IT Industry: A Cross-National Analysis', Patrick Dunleavy, Helen Margetts, Simon Bastow and Jane Tinkler, Paper to annual meeting of American Political Science Association, Chicago, 1st-5th September, 2004, Panel 25-2 'Digital Policy Issues: Inequality, E-government', September 4, available at http://www.governmentontheweb.co.uk/downloads/papers/Government-IT-Performance.pdf.
[511] 'Better Public Services through e-government', a Report by the Comptroller and Auditor General, HC704-I, Session 2001-2002, April 2002, p.1.
[512] 'Improving IT procurement: The impact of the Office of Government Commerce's initiatives on departments and suppliers in the delivery of major IT-enabled projects', a Report by the Comptroller and Auditor General, National Audit Office, HC 877 Session 2003-2004, November 2004, p.14.
[513] Ibid., p.10.
[514] Ibid., p.14.
[515] 'Better Public Services through e-government', p.17.
[516] 'The Home Office: The Immigration and Nationality Directorate's Casework Programme', National Audit Office Press Notice, HC277, March 24, 1999.

Commonly identified problems to be addressed with Government projects[517]	Common causes of failure in IT-enabled projects[518]
- Civil servants ability and aptitude to use IT - More resources to support change programmes - Further technological improvements to update existing systems - More reliable assessments of costs and benefits ('Generally, departments lack baseline data against which to monitor and measure improvements in efficiency made possibly by IT) - Partnerships with other organisations are needed to deliver integrated IT services - the risk of IT-enabled change adversely affecting existing services requires careful management - the risk of IT-enabled change adversely affecting existing services requires careful management	1. Lack of clear link between the project and the organisation's key strategic priorities including agreed measures of success. 2. Lack of clear senior management and Ministerial ownership and leadership. 3. Lack of effective engagement with stakeholders. 4. Lack of skills and proven approach to project management and risk management. 5. Lack of understanding of and contact with the supply industry at senior levels in the organisation. 6. Evaluation of proposals driven by initial price rather than long-term value for money (especially securing delivery of business benefits). 7. Too little attention to breaking development and implementation into manageable steps. 8. Inadequate resources and skills to deliver the total delivery portfolio.

Table 8 – Common problems and causes of failure in Government IT projects

Previous failures in the air traffic control systems, ambulance dispatching services, criminal records databases, benefits payment systems and other financial systems, and even the national fingerprint information system have already proven to be hazardous. In November 2004 the national automated fingerprint identification system (Nafis) crashed, shutting down access to and from all police forces. This system is operated by Northrop Grumman and holds 4 million records. It went off-line on the 24th November and some forces were not reconnected until a week later.[519] When the Government proposes that ID cards are central to Government systems, a failure could have a substantial and wide ranging impact. According to a Home Office Minister,

[517] 'Better Public Services through e-government', NAO, April 2002.
[518] 'Improving IT procurement', NAO, November 2004.
[519] 'Fingerprint system crash fuels doubts over ID card scheme', Nigel Morris, the Guardian, December 3, 2004.

> "ID cards and the national register would be right at the centre of the wheel, and a whole range of spokes could be built up around it to meet a broader vision."[520]

A failure of the Identity Card system could shut down our borders, restrict access to health care, prevent access to benefits, and reduce the security of the country. According to one observer, "[t]he consequences of anything but the briefest failure of the system could prove catastrophic."[521]

Similarly, a lack of training can result in departments failing to provide necessary services. The Passport Agency previously failed to assess and test adequately the time needed by staff to learn and work with the new system, resulting in serious delays in issuing passports.[522]

Another challenge that was identified by the NAO was that service delivery was put at risk if "departments are slow to modernise existing IT and fail to adopt appropriate standards to ensure that different systems are interoperable, secure and meet data protection and privacy needs."[523] The NAO calls for a user-led approach to these systems. Such an approach would focus on the needs of the user, creating incentives for public interaction and use.[524]

One important example of an identity project failing is the Benefits Payment Card project, which was started in May 1996 but cancelled in May 1999, is analogous to the Identity Card.[525] The project was intended to replace paper-based methods of paying social security benefits, and to automate the national network of post offices. The purpose was to provide a 'virtually fraud-free' method of paying benefits, reduce costs of transactions, increase efficiency, improve competitiveness, aid accounting, and improve service. It was estimated to cost £1 billion, and a trial project was assumed to take ten months to implement. One year into the project the contractor notified that the costs would either have to increase by 30 percent or the contract extended by five years with costs increased by 5 percent. Three years later the trial had not even begun, and the government decided to abandon the project.

A review by the NAO tried to assess what had gone wrong. It argued that the project was high risk and ambitious, "and with hindsight, probably not fully deliverable within the very tight timetable originally specified."[526] With an estimated 20,000 post offices to be equipped, involving 67,000 staff and 28 million customers per week, and 17 million benefits recipients claiming 24 different benefits, the demands on the system were easily identifiable as complex. A more rigorous process of selecting contractors was also recommended. The NAO concluded that there were a number of reasons for the

[520] 'Minister says ID technology is robust', Statement by Home Office Minister Tony McNulty, Kable's Government Computing, June 6, 2005.
[521] 'Memorandum submitted by British Telecommunications plc' to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we04.htm.
[522] 'Better Public Services through e-government', p.17.
[523] Ibid, p.35.
[524] Ibid, p.46.
[525] 'The Cancellation of the Benefits Payment Card project', Report by the Comptroller and Auditor General, HC 857 Session 1999-2000, August 2000.
[526] Ibid page 5.

project's failure, and these were not limited solely to its complexity and size, but rather down to project management.[527]

The Criminal Records Bureau is another project of similar magnitude, set up between the UK Passport and Records Agency and Capita plc. The Bureau is now a separate Agency, and manages the contract with Capita, carries out checks on the Police National Computer, and manages relationships with police, Registered Bodies and other Government Departments.[528] The Bureau now handles between 40,000 and 50,000 applications per week, guiding recruitment decisions for registered organisations.

The Bureau was supposed to start operations in September 2001 but a series of delays shifted the start date to March 2002. This occurred despite the use of independent consultants to check for due diligence in the contract bid process. The NAO instead attributes the delays to a number of reasons including

- The research on the needs of the system was poor, despite the use of a customer forum and 'roadshows' involving 5000 participants.
- Business processes could not cope with the volumes of errors and exceptions in the applications that arrived, and the complexity of dealing with both individuals and employers.
- There were limits on the number of users who could access the system at the same time, and the links between the Bureau and the Metropolitan police were slow.
- There were significant gaps of understanding in the relationship between the contractor, Capita, and the Agency.
- The Bureau could not establish data links with Customs & Excise and the British Transport Police.

When the Department for Education and Skills then announced in August 2002 that all school employees had to be vetted by the Bureau, the business process faced significant delays. Checks on social care and health care workers were delayed by up to six months. Checks on the Department of Health's list of persons considered unsuitable to work with vulnerable adults were also deferred. The Bureau's deficit is 68.2 million, though this is expected to rise to 98.8 million.[529] Fees have increased by 200%.[530]

These failures are part of a generalised problem in Government's ability to manage projects. The table below shows a recent summary of a number of government project failures over the years.[531]

[527] Ibid, p.11.
[528] 'Criminal Records Bureau: Delivering Safer Recruitment?', Report by the Comptroller and Auditor General, HC 266 Session 2003-2004, February 2004, p.1.
[529] Ibid., page 31.
[530] Ibid., p.5.
[531] 'The Coordination of e-Government in Historical Context', Joe Organ, Public Policy and Administration Volume 18, No.2, Summer 2003.

Project	Departments	IT Supplier	Dates	Notes
NPSISS-Case Record and Management System	Probation Unit/Home Office	Bull Information Systems	1995-99	Suspended at £6 million over budget. Poor planning, coordination and supplier problems blamed.
Benefits Payment Card	DSS/PO Counters Ltd	ICL Pathway	1996-99	Suspended in 1999 with £1 billion in abortive expenses. Over ambition, poor planning/coordination and supplier problems blamed.
New IT System	Passport Agency	Siemens	1997-99	Technical problems cost £12.6 million and 40-day delays in passport turnover. Management and supplier blamed.
NIRS2	Contributions Agency	Andersen (now Accenture)	1995-99	Continuing problems led to compensation of 38 million to pensioners.
IND Casework Program	Home Office	Siemens	1996-99	Delays and hardship were experienced through a 176,000 backlog of asylum and nationality cases.
LIBRA	Lord Chancellor's Office	ICL/Fujitsu Service	1998-	Collapsed in 2002 at 136 million over the initial budget and little improvement in service.
New IT System	CSA	EDS	2002-	Huge delays in a new IT system, 50 million over budget. Contributed to the CSA failing to collect £200 million.
E-Revenue	Inland Revenue	EDS and others	2001-	Technical/Supplier problems led to slow take up in online tax services. Security breaches and major error (£15 million of debts were wiped) also tarnished this flagship e-government project.
Disclosure	Criminal Records Bureau	Capita	2001-	Supplier errors caused delays and frustration for users. The project received significant negative press attention.
VAT Online	HM Customs & Excise	Microsoft/EDS	2001-	Pilot project had 66% dropout rate, as users were not attracted to the service.
Gateway	Office of the e-Envoy	Compaq	2001-	Following project problems relations with the suppliers broke down costing 6.7million, mostly recouped by the OeE selling off project assets.
Individual Learning Accounts	DfES	Capita	2000-	Allegations of security breaches and fraud led to its suspension. The relationship between DfES and supplier was criticised.
Census Online	Public Records Office	ESS/QinetiQ	2000-	Service was overwhelmed and suspended for months after 4 days. Supplier/department relations were criticised.
CPS Tracking System	Crown Prosecution Service	(PFI contract)	1990-	Over budget and delayed, the project was downscaled in 1997, to the detriment of the intended service improvements.
Housing Benefits IT System	DSS/Benefits Agency	EDS/IBM	1999-	Delays in the roll out of the system exasperated attempts to combat widespread benefits fraud.

Table 9 - Government project failures, from "The Coordination of e-Government in Historical Context", Joe Organ, Public Policy and Administration Volume 18, No.2, Summer 2003.

Two trends that may be identified from the above list of failures are the problems with security and the poor relations with contracting companies. This was subsequently highlighted by the House of Commons Public Accounts Committee, which raised privacy, security and accordingly confidentiality as a particular concern to users.[532]

These prior failings led the UK Computing Research Committee to warn the Home Affairs Committee:

> "UKCRC believes that a major factor in these failures is the unwillingness of Departments and of major IT suppliers to accept that developing software-intensive systems is an engineering task of equivalent complexity to designing a modern aircraft or building a novel sky-scraper. Because the engineering complexity of the task is not recognised, insufficient attention is given to using the best science embedded in the strongest engineering processes (a mistake that would never be made by aeronautical or civil engineers). We believe that the quality of software engineering employed on many projects is lamentable and exposes the projects to unacceptable risks of failure; unless this problem is addressed vigorously and successfully, we believe that any national ID card system will overrun dramatically and will almost certainly fail to achieve its objectives."[533]

The UKCRC is an Expert Panel of the British Computer Society, the Institution of Electrical Engineers and the Council of Professors and Heads of Computing. They concluded that significant changes in the practice of Government Computing would be required.

A Challenging Environment for Successful Projects

The UK Government has been generally unsuccessful at reigning in costs and concluding successful projects. According to one report,

> "[Private Finance Initiatives] processes were supposed to cut costs and improve deliver reliability by forcing contractors to internalise the risks of new IT systems development and to manage these processes more rigorously and tightly. For almost a decade a body of evidence accumulated casting doubt on this fundamental logic in relation to IT projects, where government could rarely bare the costs of catastrophic non-delivery and the asset value of non-working systems for contractors was also negligible. Only in 2003 did Treasury advice at last acknowledge that this was a doomed hope for government IT, withdrawing PFIs for IT projects because agencies and departments effectively had to keep intervening to bail out PFI contractors in difficulties every bit as much as with conventional procurements."[534]

[532] 'Progress in Achieving Government on the Web', Sixty-Sixth Report of Session 2001-02, HC 936, p.6 and 9.
[533] 'Memorandum submitted by the UK Computing Research Committee', submitted to the Select Committee on Home Affairs, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we52.htm.
[534] Ibid., p.20.

The UK Government has suffered a track record of cancellation of IT projects at intermediate stages and of projects that are acknowledged as wholly or partly non-working or non-productive.[535] In comparison with other countries, a large number of projects over the last decade have been scrapped, with significant losses of complete investments or with partial write-offs of investment. Many of these failures can be attributed to an ongoing insistence on highly centralized projects that give rise to increased uncertainty. Even as the Government moved on from the mistakes, failures, and incomplete projects of the 1990s, the uncertainty and inadequacy has continued into the e-government era. Research has argued that current projects seem "misplaced and overambitious", and that "central government should remedy the fundamental challenges of departmental IT project management before wide-ranging 'joined up' e-government schemes can be attempted."[536]

This is due in part to the political environment in the UK.

> "An absence of effective parliamentary scrutiny of legislation and a deficit of checks-and-balances internally under some conditions both contribute to a 'fastest law in the West' policy style in the UK. For instance, new tax, welfare and regulatory laws are regularly adopted by ministers and approved by Parliament for which IT systems have not yet been planned, tested or implemented, but which instead have to be constructed post-legislation from scratch, often within very demanding timescales."[537]

After the cost and time over-runs of years and the billions of pounds expended on a variety of systems, some e-government experts are sceptical.

The Government insists on achieving extremely broad 'purposes' for its identity card programme, leading to an unnecessarily complex system design based on vague principles. This point was made by the UK Computing Research Committee in its memorandum submitted to the Home Affairs Committee. The CRC warned the Government that if it continued to proceed with a plan based on ambiguous requirements and specifications without matching them to real-world requirements

> "it is inevitable that the technical requirements will change, leading to delays, cost escalation, and loss of control over project risks. We are advised that that a current study of problems of large scale projects by the Royal Academy of Engineering will report that poor project definition is one of the major contributors to project failure."[538]

Similarly, the British Computer Society notified the HAC that their

> "primary concern is that there does not seem to be any firm and fixed statement of what the system is meant to achieve, what success or

[535] Ibid., p.21.
[536] 'The Coordination of e-Government in Historical Context', Joe Organ, Public Policy and Administration Journal, 18-2, Summer 2003.
[537] 'Government IT Performance and the Power of the IT Industry: A Cross-National Analysis', p.22.
[538] 'Memorandum submitted by the UK Computing Research Committee', submitted to the Select Committee on Home Affairs, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we52.htm.

> failure criteria are imposed and which scope limitations have been imposed. Without such fixed objectives, the risk of failure is significantly increased. Given the already high risk attached to extremely large systems this would be a major concern."[539]

Rather, QinetiQ argued that the scheme should not be constructed around law and order, identity fraud and illegal migration and working. "It should instead be centred on the benefits to a digital society of the use of biometric authentication of registered identity."[540]

In comparison with other similar countries, the UK contract prices for government IT are relatively high. According to one study,

> "UK civil servants take great pride in insisting that competed contracts let under long terms achieve market-comparable or better prices, and point to scrutiny by the UK's strong supreme audit institution (the National Audit Office) to support their contention. And initial contracts let by departments and major agencies to contractors have often been competitively priced. However, the UK also became unique amongst the countries we analysed in the extent to which government departments effectively acknowledged that when policy changes or other new developments made alterations of existing IT systems essential then only the incumbent IT suppliers could constitute a plausible firm to deliver these changes. Large firms dealing with government grew expert in estimating the likely scale of policy-induced changes, often effectively driving a coach and horses through the carefully specified initial contracts. It became expected practice to pitch prices for initially competed tranches of work relatively low in the expectation that later revisions and extensions would create negotiated contracts of between 4 and 6 times the initial competed contract price. Assessing negotiated contracts for price competitiveness is sometimes attempted, by means of pricing standardly-designated 'function points' in systems, suggesting that initial prices are rarely matched later on."[541]

The report concludes that this leads to a situation where the UK "government-IT industry relations have become dangerously unbalanced."[542]

These aspects are reflected in controversy over the potential cost and complexity of the NHS National Programme for IT (NPfIT) the budget projection of which appears to have escalated from an initial procurement figure of £6 billion.[543] There is a National Audit Office report on the scheme due in the summer of 2005 which will examine the

[539] 'Supplementary memorandum submitted by the British Computer Society (BCS)', submitted to the Select Committee on Home Affairs, May 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we52.htm.
[540] 'Memorandum submitted by QinetiQ', submitted to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we52.htm.
[541] Ibid. p.28-29.
[542] Ibid. p.36.
[543] IT pain in the NHS tied to technology, Seamus Ward, Accountancy Age, November 17, 2004, http://www.accountancyage.com/features/1138663.

procurement processes used for placing the contracts, whether contracts are likely to deliver good value for money, how the department is implementing the programme, and the progress the programme has made. There would seem to be a case for waiting until the results of this report are known and its findings can be incorporated into the Government's assessment.

The legislative uncertainty and the constantly shifting goals give the UK one of the least admirable track records on large-scale IT projects. The infrastructure for the identity card, as envisioned by the Bill, is arguably one of the largest IT projects in the world. A database that will in time contain over 60 million records holding a vast amount of information, with on-line access, an advanced security model, and with hundreds of thousands of users, is not only difficult to design and implement, but will most likely be costly. It is for this reason that the general consensus outside of Government is that the card system will cost significantly more than the Government envisions.

In the following sections we will re-present what is known about the likely costs of the Government's proposed programme. More importantly, we will also draw out what remains unknown, rendering an enabling bill such as the one in question not only premature, but unlikely to achieve its stated goals.

16

Cost Assumptions – Costing the Government's Proposals

Cost Assumptions

Before examining details of the costings for this proposal, it is important to have a full understanding of the nature of the system that the Home Office is proposing. Unfortunately there is little detail available in the Bill itself, and the Home Office has been reluctant to disclose key data because of commercial confidentiality.

Significantly, the Home Office has not supplied essential figures. For instance, how many cards will be issued over a period of ten years? It has also been mute on potential challenges, such as how the ID card will be integrated into existing IT systems or to what extent the system will take account of the needs and wants of commercial organisations. However it is possible to reconstruct the Government's vision, and the challenges and costs that they foresee. This section reviews key Government documents that indicate some of the details of the proposed scheme. These include:

- The Entitlement Card Consultation document from 2002;
- The 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme' produced by NPL/BTexact[544] and issued in February 2003 for the UKPS, DVLA and Home Office;
- UKPS Corporate and Business Plans for 2003-2008; 2004-2009 and 2005-2010;
- The Identity Cards Bill Regulatory Impact Assessment, November 2004;
- The Identity Cards Bill Regulatory Impact Assessment, May 2005.

These documents bring together the design principles and considerations behind the Government's costing scheme.

When concrete plans for an identity cards system were first discussed in 2002, it was under the guise of an "entitlement card". The Home Office consultation report reveals to some degree the proposed structure and costs of the system.[545] Specifically, Annex 4 of this document, entitled 'How a Scheme might work in practice', gives the most helpful indication of the Government's aims. Annex 5 to this same Consultation document, 'Indicative Cost Assumptions', provides fuller information about the perceived set up

[544] Written by Toby Mansfield (National Physical Laboratory) and Marek Rejman-Greene (Btexact Technologies)
[545] As we have noted in the section of this report on Consultation, the Government's goals have shifted very little since the 2002 Entitlement Card consultation.

costs of the scheme; indeed, it outlines some costs at a level of detail that has not since been seen in a Home Office document.

A feasibility study on the use of biometrics in an entitlement scheme, commissioned by the Home Office, and conducted by experts at the National Physical Laboratory and BTexact, was released in February 2003.[546] The NPL/BTexact report deals with the feasibility of implementing a biometric in a national identity system that would apply to all British citizens and residents. The UKPS study on biometrics was released only in May 2005, and included results of the testing of the technology, as well as participant observations regarding the techniques involved.[547]

These documents apart, the only detailed description of the Government's vision and expectations appears in the Regulatory Impact Assessments. The first such RIA was released in November 2004, and re-released in May 2005 with slightly changed costings.

Essential Information

Cost estimates provided in the various Government reports cover a 10– 13 year period comprising three years to install the infrastructure, six years to roll out the scheme and four years of 'steady state' operation.[548] The costs are divided into 'set up costs' and 'operational costs', and have been increased or decreased from a 'central estimate' dependent upon the level of risk involved in the particular component of the scheme.[549]

The number of participants

The 2002 consultation document suggested that the number of people who would need to be enrolled in the scheme by the end of year six would be just over 51 million. This was calculated using population statistics from National Statistics. The number of additional people joining the scheme in the remaining four years was calculated from National Statistics estimates of the number of young people attaining 16, plus estimates from Home Office figures of non-casual visitors to the UK.[550] The final figure is estimated at 67.5 million people.[551] This is 35% higher than the figure quoted in the biometric feasibility study, which estimated that there would be only50 million participants.[552]

It is likely that the number of cards issued will exceed the number of people enrolled. This is because some individuals will hold more than one type of card, and also that replacement smartcards will be required because they are expected to wear out after 3-5 years.[553] The Home Office therefore anticipates that:

[546] 'Feasibility study on the Use of Biometrics in an Entitlement Scheme – For the UKPS, DVLA and the Home Office' By Tony Mansfield (National Physical Laboratory) and Mark Rejman-Greene (BTexact Technologies). Version 3/Issued February 2003.
[547] The findings of both of these reports are summarised and analysed in our section on Biometrics.
[548] Consultation Document, Section 5, 2002, paragraph 2.
[549] Consultation Document, Section 5, 2002, paragraph 3.
[550] Consultation Document, Section 5, 2002, paragraph 6.
[551] Consultation Document, Section 5, 2002, paragraph 8.
[552] NPL/BTexact study, 2003, paragraph 11.
[553] Consultation Document, Section 5, 2002, paragraph 7

- Allowing for those who hold more than one card (for example, a passport and an ID card), instances of loss or theft, and the 10-year lifespan of each card, 140 million cards would be issued
- If it were necessary to re-issue each card once during the 10- year period due to surface damage, the total number would be 230 million cards
- If the cards needed to be re-issued twice during the 10- year period, the total number would be 314 million[554]

Though the suggested scheme in the 2002 consultation document was based around the existing passport and driving licence systems, the DVLA's role in the national identity system was ultimately downplayed.[555]

Furthermore, the UKPS is considering a reduction in the period of validity of a passport, from ten years to five years,[556] which implies that for many individuals, passport fees will be payable every five years. The UKPS acknowledges that this will represent a major financial burden on customers, and that it could be operationally challenging, but it would remedy potential problems caused by chip damage and allow for the updating of biometric information.[557]

Type of Card selected

The choice of the type of card has implications for general system design and, in turn, the costs. In calculating draft estimates in the 2002 documents, the Home Office tried to assess the number of cards people possess and the frequency with which they have to be replaced as a result of loss, theft or amendment.[558] The total number of cards has been estimated using the current number of licences and passports issued by UKPS and DVLA each year and the additional number of people who need to be covered. It is assumed this latter category will require replacements at the same rate as those obtaining licences (8% of licence holders each year).[559] The cost of each card also depends on its longevity. Smartcards generally need replacing every 5 years (despite the Home Office's previous estimate of 3-5 years) and would cost slightly more than a simple plastic card. If a smart chip were incorporated, this would need to be replaced more frequently. In addition to costing more, it is estimated that it would need replacing twice during a 10- year period.[560]

The selection of the type of card has tangible cost effects. According to the 2003 figures, a traditional card, such as the driving licence, costs £2.50 per card. A smart card is predicted to cost a further £1. A more sophisticated smart card would cost £5.[561] Using this information, a plain plastic card system would cost £240 million over ten years; a simple smartcard re-issued once would cost £670 million over ten years; and a sophisticated smartcard reissued twice would cost £2007 million over ten years.[562]

[554]Consultation Document, Section 5, 2002, paragraph 8.
[555] Consultation Document, Section 4, 2002, paragraph 2.
[556] UKPS Corporate and Business Plans 2004 –2009, page 18
[557] UKPS Corporate and Business Plans 2004 –2009, page 23
[558] Consultation Document, Section 5, 2002, paragraph 28.
[559] Consultation Document, Section 5, 2002, paragraph 29.
[560] Consultation Document, Section 5, 2002, paragraph 30.
[561] Consultation Document, Section 5, 2002, paragraph 31.
[562] Consultation Document, Section 5, 2002, paragraph 31.

Who is to participate and Government Agencies implicated

With regard to entitlement cards for young people, the 2002 consultation document proposes the issuing of an entitlement card at the same time as the National Insurance card and number, which is currently issued to young people attaining 15 years and 9 months.[563] A lower fee for young people is suggested to encourage participation.[564]

It is acknowledged that foreign nationals, other than those staying for short holidays or business trips, will also be required to register. The work permit scheme currently covers these individuals, and a card would be valid only for the period of the work permit on which they entered the country. The Government notes that: "any changes to his employment status such as the extension of the work permit would require the issue of a replacement entitlement card".[565]

Citizens of other EEA countries would have to apply for an entitlement card, and applications would be made using passports or their respective identity cards. The full range of checks proposed might not be possible for citizens of other EEA countries, but checks would be made on the validity of the card or passport used. Applicants would also be required to provide biometric information to prevent any attempts at establishing multiple identities.[566]

Asylum seekers currently have to provide fingerprints (to a legal standard of proof) on arrival in the UK, and are then issued with an Application Registration Card (ARCs). An asylum seeker granted leave to remain would then be able to exchange their ARC for an identity card. If iris patterns were to be used in a proposed identity card system, iris patterns of all asylum seekers would also have to be photographed in order to ensure that records could be cross-matched.[567]

The Immigration and Nationality Directorate of the Home Office (IND) could be given responsibility for issuing cards to foreign nationals due to their existing expertise on the validation of foreign identity documents. However, a common database would be required to ensure that a foreign national did not apply for another type of card, such as a driving licence, using false foreign identity documents. This would also prevent UK citizens from applying for a further card by using false foreign identity papers.

Enrolment

The process of enrolling participants into the identity scheme is complex. The Government sees identity as being established through three sources: biometric identity; attributed identity (for example: name, place and date of birth and parents' names and addresses) and biographical identity.

The earliest estimate of costs was based on the total number of people covered by the scheme, rather than the total number of cards issued. Part of the costs of processing

[563] Consultation Document, Section 4, 2002, paragraph 43.
[564] Consultation Document, Section 4, 2002, paragraph 45.
[565] Consultation Document, Section 4, 2002, paragraph 48.
[566] Consultation Document, Section 4, 2002, paragraph 50.
[567] Consultation Document, Section 4, 2002, paragraph 52.

applications is covered by existing and additional staff costs. Some costs would be incurred at any regional location where biometric information was recorded, both in applications and in the use of recording equipment.[568] The 2002 consultation document estimated that the cost of 67.6 million people entering into the entitlement card scheme is £406 million.[569] Certain factors may vary this amount, notably that some applications will be more costly to process, for example, foreign residents or the housebound,, there may be insufficient demand from other organisations to participate and, conversely, a higher than expected willingness from other organisations to participate.[570] Taking these into consideration, the estimated cost is increased by 50% to £608 million.[571]

The Biographical Footprint

Establishing the 'biographical footprint' is an extensive process involving the accumulation of information on all participants. Examples given of information included in the biographical identity category are education/qualifications, electoral register entries, details of benefits claimed/taxes paid, employment history, marriage certificates issued, mortgage account information/property ownership, insurance policies and history of interaction with organisations such as banks, creditors, public authorities and utilities.[572]

The Government foresees regularised and routine methods of access to this type of information.[573] In the earlier documentation, the national identity system would allow for cross checking between the DVLA and the UK passport service, and use of the National Insurance record and electoral register for confirming personal details. Credit reference agencies could be used to verify current and previous addresses. Individuals would no longer need to send birth/marriage certificates for official purposes because of the facility to cross reference.[574] A scheme of this kind would therefore require the establishment of information sharing gateways between relevant Government agencies and the private sector, in particular with credit reference agencies.[575]

The links to other databases to access information about applicants is part of a project that the UKPS are calling the 'Personal Identification Process' (PIP). This project was mentioned briefly in both Corporate and Business Plans 2003 - 2008[576] and 2004 – 2009.[577] Both plans indicate that the 'process' is still in the preliminary stages, but the perceived benefit is expected to be one of strengthened identity authorisation.[578] The UKPS anticipate that a change in legislation will be required to incorporate fully this information-sharing scheme.[579]

[568] Consultation Document, Section 5, 2002, paragraph 24.
[569] Consultation Document, Section 5, 2002, paragraph 25.
[570] Consultation Document, Section 5, 2002, paragraph 26.
[571] Consultation Document, Section 5, 2002, paragraph 27.
[572] Consultation Document, Section 4, 2002, paragraph 20.
[573] Consultation Document, Section 4, 2002, paragraph 21.
[574] Consultation Document, Section 4, 2002, paragraph 21.
[575] Consultation Document, Section 4, 2002, paragraph 22.
[576] 'Confirming nationality and Identity and Enabling Travel', page 20
[577] UKPS Corporate and Business Plans 2004 –2009, page 21
[578] UKPS Corporate and Business Plans 2004 –2009, page 21
[579] UKPS Corporate and Business Plans 2004 –2009, page 21

The cost of these links was estimated at £41 million;[580] factors such as sophistication, technical standards and whether systems are centralised or distributed may affect this figure.

Interviews

Should an applicant fail one or more of the checks, this would not necessarily result in their being refused an identity card. Applications could be grouped into lower and higher risk categories, with the latter category requiring additional checks.[581] The UK Passport Service is planning the use of interviews for first-time applicants, in order to verify the identity and confirm the likeness of the applicant.[582] The UKPS expects some or all of first time applicants to have to attend UKPS offices or those provided by third parties, i.e. some form of high street infrastructure, to prove identity and provide biometrics.[583] The cost of such an infrastructure will be substantial including the acquisition/maintenance of property and increased staff costs.

Collecting Biometric Information

During the processing of an application, the biometric information provided by the respective applicant would be checked against a central database. The system would indicate whether there was a 'likely' match with one or more records already in the database.[584] No system based on biometric information is 100% accurate and matches are declared on the grounds of statistical probability rather than an absolute test.

Since the system is likely to produce false positives, additional procedures will be required. In such circumstances, comparisons would be made between the applicant and the declared match.[585] Government documents do not reveal the predicted frequency with which 'matches' could occur, which would impact upon any cost analysis. There will be a significant administrative burden in dealing with these situations.

The Government argues that applicants already have 'to go somewhere' to have their photo taken for their passports or for their driving licence. This is used to counterbalance any arguments about the inconvenience and costs of the new scheme for prospective applicants. It further states in its consultation document of 2002, that: "the number of biometric recorders would be far fewer than the number of photograph booths and an operator would be required to ensure that the information was recorded correctly"'. The document also proposes a scheme whereby an applicant could record their biometric information at any time convenient to them. An example provided is on provision of biometric information: the individual could be given a reference number to link to that biometric information and presumably apply for the card at a later date. However, this may increase the number of fraudulent applications, and a casual visitor could be paid to provide their biometrics. The document asserts that any card produced

[580] Consultation Document, Section 5, 2002, paragraph 12.
[581] Consultation Document, Section 4, 2002, paragraph 23.
[582] UKPS Corporate and Business Plans 2004 –2009, page 18
[583] UKPS Corporate and Business Plans 2004 –2009, page 22
[584] Consultation Document, Section 4, 2002, paragraph 31.
[585] Consultation Document, Section 4, 2002, paragraph 32.

in this way would fail at a biometric checkpoint: "but many transactions might not make use of this facility".[586]

Enrolment rate

It is difficult to assess the rate of enrolment. Already, figures differ on the number of participants in the scheme, whether of the current British population or the projected population and visitors. The NPL/BTexact study assumed that the original population estimate was only 50 million. Based on this figure, they deduced that once the scheme has been rolled out amongst the adult population, the system will have to deal with those attaining the age of 16 and new foreign residents. The feasibility study estimates this throughput to constitute 3000 enrolments daily.[587]

Costs of building and managing the Register

The Home Office stated in the 2002 consultation document that trying to ascertain the cost of the database/register by basing it on the costs of databases used in other Government departments and projects is not a useful comparator. This is due to advancing technology and the cost of existing systems including additional services, which means that the costs are not solely based on the database. The Home Office estimated that the cost of the registry would be £30 million, although the document states that this should be treated with caution, particularly as it does not cover on-going maintenance and running costs, and there is a tendency for large IT projects to overrun on costs.[588] When the cost of links to the biographical footprint-verification organisations is included, the Home Office's central estimate for IT set up costs is therefore calculated at £71 million pounds, although the 2002 document advises that this figure should be increased by 50% to £107 million.[589]

The original estimates from the Home Office on the operating costs (yearly costs, separate from the one-off basic costs) contain interesting assumptions. The total operating and maintenance cost of the infrastructure, including links, has been estimated at 25% per annum of the set-up costs. The Home Office argues that although this may be a generous estimate, such caution is necessary due to the size and potential complexities. Over the 13-year period envisioned by the Home Office in 2003, the central estimate for these operation costs is £175 million pounds. This has been increased by a further 50% to allow for the additional risks; consequently, the final estimate is £263 million.[590]

In November 2004, the Home Office estimated the *additional* running costs for the new 'National Identity Agency' to issue ID cards to be £85 million per annum when averaged over a 10-year period, and a further £50 million per annum for the verification service, again averaged over 10 years,[591] although it did not disclose exactly to what these costs would be additional. A later Home Office estimate, released in May 2005, estimates the average running cost (at 2005/06 prices) to be the considerably higher

[586] Consultation Document, Section 4, 2002, page 111
[587] NPL/BTExact study, 2003, paragraph 13.
[588] Consultation Document, Section 5, 2002, paragraph 11.
[589] Consultation Document, Section 5, 2002, paragraph 15.
[590] Consultation Document, Section 5, 2002, paragraph 17.
[591] Home Office – Identity Cards Bill Regulatory Impact Assessment, November 2004, paragraph 19

figure of £584 million plus some "set up" costs.[592] The cost of issuing cards to foreign nationals is not included in these estimates, on the basis that this is the responsibility of the IND.[593]

The UKPS is likely to be transformed into the National Identity Agency. In turn, it will be responsible for creating the Register; the UKPS is already moving towards a person-centric database.[594] Currently, the passport office operates a passport-centric database, whereby the passport number is the key locator. The transformation towards a person-centric database is significant in terms of the ever-increasing size of the new database – files now being focused on the life of the individual as opposed to the life of the passport – which quite clearly has related cost implications. The Corporate and Business Plan for 2004 – 2009 mentions the high level of involvement of the UKPS with the Home Office ID Card Programme Board[595] and, in the light of this, many of the UKPS's corporate/business aims can be recognised as early steps towards the implementation of the National Identity Register.

This affects the funding structure of the UKPS. Its revenues were predicted to more than double from £156.8 million in 2002-2003 to £318.3 million in 2007-2008, and a surplus increase of approximately 200% to £15.1 million is anticipated[596]. However, the following year's predictions place the expected revenue for 2007-2008 at between £356million and £435 million,[597] which demonstrates the increasing costs of the application process. The Home Office clearly intends that this revenue should: "fund the infrastructure for issuing biometric passports", although this appears to cover the incorporation of only one biometric identifier, notably facial recognition.[598]

The Government foresees the simultaneous introduction of a National Identity Register Number (NIRN), which they assert will simplify access to Government services.[599] It should be noted that, according to the Regulatory Impact Assessment, this is: "not currently costed as part of the functions of the Identity Card Scheme".[600] The cost of integrating the number across Government services is therefore ignored in the Government's existing cost predictions.

Costs of Passports and ID cards

It is anticipated that the running costs of the Agency will be covered by fees charged for the issue of passports/ID cards and their maintenance, i.e. fees for replacements and the verification service. However, if this revenue is not sufficient, fees may be charged for the amendment of information, such as change of address.[601] The Government originally asserted that the cost of the passport/ID card package, that is valid for 10 years, would be £85,[602] but six months later this increased to £93.[603]

[592] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 19
[593] Home Office – Identity Cards Bill Regulatory Impact Assessment, November 2004, paragraph 19
[594] 'Confirming nationality and Identity and Enabling Travel', page 20
[595] UKPS Corporate and Business Plans 2004 –2000, page 17
[596] 'Confirming nationality and Identity and Enabling Travel', page 30
[597] UKPS Corporate and Business Plans 2004 –2009, page 34
[598] Home Office – Identity Cards Bill Regulatory Impact Assessment, November 2004, paragraph 17
[599]Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 26
[600] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 26
[601] Home Office – Identity Cards Bill Regulatory Impact Assessment, November 2004, paragraph 20/21
[602] Home Office – Identity Cards Bill Regulatory Impact Assessment, November 2004, paragraph 22

Many of these costs are to be absorbed by the passport itself. This is demonstrated by the increases in the cost per passport as predicted by the UKPS. Initially, the predicted cost of a passport in 2007-2008 was set to be £52.00, an increase from £33.00 in 2002-2003.[604] The following year's corporate and business plan estimated the cost of a passport to be between £65.28 and £77.13 in 2007-08.[605] New legislation will be required to provide a statutory basis for spending public money on setting up the scheme and charging higher fees to cover the costs of enrolment, issue and verification services.[606]

Verification

In its documentation, the Government was vague on the issue of verification. It rarely states in clear terms who will be required to verify the information provided by the system, whether the verification will be on-line or off-line, and who has access to the more detailed information such as the biometrics on the Register.

Towards On-Line Verification

There are three essential types of verification considered by the Government. The off-line verification involves the comparison of the face on the card and the human holding the card, while also ensuring that the card has not been tampered with. The second form of verification involves using smart card technology to either verify through the use of a PIN, or possibly a biometric verification involving a 1-to-1 check. The third form of verification, the on-line check, involves the verification of the card and/or information held on the card with the national identity register.

As time passed, the Government appeared more willing to rely on the real-time verification. In its 2002 consultation document, the Government contended that the most basic use of the card would be a visual check. Cards would need anti-counterfeiting measures, similar to those on banknotes, to add a further authenticity check.[607] This early approach allowed for further verification from a telephone-based authentication service with a limited access to the central register. If there were a commercial benefit for such a service, such as reducing fraud, the cost of the telephone inquiry service could be recouped by, for example, using premium-rate phone lines.[608] On-line internet access to the authentication service would also be considered.[609]

However, in later documents the card became a secondary instrument, and the Government increasingly stated its intention to rely on on-line access for verification.

The Home Office is keen to implement a system of on-line checks on the basis they: "provide an optimum combination of simplicity, reliability and auditability". However,

[603] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 22
[604] 'Confirming nationality and Identity and Enabling Travel', page 30
[605] UKPS Corporate and Business Plans 2004 –2009, page 34
[606] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 3(ii)
[607] Consultation Document, Section 4, 2002, paragraph 70.
[608] Consultation Document, Section 4, 2002, paragraph 73.
[609] Consultation Document, Section 4, 2002, paragraph 74.

the IT infrastructure needed will: "require more capacity and will need to be more resilient than the current passport IT infrastructure".[610]

Points of Verification

In order for the desired policy outcomes to be achieved, the Home Office has expanded on its ideas for the final implementation of the system in the November Regulatory Impact Assessment. Whilst these do not represent clear visions of how the system will work, assumptions can be drawn from many of the assertions made. The Home Office has divided the policy objectives into four sub-categories: illegal immigration and working, terrorism and organised crime, identity fraud and delivery of public services.

With regard to illegal immigration and illegal working, the RIA states that the verification service will be available, not just to the authorities for maintaining immigration control, but also to providers of public services and private sector organisations.[611] This could lead to the purchase and use of card readers and the use of a verification service by employers. Further, mobile fingerprint readers used by the police, and already in use by the Immigration Service, are likely to be used to conduct (random) status checks on individuals. These readers must effectively have on-line access to the database.[612]

The Home Office envisages the use of cards as proof of identity when making major financial transactions, thus card readers/on-line verification will logically be required by financial service providers and some companies. It would appear that The Home Office also envisage the use of identity cards in all transactions, as demonstrated by the assertion that terrorists will find it difficult to stay in hotels, rent accommodation, hire cars, buy mobile phones and generally carry out activities.[613] The extent to which identity cards will play a role in the performance of everyday purchases is not indicated by the Home Office, although these could range from simple visual checks to on-line comparisons of biometrics. Further, the Home Office anticipates that the 'voluntary' production of ID cards will save police time; in the light of this,[614] individuals will undoubtedly be encouraged to carry the card as a matter of routine.

Expositions of the role of the ID card in the reduction of identity fraud reiterate the same perceived use of cards in the reduction of crime, in that the verification service of either production of a card or on-line checks is anticipated for transactions. The Home Office has focused on financial service providers and Customs & Excise, but use of 'chip & PIN' by retail organisations is mentioned and it is suggested that replacement readers could be modified to read ID cards.[615] This would seem to suggest that the use of the ID card (whether checked visually or on-line) could be anticipated in most commercial transactions, regardless of size.

With regard to the delivery of public services, the Home Office stated in November 2004 that the Bill in its current form contains no automatic requirement to produce an

[610] Home Office – Identity Cards Bill Regulatory Impact Assessment, , May 2005, paragraph 18(iii)
[611] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 37
[612] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 39-43
[613] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 47
[614] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 47(iv)
[615] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 53-63

ID card for any public service, but it is likely that secondary legislation will be used to include this requirement.[616] Again, the use of the verification system and a card reader infrastructure is the guaranteed implementation format.[617]

Links and Communications to the Register

Links between databases are expected to provide extra verification that an individual is who they say they are, by ascertaining or confirming further details of an individual's biographical identity. The UKPS has already instigated the use of data sharing, with the Office of National Statistics, and reports success with this objective relating to information provision concerning births and deaths.[618] Consequently, future plans to expand upon this are being considered and the UKPS is in the process of: "forging alliances with other Government departments and private sector organisations to share database information".[619] A particular example is provided by plans for a global 'British Passport Database', allowing both the UKPS and the Foreign and Commonwealth Office to access shared data, which will hold all details of passports that have been issued overseas and provide information if there is a 'stop' on a passport.[620]

The extent and nature of these expected links is unclear, especially with regard to the degree to which the private sector will be involved. On the one hand, the Government is talking about business using authentication services to reduce fraud and illegal workers, which will simultaneously provide some income.[621] On the other hand, the Regulatory Impact Assessments state that the Bill as drafted places no requirements on business, charities or voluntary bodies to make identity checks using the system.[622]

This does not mean that such bodies will never be subject to such requirements. The RIA states that verification charges will provide a source of revenue, either through an on-line enquiry facility or (direct) on-line access to the verification system with the use of card readers.[623] Whilst the term 'organisations' may simply be intended to refer to public services, it is entirely conceivable that the commercial viability intended by this verification service encompasses private sector organisations as well. Further, it is increasingly likely that a charge will be made for employee checks, a requirement under the Immigration and Asylum Act 1996, due to the 'convenience' and accuracy of the system, and the adverse inferences that will be drawn against employers who do not use the register.[624]

To prevent the use of stolen cards, a check could involve the use of a secret password, pass-phrase or PIN when the card was issued, as proposed in the 2002 consultation document.[625] Using the call centre example, during telephone verification, the authentication service would ask a random question based on this information; the

[616]Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 68
[617] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 72
[618] 'Confirming nationality and Identity and Enabling Travel', The United Kingdom Passport Service Mission, Corporate and Business Plans 2003-2008/page 12
[619] 'Confirming nationality and Identity and Enabling Travel', page 12
[620] 'Confirming nationality and Identity and Enabling Travel', page 17
[621] Consultation Document, Section 5, 2003, paragraphs 40-48
[622] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 11/12
[623] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 23(i)/(ii)
[624] Home Office – Identity Cards Bill Regulatory Impact Assessment, May 2005, paragraph 43
[625] Consultation Document, Section 4, 2002, paragraph 75.

operator would ask the card-holder for the requested information and then pass it back to the authentication service, who would confirm whether the answer was correct. As the full pin/phrase would not be exchanged, the call centre operator would not know the full pass-phrase and this would not compromise security.[626] A similar semi-PIN was originally envisioned for on-line transactions.[627]

However, use of a PIN would enable security breaches which the use of biometric information would prevent, either through an 'online check' or an 'off-line check'. Off-line checking would involve comparison of the card-holder's characteristics compared with those stored on the card. This would mean investing in suitable scanners and card readers, and would therefore be suitable only for high value transactions where the card holder was present, unless the card holder owned their own fingerprint or iris scanner.[628]

An on-line check would involve comparison of the card holder's biometric characteristics against those held on the central register. This would require that the relevant organisation purchase a scanner, a card-reader and also on an on-line connection to the authentication service.[629] In the case of iris or fingerprint scanning, matches would be confirmed or disputed by a computer system based on statistical probability, but with respect to facial recognition, human judgement could suffice. No biometric system is foolproof and: "there is always a finite probability that the system will fail to identify a valid card-holder"'.[630] Use of a digital signature incorporated into the card was briefly considered; however this would incur added costs due the need for a more sophisticated microchip.[631]

Biometrics

The Government originally established a four point-test to decide which biometric information to include in an identity card system: cost, feasibility, acceptance of the technology in principle, and acceptance of the technology in practice.

The question of feasibility covers implementation difficulties for those living in sparsely populated areas or who are housebound, and the fact that a: "nation-wide network of devices to record biometric information would have to be installed". The considerations for acceptance of the technology in practice seem largely to rest on the level of convenience when individuals visit recording devices and that: "there might still be a risk of queuing at peak times such as on Saturday mornings".[632] The Government also recognises that issues may arise for UK passport holders living abroad, and it would be difficult for all the individuals concerned to visit a consulate in person for a biometric check.[633]

The Government decided in 2002 that the most promising types of biometric identification for consideration in the entitlement card scheme are fingerprints, iris

[626] Consultation Document, Section 4, 2002, paragraph 77
[627] Consultation Document, Section 4, 2002, paragraph 78.
[628] Consultation Document, Section 4, 2002, paragraph 81.
[629] Consultation Document, Section 4, 2002, paragraph 82.
[630] Consultation Document, Section 4, 2002, paragraph 83.
[631] Consulation Document, section 4, 2002, paragraph 84.
[632] Consultation Document, Section 4, 2002, paragraph 40.
[633] Consultation Document, Section 4, 2002, paragraph 42.

patterns and facial recognition.[634] This approach was confirmed by the NPL/BTexact study that recommended specific forms of biometrics that could be used, and outlined their challenges. The report concluded that, while biometrics could be used, the costs of using all three would outweigh the benefits. That is, the report stated that the combination would improve performance but that this: "performance improvement is unlikely to be commensurate with the increased costs, and collection of the additional biometric images might be seen as unnecessarily intrusive by the public".[635]

With regard to fingerprinting, electronic scanners require well trained staff to ensure proper use. The Government originally envisaged a far simpler scanning system than that used by the police or the immigration service, originally considering the scanning of four fingers only.[636] Additionally, the prints would not be scanned to a legal standard of proof of identity and therefore future staff would not need to be as highly trained as those working for police forces or the Immigration Service to interpret the results of any potential matches detected by the computer. The Government has subsequently admitted that it wishes to have the fingerprints used to solve crimes. As the UKPS report on biometrics found that the verification rate on fingerprinting was quite low, with only an 80% success rate,[637] this would require adequately trained staff and greater care in the fingerprinting process.

The Government has previously acknowledged the notions of criminality that some people will associate with having to provide their fingerprints. It also acknowledges that any intention to apply fingerprinting across the entire population is non-trivial. In the earlier stages of the policy, the Government referred to the difficulties involved in taking the finger prints of elderly people electronically due to the increased dryness of their skin.[638] Both of these indicate that costs will be higher, both because of refuseniks and those who are unable to comply.

For the use of an iris biometric, each iris is scanned and matched against a computer record. The Government considered the use of more sophisticated cameras which do not require the individual to focus on a fixed point, and which will be more helpful for those who are partially sighted and blind. However, the Government is well aware of the challenges to this practice, because early in the process it noted that iris scanning has only been used to date on systems holding up to a few thousand records, as opposed to the many millions required by the suggested scheme.[639] In the UKPS trials, the iris verification rate was still unacceptable for a national ID programme, and better technology is required.

Facial recognition is also a biometric option. It is noted that this source of information would be less costly to implement than iris scanning or fingerprints: "as it would not require a regional network of devices to record applicants' information" and it would require no change to the existing application process.

[634] Consultation Document, Section 4, 2002, paragraph 30.
[635] 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', paragraph 38, page 12
[636] Consultation Document, Section 4, 2002, paragraph 34.
[637] UKPS study, 2005.
[638] Consultation Document, Section 4, 2002, paragraph 35.
[639] Consultation Document, Section 4, 2002, paragraph 37.

The NPL/BTexact study was the most explicit document on the potential costs that could arise from biometric operations. The report considered the need for stringent environmental conditions; for example, lighting is important because any stray illumination sources cause the iris camera to see reflections. Second attempts at the provision of biometric information may be required:, for example, in fingerprint recognition a failure to acquire may be due to damp, dirty or dry fingers.[640]

The Government's early figures under-estimated the costs of biometrics because a scheme was envisaged where the biometrics would not be integral to the system success. The 2002 consultation document argued that the biometric system would not need to be as sophisticated as those used for policing, and the costs could be absorbed in the upgrade of related systems, for example the UK Passport Service.[641]

Based on this approach, the Home Office predicted that the cost of biometric recording equipment for fingerprints and iris scanning would be £19.5 million. This figure is derived from the purchase of 2,000 sets of fixed/mobile equipment costing £10,000 each, including the cost of any requisite accompanying PC and software. The 2002 consultation document suggested that this figure may be varied due to potential volume discounts, or the need to install more equipment if there is insufficient coverage.[642] The latter factor should be particularly emphasised as the Home Office's estimate of 2,000 sets of equipment may be too conservative. The consultation document's estimated cost of £19.5 million is also increased by 50% as this is a high risk area. This takes the cost of biometric recording equipment to £29 million.[643]

The NPL/BTexact report agrees with the Home Office estimate that 2000 sets of biometric recording equipment will be required,[644] although it is likely that this estimate is still too conservative.

Costs for some items differ substantially from the figures given in the 2002 consultation document. The study considers the cost of licensing the technology. It agrees that 2,000 sets of recording equipment at fixed locations are needed, but prices these at £5,000 per set, as against the Government costing of £10,000. Conversely, the study mentions as a separate sub-category, the need for 2,000 sets of recording equipment for 'remote enrolment' and prices these at £2,000 per set. It also separates out the cost of hardware required to supplement the recording equipment and prices this at £10 million. This still produces a lower figure in terms of the set up of the recording equipment; the report estimates this as £24 million, £5 million less than the Home Office estimated in 2003.

The Regulatory Impact Assessment has the greatest variation in costs. Both Assessments insist that the readers will only cost between £250 and £750. In the light of the responses from the UKPS trial, these costings are likely to be on the low side.

[640] 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', paragraph 65a and b, page 17.
[641] Consultation Document, Section 5, 2002, paragraph 11.
[642] Consultation Document, Section 5, 2002, paragraph 16.
[643] Consultation Document, Section 5, 2002, paragraph 16.
[644] NPL/BTExact study, 2003, paragraph 14.

Other Challenges

The Government was originally sensitive to the complexities of the proposed system and the mechanisms necessary to ensure the success of a large-scale computer system that applies to 60 million people. Such a scheme would need to cater for various groups of people who may find it difficult to participate in the scheme, for example: the housebound, those living in sparsely populated areas, homeless people or 'those of an itinerant lifestyle', mentally ill people and those fleeing abusive relationships, who may wish to live under another identity.[645] Suggestions for the above categories involve some sort of home-delivery based scheme,[646] the use of third parties[647] and flexibility towards the use of an alias.[648] Later statements of Government intent are not as clear regarding these remote facilities and exceptional cases.

Staff costs are also a factor. In 2002 the Home Office predicted that staff costs would increase across the board in UKPS, DVLA and DVLNI. Additionally, the staff costs are likely to rise due to the recording or validating of information and additional checks on Government or other databases.[649] The number of staff required is predicted to fluctuate, peaking during the six-year roll out, when the majority of the population is expected to join the scheme. Factors affecting cost include any potential teething problems, high numbers of suspected fraudulent applications or, conversely, better identification of fraudulent applications, allowing a greater proportion to proceed to the fast track.[650] The central estimate for staff costs is £62 million over 13 years and this figure remains unaltered due to expertise in administering operations of this size.[651]

The NPL/BTexact report differs from the Government on the staff cost figures. The staff cost for enrolment is estimated at £330 million. It is difficult to compare this figure with that provided by the Home Office, as the latter uses the overlap with the existing UKPS and DVLA staff and therefore includes only *additional* staff costs, which it places at £62 million over 13 years. However, the report does not indicate whether the £330 million quoted includes this overlap.

In addition to the extra staff required, essential staff training will produce a further drain on resources, particularly in efforts to improve fraud prevention and detection. The UKPS not only plans to run refresher training courses for current staff, it also plans the creation of specialist fraud and intelligence units.[652]

The Government has also proposed income-generation schemes for the card process. In 2002 it introduced the concept of charging private sector service providers for an authentication service and charging other service providers for use of the card to administer their own services.[653] This form of charge should be incorporated into a costing scheme so that the full cost to the citizen/consumer is better understood. Similarly, at the time when a rise in the price of the driver's licence and the passport

[645] Consultation Document, Section 4, 2002, paragraph 97.
[646] Consultation Document, Section 4, 2002, paragraph 99.
[647] Consultation Document, Section 4, 2002, paragraph 100.
[648] Consultation Document, Section 4, 2002, paragraph 101.
[649] Consultation Document, Section 5, 2002, paragraph 20.
[650] Consultation Document, Section 5, 2002, paragraph 21.
[651] Consultation Document, Section 5, 2002, paragraph 22.
[652] 'Confirming nationality and Identity and Enabling Travel', page 16
[653] Consultation Document, Section 5, 2002, paragraph 35.

was under consideration; although the licence is no longer associated with the system, the Government did propose raising the costs of both of these documents.

In their consultation document the Government also discussed the possibility of raising revenue from both private and public sector organisations using the authentication service to check the identity of service users,[654] and from employers or financial service providers who used the authentication service to comply with their obligations under the Asylum and Immigration Act 1996.[655] The Government has estimated that employers will need to conduct 3.6 million checks per annum on new employees; on the safe presumption that only 75% of employers will conduct checks, these amounts to 2.7 million checks per annum. If 25% of these employers needed to use a premium rate phone call, then the Government could generate revenue of £0.68 million.[656]

The NPL/BTexact study also suggests an additional area of concern for costs. The study details implementation risks that: "could impact the viability of such a groundbreaking system". These include the safety and the security of the system to maintain public reassurance and protect against misuse; an excessive number of false alarms, which will lead to slower and more costly checks; speed and ease of capture of biometric images in order to avoid bottlenecks, and finally, public knowledge which is hugely relevant to public acceptance.[657]

A significant challenge is presented by any error rate in the process and production of personal identification cards, and the creation of swift remedies for individuals where this occurs. Statistics produced by the UKPS demonstrate that despite the longevity of the passport system, an annual error rate is sill positioned at 'less than 0.25%'.[658] With an error rate of 0.24%, out of 5.35 million[659] passports issued, approximately 12,840 individuals encountered difficulties with the system. A nascent system of such a size and innovation as that of the proposed ID card scheme is likely to suffer a considerably higher error rate during its first ten years, particularly when the rising demand for passports is considered: this is now estimated at an average of 6 million per year.[660]

Ensuring the security of ID cards is an essential challenge particularly as they will be seen to represent foolproof methods of identification. The UKPS has incorporated secure delivery of all passports as of February 2004[661] through a 'specialist service provider', which adds further costs to the unit cost per passport. ID cards will also have to be delivered through such a process.

[654] Consultation Document, Section 5, 2002, paragraphs 40-42.
[655] Consultation Document, Section 5, 2002, paragraphs 43-48
[656] Consultation Document, Section 5, 2002, paragraph 45
[657] 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme', paragraph 113, page 31-32
[658] 'Confirming nationality and Identity and Enabling Travel', page 27
[659] 'Confirming nationality and Identity and Enabling Travel', page 12 (average of 5.2 – 5.5 million passports)
[660] UKPS Corporate and Business Plans 2005 – 2019, paragraph 2.4.1
[661] UKPS Corporate and Business Plans 2004 –2009, page 23

17

Cost Projections

As we have identified throughout this report, the government's scheme does not provide a stable cost environment. Experimental technology, a high security threat and uncertain public trust are factors that will create a high degree of uncertainty in any projected costing. We are therefore unable to provide any more than a spectrum of possible costs. Within this range, however, we are confident that most cost elements are addressed.

We accept the basis of the population projections contained in the indicative cost assumptions published in the "Entitlement Card and Identity Fraud" consultation paper, 2002.

At the end of the rollout period, 67.5 million people would be covered, comprising the resident population aged 16 and over, plus the number of sixteen year olds entering the scheme in the four years after the rollout along with the number of non-casual visitors to the UK from overseas. It is, however, unclear whether "non casual" visitors includes British nationals who are resident overseas.

We have assumed that the card envisioned for this system is a "sophisticated" smart card, and that – as foreshadowed in the original cost estimates –it will be re-issued twice during a ten-year period

As noted above, at this stage in the development of the government's proposals it is possible to suggest only a range of probable costs. To date the Government has been reluctant to discuss cost elements of this scheme in any detail. This is due in part to its claim that the matter of cost is commercial in confidence, and due in part to the enabling nature of the legislation. The ongoing dispute over costs is due in large part to the fact that the Government is either not certain exactly what the ID infrastructure will entail, or is unwilling to disclose these details.

The Government has not undertaken any detailed cost assessment of their identity card scheme. In response to an inquiry from Privacy International concerning HM Treasury analyses of the costs of creating and maintaining the system, the Treasury responded:

> "The Treasury did not conduct any separate analysis of the costs of creating and maintaining a national identity card, and therefore holds no documents relevant to your request."[662]

Nevertheless, enough is now know about the details of the proposal to develop cost projections with some degree of certainty. This section will explore the basis of those costs. Previous sections of this report have set out the technological environment in the UK that has created the dynamics for some of those cost elements.

In developing these cost projections we have taken into account the publication of two recent documents: the UKPS biometrics trial and the new Regulatory Impact Assessment (RIA).

The best available estimate contained in the RIA is that the combined passport and ID card will incur £584 million per year (£5.84 billion over ten years).

Government Underestimations

We suggest that the Government's current figure substantially underestimates the likely cost of the scheme. The key reasoning behind this view is as follows:

Biometric equipment. The UKPS trial, together with other research, indicates that there is likely to be significant disadvantage to disabled enrolees. As foreshadowed in our Interim Report, such disadvantage is likely to breach the Disability Discrimination Act, and the technologies and techniques used in enrolment and verification must therefore be improved to the point where no unnecessary disadvantage is created. Iris scanners that substantially engage the user will be necessary. Video or rapid sequence technology will be required to accommodate a number of eye conditions. Sophisticated ergonomic features and enhanced user interface features will be necessary to ensure that ensure that the machinery assists the user to the maximum extent. The relatively high unit cost of the equipment, as set out in our estimates, reflect the importance of ensuring that inherent discrimination is limited to the greatest possible extent. The cost of developing and deploying the appropriate technology in this regard will be far in excess of the government's estimates. For example, the RIA states that biometric card readers will cost between £250 and £750. Even the NPL figures of 2003 are higher than this, estimating £5000 per office (though no mention is made of how many readers each office would house). A more likely figure for secure and reliable non-discriminatory equipment (using high-end fingerprint and iris recognition) would be in the range of £3,000 - £4,000 per unit (for iris and fingerprint verification). We also believe that this equipment must be replaced or upgraded at least every three to four years to ensure that security is maintained.

Validity period. The RIA estimates an indicative unit cost for an ID card and passport at £93. This assumes a ten-year life for a card and a recorded biometric. However, all technical and scientific literature indicates that biometric certainty diminishes over time, and it is therefore likely that a biometric – particularly fingerprints and facial features –

[662] Letter to David Banisar, Deputy Director of Privacy International, from John Adams, Manager of CEU, HM Treasury, April 7, 2005.

will have to be re-scanned at least every five years. This cost must be taken into account. If the enrolled biometrics do not significantly mach the re-enrolled biometrics, it may be necessary to conduct another full identity check. Northrop Grumman, the operator of the national fingerprint information system (Nafis) argued that cards would need to be replaced on average every three years.[663] The question of how a card subject is accurately verified to receive a new card is unclear, but we feel that the process will necessarily be costly and time-consuming.

Enrolment. The government appears to have underestimated the cost of other elements of enrolment. The "biographical footprint checking" component of enrolment will involve considerable effort, and will encounter significant problems regarding the accuracy and integrity of historical data. This component could conservatively add another £10 - £20 to the unit cost. The envisioned use of credit reporting agencies to confirm some personal data will, in all likelihood, create significant problems relating to enrolment integrity. We calculate that a median of 60,000 person-years will be expended in registering the entire population, plus "non casual" visitors. A further median of 60,000 person years will be expended in front-office operations.

Card replacement. As we outlined elsewhere in this report, cards will have to be replaced at least twice during a ten-year period. We believe the card selected will have to embrace substantial processing power to ensure that security and functionality is fully exploited. Research and development on encrypted biometrics will be required before this generation of cards can be rolled out.

The Register. The cost of developing, building and maintaining the national register is difficult to assess at this early stage. However there are clear parallels between the proposed register and the NHS Spine. The Register will involve greater complexity and must embrace more rigorous security measures. It must also incorporate biometrics – something that we believe will be a technological challenge far greater than the government has anticipated. We have therefore costed the Register at between two and four times the contract price over ten years of the NHS Spine project.

Non-Co-operation. While the government has attempted in the legislation to address the issue of challenges to the system by "refuseniks" through the use of civil and criminal penalties, there is evidence that this population could nevertheless create a substantial additional cost burden. The administrative costs of handling this group will be substantial. It will be difficult to distinguish between intentional non-cooperation and a genuine inability to cooperate. The proposed scheme differs from benefits administration or other government benefits and services delivery in that it essentially requires user trust and cooperation. Dedicated and systematic disruption by even a tiny element of the population may create an administrative burden equivalent to the cost of managing ten or twenty times that number of people. We believe, based on results of opinion polling, that this group of dedicated non-co-operators may be quite significant, possibly as high as two per cent of the population. One such person working strategically and systematically can, quite feasibly, exhaust 200 hours of administration time through the generation of queries, appeals, access requests, database modifications and general civil disobedience.

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

Register updates. There is a requirement on individuals to notify the identity register whenever there is a change in personal circumstances. This would mean, for example, that a person would have to contact the register when changing address or name, or when disability or change of occupation may affect the recorded biometric. This requirement may result in 250 million – 1.2 billion contacts with the register over ten years (between 4 and 20 contacts per person over ten years). This additional cost must be taken into account. If human management is necessary to ensure that changes are verified, this facet will add between £700 million and £4 billion to the ten-year rollout of the scheme. This is based on a projected cost of £3 - £4 per contact with Register staff. In taking this cost into account we assume that the cost will not be directly charged to the individual, although the RIA does not rule out this possibility. In any event, it is valid to include this component in the overall costings.

Integration costs. There will be an obligation across the public sector to implement some form of ID checking using the card and the register. There appears to be general assumption that the identity scheme in such circumstances will be a stand-alone system. We do not see how this can be the case. All public sector systems using the identity scheme must be modified so that identity numbers and identity checks can be triangulated, checked and audited through the records held by each organisation. The "audit trail" feature described in the Bill can only be referenced in circumstances that are in the "public interest". Routine administrative reference and verification of the *fact* of an identity check must be integrated into existing systems. This integration will necessitate the modification of many government IT systems. This integration cost has not been factored into the government's estimates.

Other public sector costs. Based on the RIA it appears a majority of other costs must be absorbed by each department or agency. The cost of verification administration, staff training, physical facilities costs and communications costs must be incorporated into the final estimate. This cost, in the public sector at least, is unlikely to be passed on to the individual.

Private sector integration. While the Bill contains no overt requirement on industry to use the identity card system, it is clear that the current ID checking obligation on certain sectors (e.g. financial and professional services) will require a consequential involvement in the scheme. This obligation will apply equally to employers. These costs are likely to be considerable.

Choice of reliable technology. Key elements of this scheme must conform to unusually rigorous standards. The UKPS trial failed in part because the equipment selected was inappropriate to user requirements and to the dynamics of the trial. Because of the critical nature of this scheme, we believe it will be necessary to select higher-end technology. The level of system security required, as outlined elsewhere in this report, will necessitate the selection of technology that conforms to unusually high standards.

Further Challenges

We have not at this point taken into account the potential for savings arising from the implementation of the scheme other than those that may accrue from reduced identity

fraud in the benefits sector. Some of these other areas are set out in the RIA. Nor have we assumed that contracts established for this project will go over-cost more than to the extent already factored into the RIA costings. In doing so, both we and the Government are ignoring the advice from the Institute for Electrical Engineers to that cost analyses "should be based on typical outcomes of other complex projects, not on stand-alone estimates that invariably assume over-optimistic development and performance achievements."[664]

Further assessment is needed to derive an accurate figure. Our best estimate at this point, taking all these factors into account, is that the national identification scheme's implementation and running costs, together with direct associated costs and compliance, will be in the range of £10.6 billion - £19.2 billion during the implementation (operation of the first ten years) of the scheme.

	Low	**Median**	**High**
Issuing Identity Cards Over a 10-Year Period	814	1015	1216
Passports (Based on Passport Service Figures)	3936	3936	4065
Readers for Public Sector (As Specified in the Bill)	291	306	317
National Identity Register	1559	2169	2910
Managing the National Identity Register	2261	3658	5341
Staff Costs Over a 10-Year Period	1719	3368	5308
Miscellaneous	22	64	117
TOTAL	**10602**	**14516**	**19274**

Cost Projections – All figures are in £millions. See Appendix 2 for more information.

This figure does not take into account potential cost over-runs in the development of the scheme, nor does it take into account the cost of more general industry use, implementation or compliance.

[664] 'Memorandum submitted by the Institute of Electrical Engineers', submitted to the Select Committee on Home Affairs, January 2004, available at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we29.htm.

18

Design Principles and Options

The controversy, challenges and threats arising from the Government's identity proposals are largely due to the technological design itself. While 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 that will cause a significant difference in outcome for society. 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 radically shape future policy decisions, and may even determine entire courses of action. For example, the choice of which arm of the military would be responsible for the U.S. 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, given that 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.

Other sections of this report address issues raised by the international environment and public opinion. This section identifies the core differences between the scheme proposed here with those in other countries. It looks to public opinion as a guiding

principle in the design of an alternative system, developing an infrastructure that could be built on existing trust relations and local identity requirements. The audit trail is the greatest challenge in 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 goes much further 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".[665] 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 on 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.

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 …"

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 of the privacy rights of the individual, then compliance with ECHR requires these technological alternatives to be adopted.

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

Audit trails and the resulting legal questions

The Identity Cards Bill defines an "audit trail" that will be held within the National Identity Register.[666] This 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 primary importance in evaluating the design of the system and its 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.[667]

On the face of the Bill, access to the audit trail is limited to Agencies concerned with serious crime and national security. But 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.[668]

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.[669]

The Home Office envisions a "single, standard verification service, operating online to achieve full security, (with a) full audit trail of card use".[670] Consequently, the audit trail could contain an entry for each instance of online verification with the central database,

---

[666] 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.
[667] JCHR, 5th Report, January 26, 2005, para.13 http://www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/35/35.pdf.
[668] Ibid para.42.
[669] http://www.homeoffice.gov.uk/docs3/ria_251104.pdf
[670] 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 and why any checks took place.

The privacy implications were briefly explored in Commons Standing Committee:[671]

> 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[672]: ... 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

[671] Identity Cards Bill Standing Committee, Hansard, January 27, 2005, http://www.publications.parliament.uk/pa/cm200405/cmstand/b/st050127/am/50127s02.htm.
[672] 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."[673]

The Home Office has even attributed their decision to create such extensive data trails to "representations from the information commissioner".[674] 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:

---

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

[674] 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.[675] 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. Therefore, 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 by 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.

[675] *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 trail 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.

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 the following 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);
- The audit trail should 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 is 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.[676]

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

[676] 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[677] 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 lawful provided 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

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

"Federated Identity"[678] systems, at least one of which has been endorsed by the French government[679] 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, biometric information should not be 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, each public or private-sector service wishing to issue cryptographic security tokens derived from personal data in the scheme should 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 respond that they already carry around many forms of ID. There are two assumptions behind their responses:

1. Individuals possess many forms of identification.
2. An ID Card would reduce the number of cards an individual would need to carry.

There are indeed many ways for individuals to identify themselves to various public and private sector entities. The ID card as proposed by the Government could be used as a unique identifier with all of these entities. But the ID card will transform all of these. In particular, the Government's proposed ID card is poorly designed for UK citizens' daily lives. The ID card can never replace all of these forms of identification.

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 this access takes place without the

[678] 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/.

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

disclosure of a universal ID number. The forms of identification presented to these entities either show proof of entitlement, or provide service-specific account details. The advantage of the existing situation is not just that it is privacy-protecting. Rather, existing systems are purpose built and necessarily proportionate in their demands for personal information. They support 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. The student 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 personal information 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
Driving license and number	On-line usernames

Table 10 - Popular Identification Methods and Identifiers

As these examples illustrate, individuals today are represented by an abundance of identifiers that are designed to be relied on by a small number of service providers in specific contexts. An Internet Service Provider does not record customers' NHS numbers (and has no knowledge or concern whether users have been issued such an identifier, nor any means of linking to such a number). Sports club membership cards are not linked with employment 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.[680]

Local identifiers enable service providers to identify individuals within their specific transaction contexts, to create accounts for them, and to effectively deal with fraudsters.

[680] 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 given are accurate, by checking against a national registry.

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 a customer's name, birth date or birthplace but merely whether he is 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. These 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.

A constructive way forward

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 and could build on existing societal relationships, to better ensure 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 proportionate data practices.

These solutions are well known to the private sector, but are rarely sought out when governments endeavour to develop national identification systems. The reasons for government reluctance to consider these technologies are many. One is 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. Instead 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 necessary technology exists.

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 by 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 individuals 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 UK 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 is a plurality 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 on some spectrum of properties between the 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.

Embedded master identifiers can also 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 necessary as 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 by 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.

Architectural Considerations: Designing for information security and privacy

Individuals can currently gain access to government and private-sector services without disclosing a universal identifier. In a number of countries with identity cards, this practice is constitutionally essential. Citizens either present entitlements that are not inescapably linked to identifiers or they provide service providers with local identifiers that cannot readily be linked to other identifiers used by the same individuals in other activity domains.

Individuals today are represented by an abundance of local identifiers that are each relied on by only one or a few service providers. Local identifiers enable service providers to identify individuals within their own domains, to create accounts on them, and to effectively deal with fraudsters. At the same time, the segmentation of activity domains ensures that identity thieves (whether outsiders or insiders) cannot cause cross-domain damage, and that service providers and other parties have limited profiling and surveillance powers over individuals.

The UK's proposed 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 activity domains. 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 all activity domains on the basis of the universal electronic identifiers that would inescapably be disclosed whenever individuals interact with service providers.

A variation of the envisioned national ID card architecture whereby service providers would delegate the authentication of individuals to central authorities would serve to worsen these problems. These central authorities would become all-powerful in that

they would house the power to track and trace all actions of individuals across all service providers in real time. In addition, these authorities would have the power to selectively impersonate individuals wherever they go and to deny them access to services across all activity domains – all at a single press of a central button.

The currently envisioned ID card architecture for the UK also has severe implications for the autonomy and security of service providers. When the same universal electronic identifiers are relied on by a plurality 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 could cause significant 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 card as currently envisioned by government poses grave threats to the privacy of UK citizens as well as to the autonomy and security of service providers.

The source of the problem

The main problem with the envisioned ID card infrastructure is that the UK government has modelled its design after enterprise architectures for identity and access management. Enterprise architectures centrally house the capability to electronically trace and profile all participants. This gives the enterprise the power to provide and monitor access by employees (and possibly "extended" user groups who access corporate resources, such as suppliers) to their corporate resources from a central location, and to centrally shut down all their access rights in case they leave the company.

By way of example, consider the Liberty Alliance ID-FF architecture, an industry effort to standardize so-called federated identity management for the enterprise. ID-FF describes a mechanism by which a group of service providers and one or more identity providers form a circle of trust. Within such a circle, users can federate their identities at multiple service providers with a central identity provider. Users can also engage in single sign-on to access all federated local identities without needing to authenticate individually with each service provider. Liberty Alliance ID-FF leaves the creation of user account information at the service provider level, and in addition each service provider only knows each user under a unique "alias." However, the user "aliases" (also referred to by ID-FF as "pseudonyms") in Liberty Alliance ID-FF are not pseudonyms at all: they are centrally generated and doled out by the identity provider, which first and foremost acts on behalf of (and in the security interests of) the service providers.

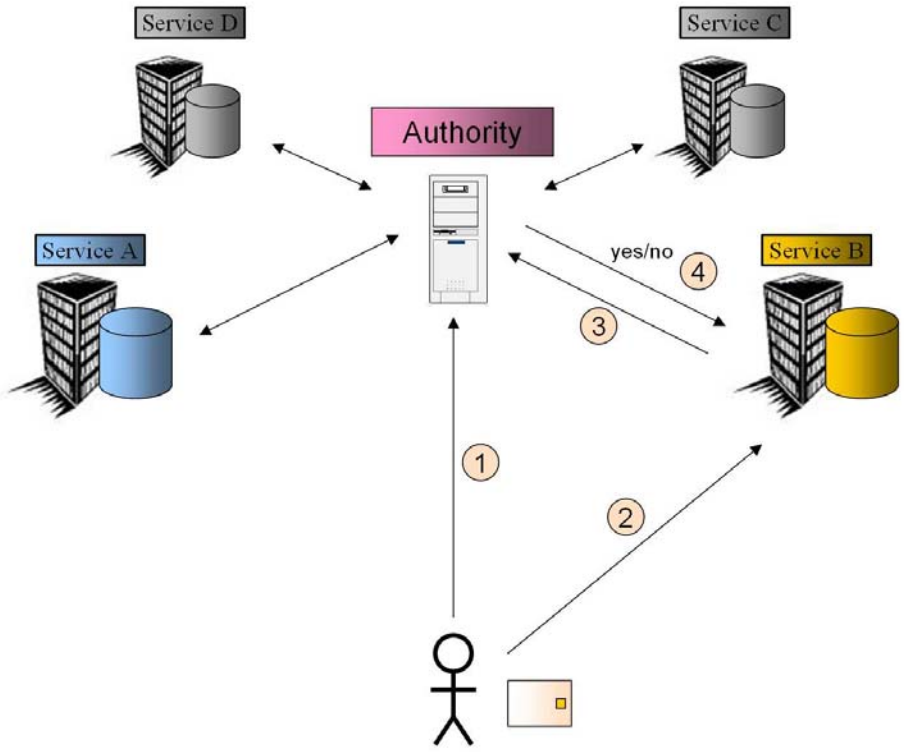


Figure 1 - Modern Enterprise Identity Architectures

About Modern Enterprise Identity Architectures.

The above figure illustrates how modern enterprise identity architectures function, such as Liberty Alliance's ID-FF. To gain access to a service, a user (e.g., a company employee) engages in the following steps.

Step 1. The user logs in to a central server ("authority"), using a password or a stronger form of authentication.

Step 2. The user requests access to a service, such as a corporate resource.

Step 3. The service electronically queries the central authority, asking it if it has authenticated the user. (This step may be accomplished by redirecting the transfer through the user, but this does not change the privacy implications of the architecture.)

Step 4. The authority verifies the user's identity and whether or not that user has just been authenticated, and proceeds by informing the service provider of its decision. Note: Step 1 may take place at this point.

While enterprise identity architectures such as the Liberty Alliance ID-FF architecture may be adequate for the corporate management of the identities of employees and suppliers who access their corporate resources, it would have highly problematic implications if used for government-to-citizen identity management. The identity provider and the service providers would have the power to electronically monitor all citizens in real time across all government services, and its insiders (as well as hackers and viruses) would have the power to commit undetectable government-wide identity theft with a single press of a central button.

Carving out independent "circles of trust" is not a solution to this problem either. The only way to break out of the individual circle-of trust "silos" that would result would be to merge them into a "super" circle by reconciling all user identifiers at the level of the identity providers, which would only exacerbate the ID-FF privacy and security problems.

More generally, panoptical identity architectures may be perfectly legitimate for a company to deal with the access rights of its own employees, but they have unacceptable privacy implications when adopted for government-to-citizen interactions. They would also eliminate the ability of government service providers to function autonomously, and would introduce enormous security risks to citizens and government alike; fraudulent insiders and successful hackers would have the ability to electronically impersonate citizens across government areas, to cause false denial-of-access to citizens on a fine-grained per-transaction basis, and to cause massive identity theft damage.

How to design a privacy-preserving 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 national ID card that eliminates any unnecessary powers. These technologies can be used as building blocks to design a national ID card system 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 in fact be much more secure than the currently envisioned national ID card, because it would minimize the scope for identity theft and insider attacks.

Individuals would be represented in their interactions with service providers by local electronic identifiers that service providers would electronically link up to legacy identity-related information (i.e., accounts) that they hold on individuals. These local electronic identifiers within themselves are untraceable and unlinkable, and so any pre-existing 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." (Different sets of the local identifiers issued to an individual might have different master identifiers embedded within them.) The embedded master identifiers would remain unconditionally hidden when individuals authenticate themselves using their local electronic identifiers, but their hidden presence can be leveraged by service providers for cross-domain security and data sharing purposes without causing privacy problems.

For example, service providers can securely share identity assertions across unlinkable activity domains, in a privacy-preserving manner and under the user's control. Invisibly embedded master identifiers of fraudulent users can be revoked in a manner that does not violate the privacy of individuals.

Figures 2, 3, and 4 below explain the basic architecture, which ensures that citizens enjoy the convenience of single sign-on with government services while the government services enjoy the benefits of secure authentication in their respective domains.

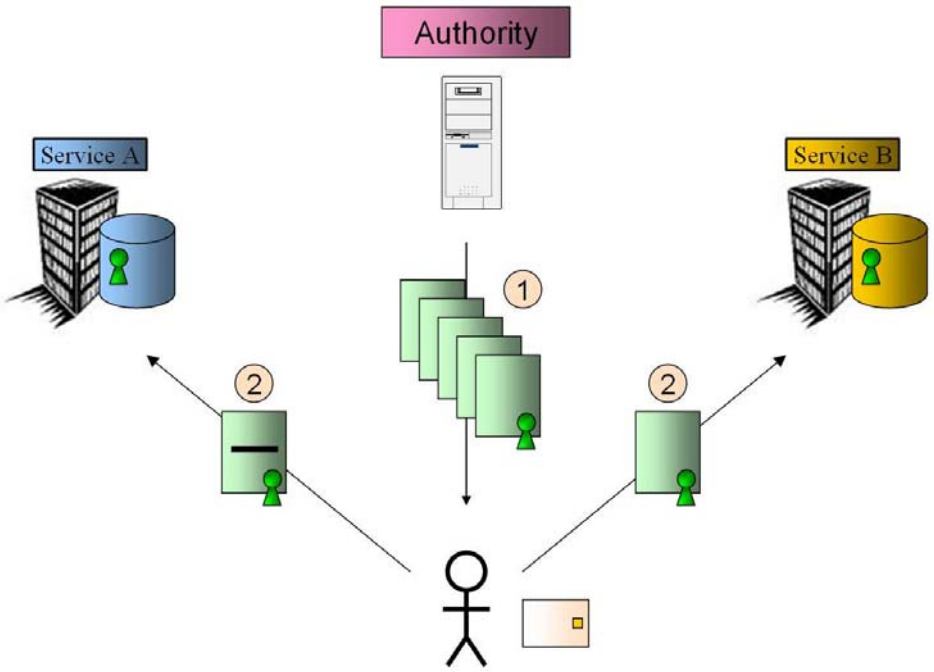


Figure 2 - Enrolment and access to Government services

Step 1: In a one-time enrolment phase, Bob's ID card retrieves several "unidirectional" identifiers from a Government Authority. The Authority endows these identifiers with relevant security properties (e.g., to prevent Bob from cloning or lending his identifiers), and cryptographically embeds a unique number into all of Bob's identifiers. The Authority may also endow Bob's unidirectional identifiers with optional attribute information (e.g., residency information) to allow service providers to make a more informed decision about Bob. However, the Authority never actually gets to see the unidirectional identifiers it issues to Bob. From a privacy perspective, each of Bob's unidirectional identifiers is the equivalent of a unique randomly self-generated number, in spite of the fact that the Authority has "certified" it.

Step 2: The first time that Bob accesses a Government Service, his ID card transmits a fresh unidirectional identifier to that Service. In doing so, Bob's card can selectively hide any irrelevant attribute information that may have been tied to the presented identifier. The invisibly embedded unique number remains unconditionally hidden. Bob's card uses a different identifier at each Service.

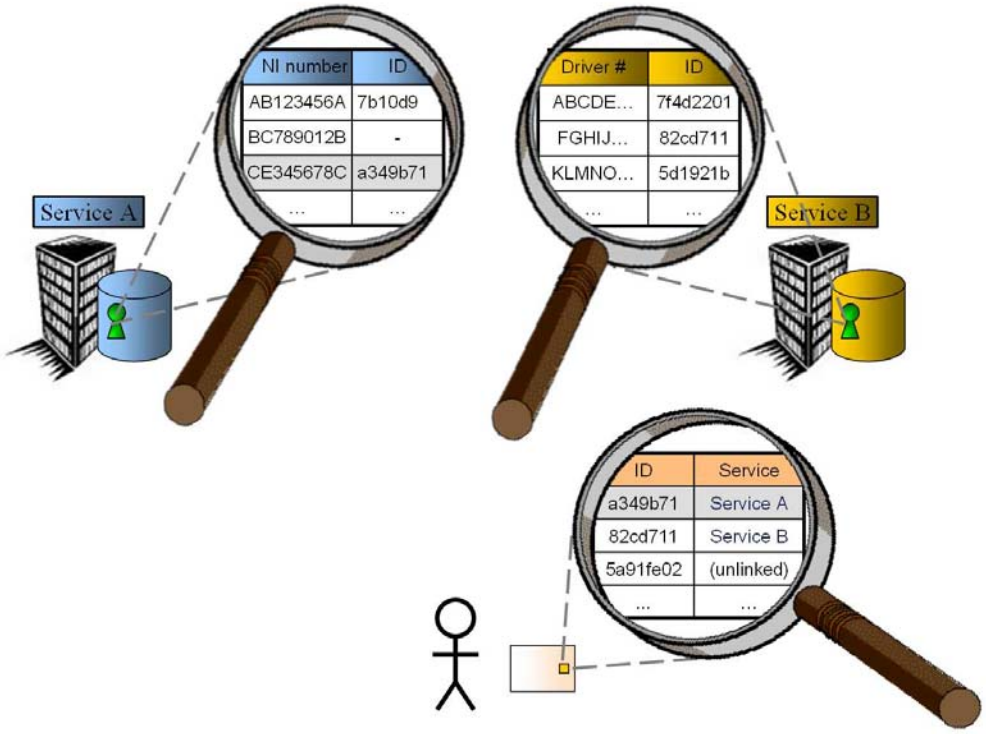


Figure 3 - Unidirectional Identifiers

Each Government Service associates the unidirectional identifier it received from Bob with the legacy account information it holds on Bob (indexed, in this example, by his national insurance number at Service A and by his driver number at Service B). Likewise, Bob's ID card keeps track of which unidirectional identifier it has hooked up to which Government Service. Because Bob's unidirectional identifiers are the equivalent of randomly self-generated numbers, they are unlinkable and untraceable within themselves. The implication: Service A, Service B, and the Authority (even when pooling all their data) do not gain any linking, tracing, and profiling powers over Bob. In effect, the Government Services have merely associated a unique random number to their pre-existing accounts on Bob. Consequently, Service A and B continue to know Bob exactly as they used to know him – in this case under his national insurance number and his driver number, respectively. However, underneath the hood (through the embedded master identifier that is invisibly present in each of Bob's unidirectional identifiers), Bob's accounts with Service A and B are now securely connected, in a privacy-preserving manner.

The privacy guarantees described in the above figures do not require users to rely on third parties. Rather the power to link and trace the activities of a user across his or her activity domains resides solely in the hands of that user. Note that the described privacy-preserving ID infrastructure does not make government services anonymous or pseudonymous where they previously were not. Instead, it avoids any degradation in privacy that citizens currently enjoy when communicating and transacting with government organizations.

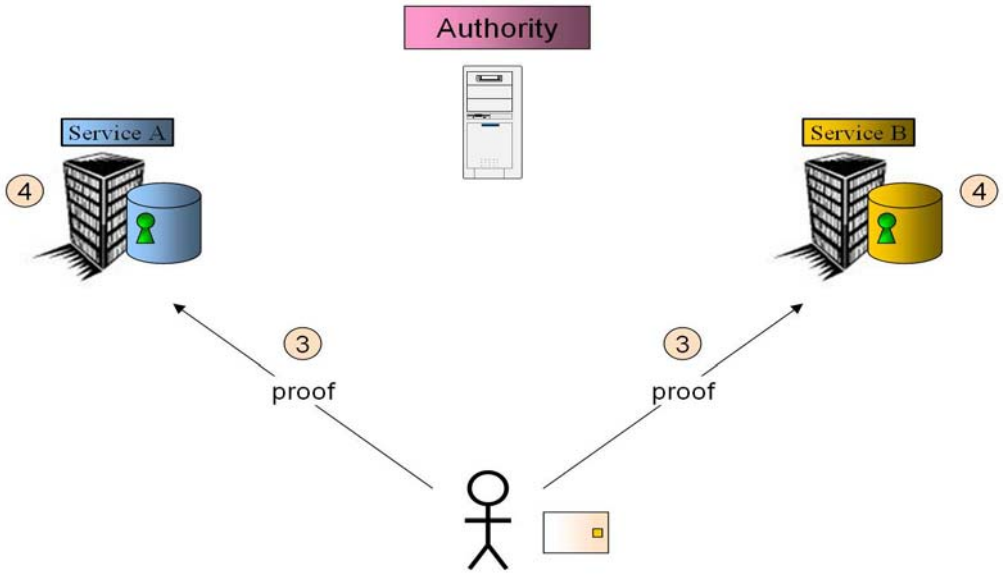


Figure 4 - Authentication

In subsequent visits to a Government Service, Bob's ID card simply authenticates to the Service with respect to the identifier that has been associated with his user account at that Service. To this end, Bob's ID card generates a cryptographic proof-of-possession of a private key that corresponds to the hooked-up identifier. This proof cannot be forged by anyone – generating a proof requires knowledge of the identifier's private key for the identifier, which never leaves Bob's ID card. The Service can locally verify Bob's authenticity by cryptographically verifying the submitted proof; there is no need to consult any other party in order to verify Bob's authenticity. In sum, Bob enjoys the convenience of single sign-on at the various Government Services, while each of the Government Services can securely authenticate Bob within its own domain.

The figures below illustrate three optional services that may be built on top of this basic privacy-preserving ID card architecture without degrading the security, privacy, and autonomy of citizens and government service providers:

- The first shows how the government could centrally collect non-repudiable audit trails that are not privacy-invasive.
- The second shows how government services could securely share account information they hold on a citizen, even though they do not know that citizen under a common identifier.
- The third shows how a group of designated government services could revoke access to a citizen who commits abuse at any one service in the group, even though they do not know that citizen under a common identifier.

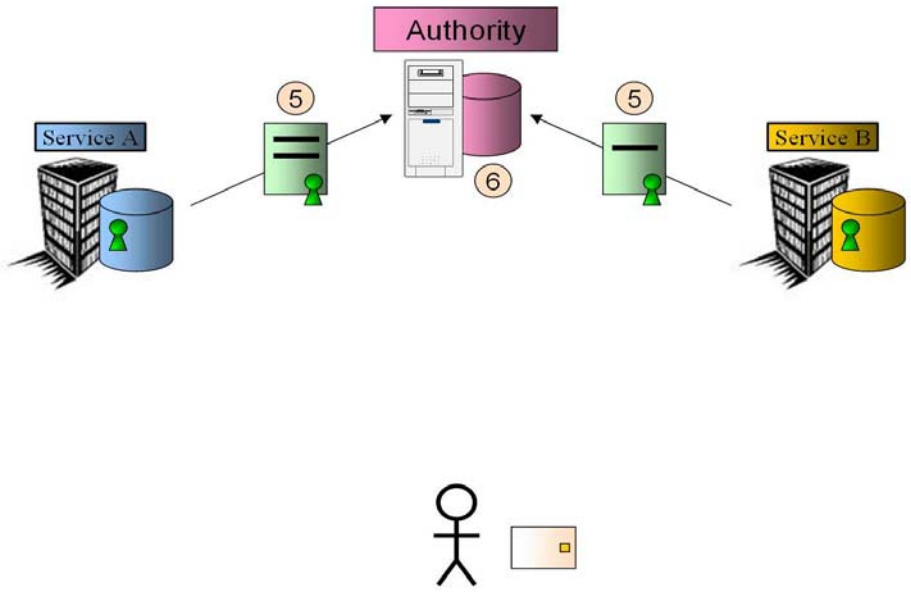


Figure 5 - Non-repudiable audit trails

This figure shows how, on top of the basic system outlined in the above figures, the government could centrally collect non-repudiable audit trails that are not privacy-invasive.

Step 5: Government Services A and B can forward non-repudiable digital audit trails to the central Authority (or any other auditing body); they can capture these whenever Bob interacts with them using his various local unidirectional identifiers. The Government Services can optionally censor the audit data prior to forwarding it, so as to protect Bob's privacy interests or their own privacy and autonomy interests vis-à-vis auditors.

Step 6: The Authority can keep the audit trails and verify the validity of transactions. In case of a dispute, censored data can be uncensored with the help of the appropriate Government Services. The Authority cannot trace and link the actions of Bob across Government Services on the basis of the non-repudiable audit trails, unless Bob has chosen to specifically enable this. (Bob can decide on a per-transaction basis.). However, as we will see below, the invisible presence of the embedded master identifier in the audit trails can be leveraged for cross-domain security purposes.

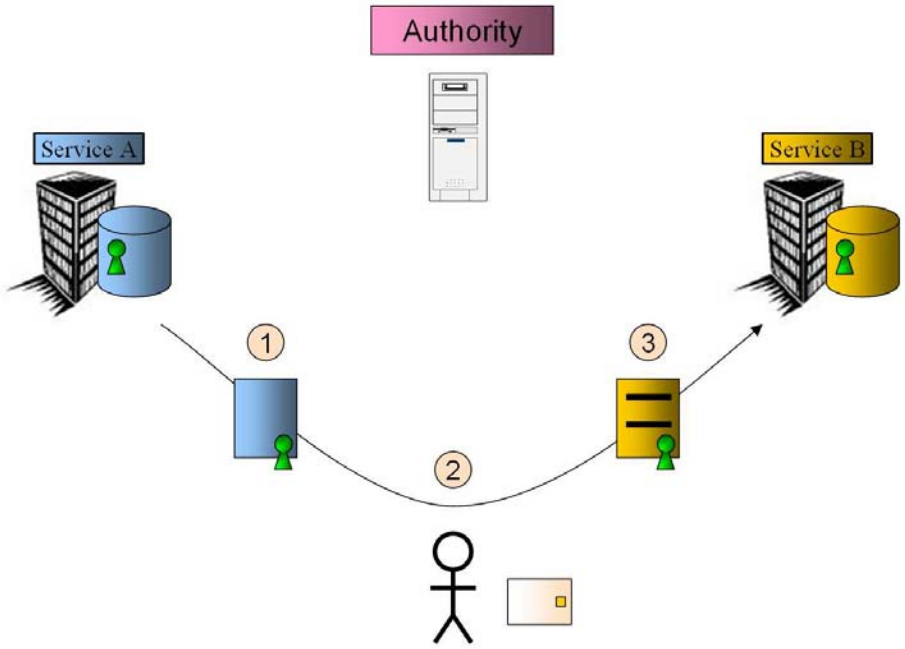


Figure 6 - Secure sharing of account data amongst services

This figure shows how, on top of the basic system outlined in Figures 2, 3, and 4, government services could securely share account data about Bob, even though they do not know him under the same identifier.

Step 1: Service A makes an "assertion" about Bob based on the account information it has on Bob, and sends the assertion in digitally protected form to Bob (or a representative that Bob may designate on a case-by-case basis). An assertion is either account information or a statement related to it; for example, Service A may make an assertion regarding Bob's residency.

Step 2: Bob's ID card sanitizes the protected assertion by "randomizing" any information that would otherwise lead to an increase in linking and profiling powers by Service A and B over him.

Step 3: Bob's card selectively discloses to Service B the minimal assertion information needed by Service B. Bob can even forward merely a property about the asserted information. For example, if Service A has asserted Bob's city of residence and street name, Bob could disclose to Service B only the fact that his city is in a certain region of the country, without revealing the city name. Service B can verify on its own the origin of the data (Service A), its integrity (Bob did not modify it), and the fact that it relates to Bob -- even though Service A and Service B do not know Bob under the same identifier. The fact that the transferred assertion information truly pertains to Bob and has not been transferred by Bob to another user can be verified by leveraging the presence of the embedded master identifier that is invisibly present in the identifiers that have been hooked up to Bob's accounts at Service A and B.

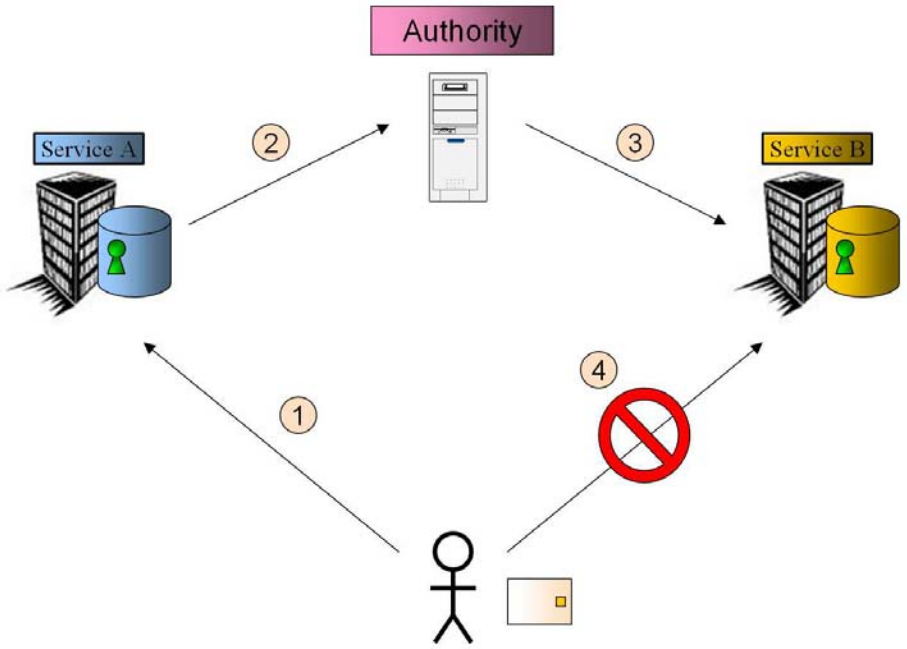


Figure 7 - Revocation

This figure shows how, on top of the basic system outlined above, Government Service B could revoke access to Bob in case Bob commits a fraud Service A, even though they cannot correlate the identities they manage in their own domains.

Step 1: Suppose Bob commits a fraud at Service A, and it is legitimately desirable for the government to be able to deny Bob access to Service B.

Step 2: Service A informs the Authority about the fraud, and provides some revocation information associated with the unidirectional identifier that Bob uses at Service A.

Step 3: The Authority broadcasts this revocation information to Service B and any other appropriate service for which cross-domain blacklisting has explicitly been enabled.

S**tep 4:** When Bob tries to access Service B, he can be denied access, even though he is known only under different unlinkable uni-directional identifier at that service. Again, this is accomplished by leveraging the master identifier that is invisibly present in Bob's unidirectional identifiers at the Service A and B.

The optional revocation feature described in the above figure does not impinge on Bob's privacy, for two reasons.

Firstly, in order to this revocation feature to work, Bob's unidirectional identifiers at Service A and B must have been issued by the Authority in a special manner with the cooperation of Bob's card at issuing time. Bob's card knows which of the identifiers it has been issued have built-in revocation capability, and could in fact refuse to cooperate in the creation of revocable identifiers. In practice, Bob's card could be issued a mix of revocable and non-revocable unidirectional identifiers. For services that have no lawful reason to be able to revoke Bob's access across their respective domains, Bob's card would hook up unidirectional identifiers that do not possess the described revocation feature. For instance, it would be unreasonable for Bob's utility providers to be able to

deny access to him if he is late in paying his subscription fees at the local library. In special cases, however, conceivably there may be a lawful requirement that access can be denied at a group of service providers (but not outside of this designated group) to users who abuse their access rights at any one of them. For these particular services, Bob's card could agree to enable revocable unidirectional identifiers. The important point to note is that the choice is up to Bob, who may refuse to hook up a revocable identifier if he deems the request to be unlawful or unreasonable.

Secondly, in order for Service B in the above figure to be able to deny access to Bob in case Bob has abused his access rights at Service A, Service B must ask each user who wants to gain access to its service to submit a cryptographic proof that the invisibly embedded number in their local identifier with Service B is different from the revoked number that Service A has passed on to Service B. If the embedded number of an access requestor is equal to the blacklisted number, no valid cryptographic proof can be created. The important points to note are: (a) entries on the revocation list are meaningless random numbers to everyone, (b) the list of revoked numbers must be sent to each user who is requesting access, so each user sees that they are asked to prove they are not on the list, and (c) proving that one is not on the revocation list does not invade one's privacy.

Conclusion

It is inappropriate for government to model the design of a national ID card infrastructure for citizens after architectures for enterprise identity management that centrally house the capability to electronically trace and profile all participants. In the context of a national ID card infrastructure, the privacy implications for citizens of such panoptical identity architectures would be unprecedented. Panoptical identity management architectures would also eliminate the ability of government and private sector service providers to function autonomously, requiring a transformation of their own systems for integration purposes. It would introduce enormous security risks to citizens, companies and government alike, as fraudulent insiders and successful hackers would have the ability to electronically impersonate citizens across organisations, to cause false denial-of-access to citizens on a fine-grained per-transaction basis, and to cause massive identity theft damage.

Using modern authentication technologies that have been designed to preserve privacy, it is entirely feasible to build a national ID card infrastructure that simultaneously addresses the legitimate security and data sharing needs of government and the legitimate privacy needs and identity theft concerns of citizens. This approach is not only much better for the citizen, but also for government itself.

In the context of a national ID card infrastructure, security and privacy are not opposites but mutually reinforcing, assuming proper privacy-preserving technologies are deployed. In this context, privacy is essentially the same as security against insiders. In order to move forward constructively with a national ID card, it is important for government to adopt technologies that provide multi-party security while preserving privacy.

Note 1: Microsoft's take on digital identity

Privacy and security experts are not alone in critiquing the use of enterprise identity management architectures outside of enterprise-to-employee contexts. Big companies are increasingly finding it problematic.

One prominent example of this is Microsoft. Mid 2004, Microsoft publicly acknowledged that its original Passport strategy for distributed digital identity for individuals online has been a complete failure outside of the narrow context of access to specific Microsoft services. Other service providers did not appreciate the loss of their autonomy, and individuals were highly concerned about the privacy and identity theft risks of Passport.

Following this debacle, Microsoft completely revised its strategy for distributed identity management, taking instead a user-centric approach. In a recent white paper, Microsoft discusses what it believes are fundamental requirements that must be met by any distributed identity management infrastructure that involves individuals. Specifically, the white paper discusses seven "laws of identity" that "explain the successes and failures of digital identity systems." It states that:

> "… The system must be designed to put the user in control—of what digital identities are used, and what information is released. … Law of Minimal Disclosure: The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution. … The concept of "least identifying information" should be taken as meaning not only the fewest number of claims, but the information least likely to identify a given individual across multiple contexts. … Law of Directed Identity: A universal identity system must support both "omni-directional" identifiers for use by public entities and "***unidirectional***" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles. … A unidirectional identity relation with a different site would involve fabricating ***a completely unrelated identifier***. Because of this, there is ***no correlation handle*** emitted that can be shared between sites to assemble profile activities and preferences into super-dossiers. … Public key certificates have the same problem when used to identify individuals in contexts where privacy is an issue. It may be more than coincidental that certificates have so far been widely used when in conformance with this law (i.e., in identifying public Web sites) and generally ignored when it comes to identifying private individuals. …"[681]

Note 2: A look at the French e-government initiative

In 2003, the ministry in charge of e-government in France published a four-year strategic plan[682] (PSAE) for 2004-2007 for e-government services to citizens, the

[681] Available at http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/lawsofidentity.asp

[682] Available at http://www.adae.gouv.fr/IMG/pdf/Le_plan_strategique-GB.pdf.

private sector, and the public sector. The strategic plan lays out several good design principles with regard to how to build an identity management infrastructure for e-government:

- Page 12: "… do not authorise uncontrolled generalised exchanges between departments."
- Page 13: "… grant citizens more transparency in the monitoring of their administrative papers and better control of their personal details … enable citizens and professionals to have tools and services which will enable them to exercise their rights more simply and completely. … Data storage will remain decentralised within each government department. Centralised storage … will only be retained for each service where other possibilities cannot be realistically considered."
- Page 14: "One of the questions which is causing the most serious doubts regarding the possible undermining of privacy relates to the uniqueness or multiplicity of means of identifying the citizens to the government authorities. … The CNIL has ruled against [the use of a single identifier] ("to each sphere its identifier") … The Government … wishes to retain sectoral identifiers."
- Page 15: "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."

This is certainly a significant step forward. However, the PSAE report goes on erroneously to refer to Liberty Alliance ID-FF as an architecture that meets it requirement on page 15, without realizing that the "identity federator" in ID-FF does have the ability to make the link between different citizen identifiers.

19

An Alternative Blueprint for a National Identification System

This report has established a number of shortcomings and deficiencies in the government's identification proposals. These include cost, complexity and probable failure to attract consumer trust. In reaching those conclusions we recognise the importance of constructing an alternative model. In this section of the report we set out our vision for a more cost effective, secure, reliable and trusted identity structure that meets key objectives of the current Bill.

In doing so we have adopted the following assumptions:

- No national identification system is totally secure, nor can any system ever be immune to the risk of accepting false or multiple identities. Any such claim would not only be demonstrably false, but it would lead to substantial and sustained attacks. Biometrics can be spoofed, registration data falsified, corruption exploited and social networks manipulated. At both a human and a technological level, a fixation on achieving perfect identification across the entire population is misguided and counter-productive. Such emphasis is disproportionate and will lead to substantial problems relating to cost, security and trust.

- The choice of any national identification system should involve careful and sensitive consideration of key aspects of cost, security, dependability and functionality. This exercise is not necessarily a Zero Sum equation where the value of one element is traded off against the value of other elements. The aim of a genuine evolution of thinking is to achieve high scores on all key elements of the scheme. Only a spirit of openness makes it possible for this outcome to be achieved.

- Public trust is the key to a successful national identification scheme. Public trust can only be secured if issues of cost effectiveness, dependability, security, legal rights and utility are addressed, and are seen to be addressed. We believe it is possible to achieve these goals while also ensuring a system that offers reliable means of achieving the government's stated objectives.

- A genuinely cooperative approach to finding a national identity solution must involve consultation based on principles as well as objectives. We believe the government's model has failed because it has evolved exclusively through the

pursuit of objectives. While this may create an identity system that suits key stakeholders involved in specific goals, the approach imperils other essential aspects such as public trust.

We have identified a set of principles that should guide the design and execution of a national identity scheme:

An identity system must be proportionate. Aspects such as complexity, cost, legal compulsion, functionality, information storage and access to personal data must be genuinely proportionate to the stated goals of the identification system.

An identity system should be inspired by clear and specific goals. Successful identity systems embrace clear objectives that facilitate responsive, relevant and reliable development of the technology, and which limit the risk of exclusion and abuse.

Identification systems must be transparent. Public trust is maximised when details of the development and operation of an identification system are available to the users. Other than the identifier and card number, no information should be hidden.

Identity disclosure should be required only when necessary. An obligation to disclose identity should not be imposed unless the disclosure is essential to a particular transaction, duty or relationship. Over-use of an ID system will lead to the increased threat of misuse and will erode public trust.

An identity system should serve the individual. Public trust will not be achieved if an identity system is seen as a tool exclusively for the benefit of authority. A system should be designed to create substantial economic, lifestyle and security benefits for all individuals in their day-to-day life.

A national identity system should be more than just a card. Identity systems must exploit secure and private methods of taking advantage of electronic delivery of benefits and services.

Personal information should be controlled by the individual. Any biometrics and personal data associated with an identification system should remain to the greatest possible extent under the control of the individual to whom it relates. This principle establishes trust, maximises the integrity and accuracy of data and improves personal security.

Empathetic and responsive registration is essential for trust. Where government is required to assess and decide eligibility for an ID credential, the registration process should, to the greatest possible extent, be localised and cooperative.

Revocation is crucial to the control of identity theft and to the personal security of individuals. Technology should be employed to ensure that a biometric or an identity credential that has been stolen or compromised can be revoked.

Identity numbers should be invisible and restricted. Any unique code or number assigned to an individual must be cryptographically protected and invisibly embedded

within the identity system. This feature will protect against the risk of identity theft and will limit "function creep" through extended use of the number.

Capability for multiple authenticated electronic identities. An identity system should allow individuals to create secure electronic identity credentials that do not disclose personally identifiable information for use within particular social or economic domains. The use of these different credentials ensures that a "master" identifier does not become universally employed. Each sectoral credential is authenticated by the master identifier assigned to each individual. The use of these identifiers and their control by individuals is the basis for safe and secure use of federated identity systems.

Minimal reliance on a central registry of associated data. Wherever possible, in the interests of security and trust, large centralised registries of personal data should be avoided.

Permit secure and private backup of associated data. An identity system should incorporate a means of allowing individuals to securely and routinely back up data stored on their card. This facility will maximise use of the identity credentials.

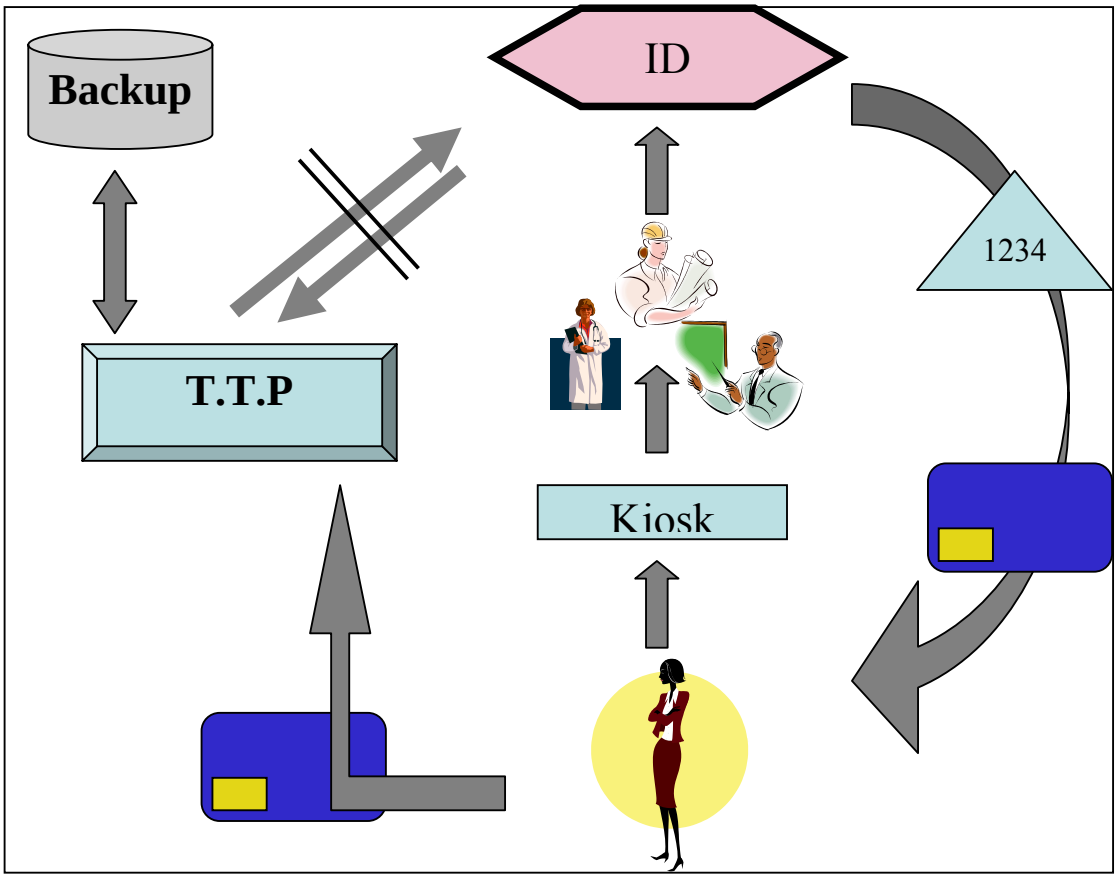


Figure 9 – LSE Alternative Model.

The LSE's ID model embraces these principles, and has a number of key features:

- The database controlled by central government contains the minimum amount of information necessary to authenticate cards and to store unique ID codes. This reduces the security and privacy threats to a reasonable level. The potential for hostile attacks and mass identity theft is substantially reduced.

- Personal information remains under the control of the individual. This facilitates the use of the card and the related master identifier for a variety of e-government and e-commerce functions.

- In the LSE model, the government establishes a network of Trusted Third Parties (banks, police stations, court houses, solicitors) that are authorised to maintain secure backups of the information contained on the card.

Summary of stages

The operation of the system can be summarised as follows.

1. To obtain the card, applicants visit a job centre, post office or other authorised facility. There they enter an electronic kiosk that takes a digital photograph, accepts basic identifying data, and embeds these into the coded application form that is dispensed at the point of contact. A temporary electronic file is created containing this data.

2. The applicant secures the endorsement of two or three people in a position of trust. These people have already been accredited and own an identity card. Once endorsed by the referees, the form is handed in at a post office or other facility.

3. The form is sent for processing. Processing of the form is largely automated. Random checks on some references will in time be conducted online or via email.

4. When the card is ready, the holder takes it to a "trusted third party" - a bank or post office for example – which is local to the applicant. The card is then connected to the Government's temporary file. If the codes match, the card is validated and all data is deleted from the government file apart from the name, code and card number. A copy of the data on the card is stored securely at the TTP.

5. The mater identifier can be used as a means of establishing a number of assured sectoral (or "spin-off") identities that can be used in numerous domains. This "private credential" facility allows the development of such innovations as federated identity management.

The scheme in detail

Identity vetting and registration.

All identity registration depends on one or more of three common processes (a) personal interview, (b) production of primary documents, (c) endorsement of applicant by referees.

In the government model, vetting (authentication) would require all three elements. Additionally, it is proposed to register an applicant's biometrics and to undertake "biographical footprint checking" to inquire more thoroughly into life history and activities.

We believe this proposal should be replaced with a less costly and less intrusive approach. The current passport application procedure, while vulnerable to some current risks, establishes the basis of an alternative model.

We propose abandoning mandatory personal interviews and replacing these with a more informal and flexible process. Personal interviews can still be conducted on request but we believe most people would prefer a more localised procedure. A substantial part of the procedure is automated, with scope for manual checking and auditing.

The application procedure – Stage One.

The applicant first visits a post office or government facility such as a Job Centre or local government office, where electronic kiosks have been installed. One of the functions of these kiosks is to dispense tamper resistant application forms. The kiosks are designed to permit a second person to be present to assist the applicant when needed.

When activated by the applicant, the kiosk displays a short video explaining the application procedure. This video can be repeated at any time during the process. Visual and audio prompts support the procedure throughout, and the applicants are asked at each stage whether they are happy to proceed.

Through a keyboard, applicants then supply the kiosk with their name and National Insurance number (NINO). The NINO is checked online to verify the applicant's name, though at this stage the success of the application does not depend on a match. The applicant is notified if a match to the NINO is not found, but no other action is taken.

Note. *We do not see the NINO as a reliable identifier by itself. Its use in this situation does however have the dual benefit of allowing a triangulation for security, with the added benefit of providing a means of eventually cleaning the NINO database.*

The applicant can submit the paper form without the NINO, but must supply additional data so the number can be manually found. This circumstance will be dealt with on a case-by-case basis at the processing stage. If a match still cannot be made, or if the applicant has no NINO, a personal interview may be necessary.

The kiosk then takes a digital photo of the applicant and embeds this onto a coded paper form. The final printed form will thus contain the photograph, name and unique reference number for the application.

Finally, applicants are asked to provide a simple biometric of choice, such as a single fingerprint, for local verification against the card that is to be issued (not for the current purpose of mass matching one-to-many against the entire population). A PIN can also be requested for additional security. Total time for the procedure in the kiosk will vary from 5 to 15 minutes.

The form is immediately printed and dispensed to the applicant, and the data is simultaneously uploaded as a secure temporary file. This temporary file is inactive, and at this stage is not scrutinised either electronically or by a human. Another form can be obtained by again visiting the kiosk and by repeating the procedure.

The form will have a number of pages, each of which contains the basic data.

Note. *Consideration was given to making the application an online process. The option was viewed as unworkable because referees are often contacted in an informal setting.*

The application procedure – Stage Two.

Once in possession of the form, the applicant secures endorsement on it from a "trusted personal network" of either two or three referees of good standing. The current passport application guidelines suggest an extremely wide spectrum of people who would be considered suitable as referees. These include accountants, bank/building society officials, chemists, chiropodists, local or county councillors, civil servants (permanent), dentists, engineers (with professional qualifications), fire service officials, funeral directors, insurance agents (full time) of a recognised company, journalists, justices of the peace, local government officers, minister of a recognised religion, nurse (SRN and SEN), opticians, paramedics (state registered), police officers, post office officials, social workers, solicitors, surveyors, teachers, lecturers, trade union officer and qualified travel agents. Almost two million people in Britain belong to one or more of these categories.

It should be noted that for this referee based system to function securely, the identity scheme must be built in two stages. The first concentrates on attracting identity credentialing from amongst the referee groups. This means, in practice, asking professional organisations, government agencies, the uniformed branches and other organisations to encourage their members and staff to register early for an identity card. The second stage commences once this first group are to a large extent enrolled in the system. This will be the key rollout of the scheme throughout the community. This model operates effectively in Sweden (see section on international environment and obligations).

Each page of the form has a section for a single referee. This ensures that a referee cannot see who else has vouched for the applicant unless the applicant wishes to disclose this information.

The current passport requirement is a single referee who has known the applicant for two years. It is proposed to set the new standard at two years for one referee, and one year for the other referee(s).

Note. *It should be kept in mind that if any applicant is unable to secure these referees, or has difficulty dealing with the process, the option of a personal interview would be available. However it is expected that many people in this situation will have a person who will help them through the process without the need to be interviewed.*

As an additional security measure, the applicant's writes the NINO on the form. The applicant then delivers the completed form to a kiosk centre, where it is forwarded through internal mail for processing.

The application procedure – Stage Three.

From the perspective of government, the approval stage of this model is the most labour intensive element of the application procedure, though much less labour intense in most cases than the current proposals.

The paper form is manually checked. Its number is matched with the temporary file number, and the digital photo on each is then compared. This is to ensure that the document was not spoofed or the photo altered during the endorsement phase. The NINO recorded on the temporary file is also compared with the NINO on the form.

Note. *It is possible to automate this process, though this may be difficult if the form has been damaged. Automation is perhaps more achievable if the forms are scanned electronically at point of receipt. Key details on the temporary file should exactly match the completed form.*

Assuming that all data matches correctly, the referees must be verified. This would be done randomly and the process could again be automated. We believe that in time this element of the checking can also be largely automated using a secure online facility that can be used by referees.

Setting up the registration.

Once registration has been completed (following approval at stage 1), a unique identifier code (master identifier) would be generated. This code, equivalent in some basic respects to a unique national identification number, is both invisible and cryptographically protected.

This code is then placed onto a card. The government keeps a temporary record of the application information together with any supporting information, and then places this data, encrypted, onto the card. At this stage the identifier is dormant and so cannot be used until a final stage has been completed.

Distributed backup.

Once in receipt of the card, the newly validated citizen at leisure then attends an authorised Trusted Third Party (TTP) of choice (such as a bank, solicitor, local

government office, court or police station). Each TTP is equipped with card reading machinery, secure data storage and a secure means of communicating with the centrally held data. The newly issued card is locally verified by a PIN and the biometric to authenticate the user. The TTP then communicates securely with the government's records for confirmation that the card is still valid.

The TTP downloads all remaining data relating to the applicant and places these on the card.

Once downloaded, all but the essential data held by government is removed. Essential data is possibly no more than the unique code, card number (which is invisible) and possibly the name of the cardholder. At this point the identifier becomes "active". The TTP keeps a secure backup of the data on the card, along with any certificates and biometrics.

Note. *This process can be conducted privately through a privacy platform without the need for a TTP. The crucial element in this stage is that the data is securely backed up so the registration process does not have to be repeated if the card is lost.*

The individual now possesses a card, a unique identifier and a secure backup that can be updated at will.

How this scheme will benefit UK businesses

This scheme has certain significant commercial advantages over the Government's proposals. The most important of these advantages is the ability for the individual to voluntarily add further information, certificates or identifiers to their card. For example, when visiting their bank to register a TTP, the individual could also receive an identifier from the bank that authenticates them as a legitimate account holder. This identifier could then be used for online banking, ATM transactions etc., and effectively replace their existing bank cards. Other identifiers could be added in a similar way at the request of the cardholder.

Key to this feature is the fact that the TTP will have the opportunity to authenticate the individual during their registration, and can therefore trust that they are the legitimate card holder; the issue of liability is thereby removed, since the TTP has confidence that it has placed the correct identifier on the card. In the Government's proposed scheme, this feature is unavailable, since liability for any fraudulent use of the identity card must rest with the Government.

By reducing the overall system cost, and incorporating features that will deliver potential benefits to business, we anticipate that a greater proportion of the overall cost will be voluntarily met by those organisations that stand to benefit from their participation, and hence the cost that is passed onto the taxpayer may be significantly lower than that proposed in the Government's scheme.

Cost

The government's proposals will involve approximately 60,000 person-years for personal interviews, document handling, checking procedures and management for registration of the entire population.

Using automated techniques and streamlined administration, the alternative system would involve perhaps one eighth of this workload. The kiosks and TTP backups will partially erode these savings, but these facilities will allow a citizen driven interface with the system, thus reducing the requirement for ongoing administrative, data input and support staff.

The absence of personal data held by the government will eliminate the need for a legal requirement on individuals to constantly update their file held in a central register. This element alone will produce a saving of between £1 billion and £3 billion over the rollout period. The automated registration process will save at least as much again.

The technologies discussed in this proposal are mostly available as 'off-the-shelf' software, hardware, and identification standards. 'Federated Identity' schemes such as this are in widespread commercial use, and we anticipate that they can be cost-effectively scaled to cover the entire UK population. In the interest of independence we have not published the alignment of such schemes with our proposed method, but we encourage providers of these mechanisms to describe how their technologies will fulfil the requirements of our proposal.

A comprehensive costing of the alternative model will be produced later in 2005, though it is anticipated that the scheme will involve costs that are substantially less than those imposed by the current model.

Appendix 1: 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 first piece of legislation introduced in November 2004, and the subsequent legislation introduced in May 2005.

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.

Table 11 - Comparison with HAC Report Findings.

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 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)	Conditionally supported. While proportionality is a key consideration in the development of the 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 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)	Conditionally supported. While a successful outcome will depend on a package of measures, risk assessment has not been undertaken to assess 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 ease with which terrorists can operate. (Paragraph 94)	Not supported by research. This reasoning appears to have little foundation in evidence. Research should be undertaken before reaching conclusions on these questions.
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 of the design of the system. (Paragraph 144)	Supported by research.
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 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)	Not supported by research. This requirement would create a range of additional security and 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 databases should be coherent and consistent. (Paragraph 186)	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.
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 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)	Supported by research.
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 Assessment with the Bill. (Paragraph 213)	Supported by research.
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 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)	Supported by research.
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 of function creep in which the state uses the register to identify individuals without amendment by Parliament. (Paragraph 233)	Supported by research.
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 driving licence. This offence should be reviewed in the light of the proposed legislation on identity cards. (Paragraph 254)	Supported by research.
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 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)	Conditionally supported. See Appendix on audit trails.
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 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)	Supported by research.

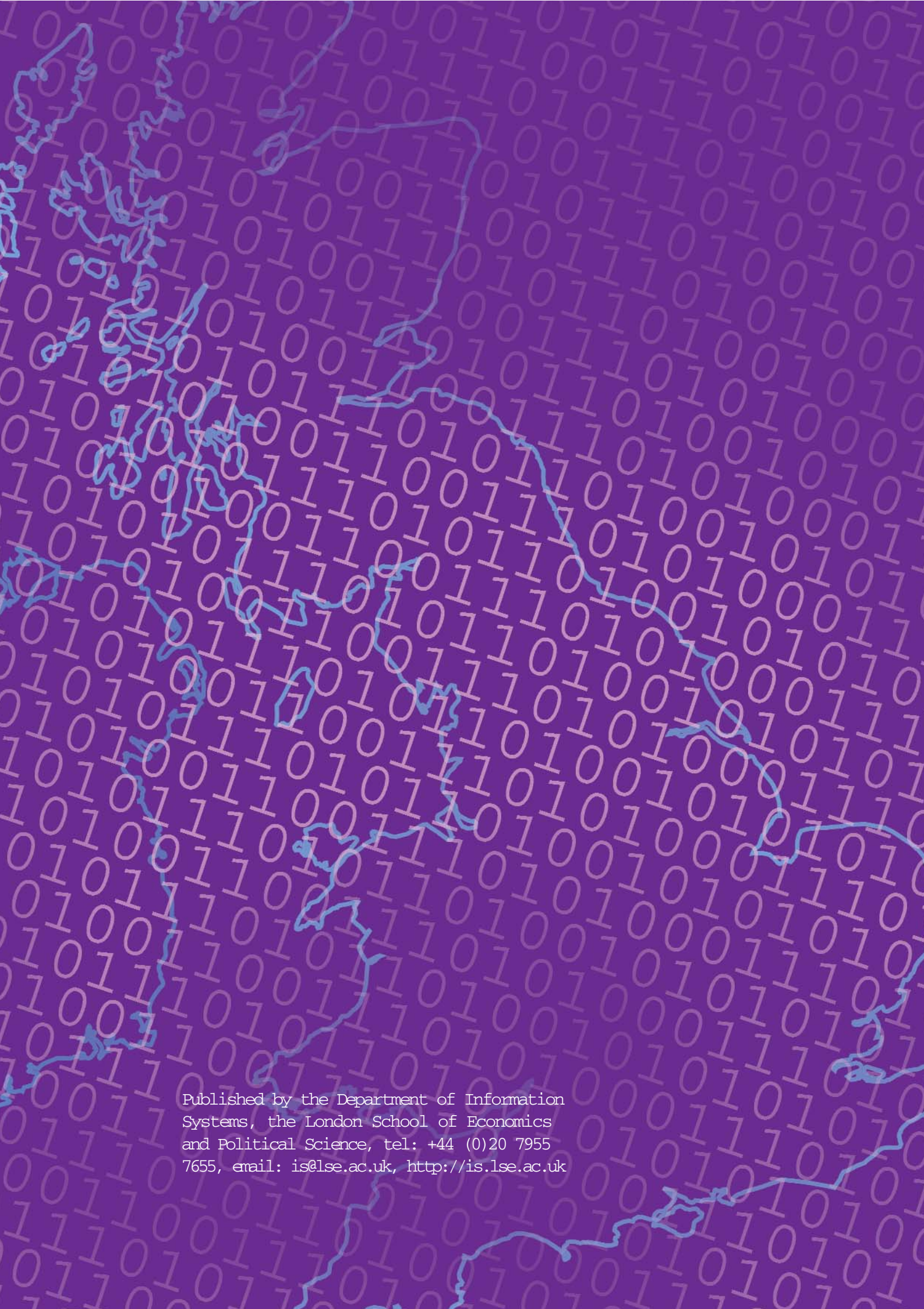
Appendix 2: Cost Projections

All figures are in millions. These are ten-year rollout figures based primary on Government statistics. Where information is inconsistent, median figures have been brought down toward the lower estimate.

	Low	Median	High
Issuing Identity Cards Over a 10-Year Period			
Initial costs to establish issuing processes			
Includes			
- Set up of policies, procedures			
- Audits and dealing with exceptional cases	8	12	16
Purchase of biometric smartcards			
- 67.5 million population at full rollout	270	338	405
Printing personal information on cards	14	14	14
Renewal of cards			
- Assumes that cards will have to be re-purchased and re-issued every four years			
- This figure covers the ten year rollout period	405	506	608
Re-issuing of cards			
Includes			
- Projected defective rate of 0.25%			
- New cards issued because of change of circumstances during application and enrolment phase			
- Data errors			
- Damaged cards			
- Lost or stolen	117	145	173
Total Cost of Issuing Identity Cards	**814**	**1015**	**1216**
Passports (Based on Passport Service Figures)			
Total cost of issuing existing booklet passports	1994	1994	1994
Total cost of issuing new passports			
- Personal interviews for first time applicants			
- Changing passport-centric system to passport-holder-centric system			
- Placing digital photograph on passport			
- Basic UKPS staffing costs	1814	1814	1814
Replacement passports			
Includes			
- Projected defective rate of 0.25%			
- New passports issued because of change of name			
- Lost or stolen passports	128	128	257
Total cost of passports	**3936**	**3936**	**4065**
Readers for Public Sector (As envisioned in the Bill)			
Purchase of Readers			
Includes			
- Card, Fingerprint, Face, Iris, and combined readers			
- For use at selected public service points envisioned in the Bill			
- Replacement technology every three years			
- Replacement of damaged readers (faulty readers catered for in three-year warranty)	261	261	261
Interfacing with Register			
- Secure communications to National Identity Register for each reader and/or public service point	30	45	56
Total cost of readers	**291**	**306**	**317**

National Identity Register			
System Contract over 10-year period (database only) Includes - Research, analysis and development of system - Security assessment and certification - Hardware and software costs - Replacement hardware, software, updates, dealing with system down-times and failure, recertification - IT Department operational costs - Risk margin	298	298	429
Deployment and Adaptation of Systems - Establishing 'pull' from various Government systems required for basic information verification - Adaptation of first-round Government systems for 'push' of information, in accordance with the Bill (various Home Office information systems, Police Databases, Department of Work and Pensions systems)	1261	1871	2481
Total cost of National Identity Register Infrastructure	**1559**	**2169**	**2910**
Managing the National Identity System			
Enrolment of UK population, including - Set up costs - Planning and logistics (policies, practices, audits)	208	213	556
Running costs (maintenance, overheads) - Property leasing and mobile registration centres - Property servicing charges	608	810	1013
Updating information - Changing information on the registry due to change of circumstances - Verifying individual's prior circumstances through verification of biometrics at a registration centre - Verification of the veracity of the new information	203	540	675
Servicing verification - Verification queries from a variety of public sector organisations, in accordance with the Bill - Verification queries from employers - Call centre management	203	540	1013
Verifying biographical footprint of enrolees - Contacting various public sector databases - Contracts with private sector data aggregators and credit bureaux - Document vetting and verification - Verification of individual's prior circumstances, including through verification of biometrics at registration centre - Verification of the veracity of the corrected information	675	878	1013
Correction of entries in the National Identity Register, including - Policies, procedures, and documentation - Regular data integrity checks and compliance with Data Protection Act (including servicing of Subject Access Requests)	53	75	113
Enforcing enrolment of the UK population	65	130	195
Re-enrolment for altered biometrics - Verifying prior information - Collecting new biometrics - Audit	203	405	675
Identifying and policing fraud	43	67	88
Total cost of managing the National Identity System	**2261**	**3658**	**5341**

Specific Other Staff Costs Over a 10-Year Period			
Enrolment Staff			
- Staffing of registration centres for the initial roll-out			
- Training for use of systems			
- Security training			
- Background checks			
- Management	838	838	1118
Staff for the National Identity Register			
- Security training			
- Background Checks			
- Call centre employees			
- Staff for face-to-face meetings to verify changes to the register			
- Full public interface (taking into account non-co-operators)	813	2433	4056
Staff training for public service points			
- Accessing Register			
- Use of biometric readers	68	97	134
Total staff costs	**1719**	**3368**	**5308**
Miscellaneous			
Design, feasibility, business case (already awarded)	12	12	12
Consultancy and other costs	10	52	105
Total miscellaneous costs	**22**	**64**	**117**
TOTAL	**10602**	**14516**	**19274**



Published by the Department of Information Systems, the London School of Economics and Political Science, tel: +44 (0)20 7955 7655, email: is@lse.ac.uk, http://is.lse.ac.uk