palgrave
macmillan

Global Challenges for Identity Policies

Edgar A. Whitley and Gus Hosein

Global Challenges for Identity Policies

TECHNOLOGY, WORK AND GLOBALIZATION

The Technology, Work and Globalization series was developed to provide policy makers, workers, managers, academics and students with a deeper understanding of the complex interlinks and influences between technological developments, including information and communication technologies, work organizations and patterns of globalization. The mission of the series is to disseminate rich knowledge based on deep research about relevant issues surrounding the globalization of work that is spawned by technology.

Also in this series:

BRICOLAGE, CARE AND INFORMATION SYSTEMS
Chrisanthi Avgerou, Giovan Francesco Lanzara and Leslie P. Willcocks

ICT AND INNOVATION IN THE PUBLIC SECTOR
Francesco Contini and Giovan Francesco Lanzara

KNOWLEDGE PROCESSES IN GLOBALLY DISTRIBUTED CONTEXTS
Julia Kotlarsky, Ilan Oshri and Paul C. van Fenema

OFFSHORE OUTSOURCING OF IT WORK
Mary C. Lacity and Joseph W. Rottman

e-GOVERNANCE FOR DEVELOPMENT
Shirin Madon

OUTSOURCING GLOBAL SERVICES
Ilan Oshri, Julia Kotlarsky and Leslie P. Willcocks

EXPLORING VIRTUALITY WITHIN AND BEYOND ORGANIZATIONS
Niki Panteli and Mike Chiasson

GLOBAL SOURCING OF BUSINESS AND IT SERVICES
Leslie P. Willcocks and Mary C. Lacity

Global Challenges for Identity Policies

Edgar A. Whitley
Reader in Information Systems, London School of Economics and Political Science

and

Gus Hosein
Visiting Senior Fellow, London School of Economics and Political Science

palgrave
macmillan

Softcover reprint of the hardcover 1st edition 2010 978-0-230-54223-5

First published 2010 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC,
175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN 978-1-349-35989-9 ISBN 978-0-230-27137-1 (eBook)
DOI 10.1007/978-0-230-27137-1

This book is printed on paper suitable for recycling and made from fully managed and sustained forest sources. Logging, pulping and manufacturing processes are expected to conform to the environmental regulations of the country of origin.

A catalogue record for this book is available from the British Library.

A catalog record for this book is available from the Library of Congress.

10 9 8 7 6 5 4 3 2 1
19 18 17 16 15 14 13 12 11 10

This book is dedicated to
Edgar and Susi Whitley
and
Simon Davies

This page intentionally left blank

Contents

Figures and Tables

Figures

Tables

Abbreviations

ACR-ICard	Alien Certificate of Registration Identification Card (The Philippines)
ATM	Automated Teller Machine (cash machine)
BELPIC	Belgian Personal Identity Card (Belgium)
BID	Bureau of Immigration and Deportation (The Philippines)
CEO	Chief Executive Officer
CGT	Confédération générale du travail (France). "General Confederation of Labour", a national trade union centre
CIP	Citizens Information Project
CRB	Criminal Records Bureau (UK). An executive agency of the Home Office which vets applications for people who want to work with children and vulnerable people
DHS	Department of Homeland Security (U.S.)
DNA	Deoxyribonucleic acid
DPA	Data Protection Act 1998 (UK)
DVLA	Driver and Vehicle Licensing Agency (UK)
DWP	Department for Work and Pensions (UK)
EEA	European Economic Area
e-ID	electronic ID
EIDA	Emirates Identity Authority (UAE)
EU	European Union
FOIA	Freedom of Information Act
FTC	Federal Trade Commission (U.S.)
GAO	Government Accountability Office (U.S.)
GP	General Practitioner (doctor)
HAC	Home Affairs Committee (UK). Charged with examining the expenditure, policy and administration of the Home Office and its associated public bodies
HANIS	Home Affairs National Identification System (South Africa)
HEW	Department of Health, Education, and Welfare (U.S.). A HEW committee called "The Secretary's Advisory

	Committee on Automated Personal Data Systems" produced a study of record keeping practices in the computer age. Its report, commonly known as the "HEW Report", has formed the basis of much privacy legislation.
HIC	Health Insurance Commission (Australia)
HKID	Hong Kong Smart ID card (China)
HMRC	HM Revenue & Customs (UK)
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technologies
IGO	Intergovernmental organizations
INA	Immigration and Nationality Act 1965 (U.S.)
IND	Immigration and Nationality Directorate (UK). This has since been replaced by the UK Border Agency, an agency of the Home Office.
INES	Identité national électronique sécurisée (France).
IPS	The UK Identity and Passport Service, an agency of the Home Office
IT	Information Technology
ITADA	Identity Theft and Assumption Deterrence Act 1998 (U.S.)
LSE	London School of Economics and Political Science
MRI	Magnetic Resonance Imaging
MRTD	Machine Readable Travel Document
NAO	National Audit Office (UK)
NATO	North Atlantic Treaty Organization
NHRC	National Human Rights Commission (Thailand)
NINo	National Insurance Number (issued by UK Department of Work and Pensions). It is used as a reference number for the whole benefits and tax credits system
NIR	National Identity Register ("the Register")
NIRNo	National Identity Registration Number.
NIS	National Identity Scheme ("the Scheme")
NIST	National Institute of Standards and Technology (U.S.)
NO2ID	UK-wide nonpartisan campaign opposing the government's planned identity card, National Identity Register, and the 'database state' more generally.
OECD	Organisation for Economic Cooperation and Development
OGC	Office of Government Commerce (UK)
ONS	Office for National Statistics (UK)
PIN	Personal identification number
PKI	Public key infrastructure
PQ	Parliamentary Question

PS	Passport Service (UK). Forerunner of the Identity and Passport Service
REAL ID	REAL ID Act 2005 (U.S.). Imposes certain security, authentication and issuance procedures standards for the state driver's licenses and state identity cards, for them to be accepted by the federal government for "official purposes"
SSG	Strategic Supplier Group
SSN	Social Security Number (U.S.)
STS	Science and Technology Studies
TWIC	Transportation Worker Identification Credential (U.S.)
UAE	United Arab Emirates
UKPS	UK Passport Service, forerunner of the IPS
US VISIT	United States Visitor and Immigrant Status Indicator Technology. A U.S. immigration and border management system which provides visa-issuing posts and ports of entry with the biometric technology that enables the U.S. government to establish and verify identity.
USA-PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001
WA	Written Answer to a Parliamentary Question

Acknowledgments

We would like to thank our friends who supported us and read through edits of emails, that later grew into briefings, that later grew into reports that later became chapters; our colleagues in the policy world who posed Parliamentary Questions, clarified legal issues, and raised issues in our work and with our work; and for our critics who kept us thinking and kept us on our toes.

At LSE, we are grateful for the unwavering support of Sir Howard Davies, Director of LSE, Professors Ian Angell, Patrick Dunleavy, and Leslie Willcocks and the members of the LSE Identity Project Advisory Board. We are also grateful to Simon Davies for helping to get us into this mess.

Special thanks go out to Dave Birch, Stefan Brands, Phil Booth, Jerry Fishenden, Guy Herbert, Chris Pounder, Angela Sasse, Toby Stevens, and Robin Wilton for sharing their views on identity policy over the years as well as other unnamed individuals who have given invaluable feedback on this work and sustained us with their drive and interest in this complex issue.

Aaron Martin, as ever, and Vivien Priestley helped considerably with their careful reading of the book. Melissa Nolas deserves gratitude for not only putting up with the company we kept but for becoming an advocate.

Some of the ideas presented in the book are developments of earlier work, published in various identity project publications (available at http://identityproject.lse.ac.uk).

An earlier version of Chapter 6 appeared as Whitley, Edgar A. and Hosein, Ian R. (2008) Doing the politics of technological decision making: Due process and the debate about identity cards in the UK. *European Journal of Information Systems* 17(6), 668–677. Reproduced with permission of Palgrave Macmillan.

Series Preface

We launched this series in 2006 to provide policy makers, workers, managers, academics, and students with a deeper understanding of the complex interlinks and influences among technological developments, including information and communication technologies (ICT), work, organizations, and globalization. We have always felt that technology is all too often positioned as the welcome driver of globalization. The popular press neatly packages technology's influence on globalization with snappy sound bites, such as "any work that can be digitized will be globally sourced." Cover stories report Indians doing US tax returns, Moroccans developing software for the French, Filipinos answering UK customer service calls, and the Chinese doing everything for everybody. Most glossy cover stories assume that all globalization is progressive, seamless, intractable, and leads to unmitigated good. But what we are experiencing in the twenty-first century in terms of the interrelationships between technology, work, and globalization is both profound and highly complex.

The mission of this series is to disseminate rich knowledge based on deep research about relevant issues surrounding the globalization of work that is spawned by technology. To us, substantial research on globalization considers multiple perspectives and levels of analyses. We seek to publish research based on in-depth study of developments in technology, work, and globalization and their impacts on and relationships with individuals, organizations, industries, and countries. We welcome perspectives from business, economics, sociology, public policy, cultural studies, law, and other disciplines that contemplate both larger trends and micro-developments from Asian, African, Australia, and Latin American, as well as North American and European viewpoints.

As of this writing, we have reached a critical milestone in the series in that we have ten books published or under contract. These ten books are introduced below.

1. *Global Sourcing of Business and IT Services* by Leslie P. Willcocks and Mary C. Lacity is the first book in the series. The book is based on over 1,000 interviews with clients, suppliers, and advisors and fifteen

years of study. The specific focus is on developments in outsourcing, offshoring, and mixed sourcing practices from client and supplier perspectives in a globalizing world. We found many organizations struggling. We also found some organizations adeptly creating global sourcing networks that are agile, effective, and cost efficient. But they did so only after a tremendous amount of trial-and-error and close attention to details. All our participant organizations acted in a context of fast-moving technology, rapid development of supply-side offerings, and ever-changing economic conditions.

2. *Knowledge Processes in Globally Distributed Contexts* by Julia Kotlarsky, Ilan Oshri, and Paul van Fenema, examines the management of knowledge processes of global knowledge workers. Based on substantial case studies and interviews, the authors – along with their network of co-authors – provide frameworks, practices, and tools that consider how to develop, coordinate, and manage knowledge processes in order to create synergetic value in globally distributed contexts. Chapters address knowledge sharing, social ties, transactive memory, imperative learning, work division, and many other social and organizational practices to ensure successful collaboration in globally distributed teams.

3. *Offshore Outsourcing of IT Work* by Mary C. Lacity and Joseph W. Rottman explores the practices for successfully outsourcing IT work from western clients to offshore suppliers. Based on over 200 interviews with 26 western clients and their offshore suppliers in India, China, and Canada, the book details client-side roles of chief information officers, program management officers, and project managers and identifies project characteristics that differentiated successful from unsuccessful projects. The authors examine ten engagement models for moving IT work offshore and describe proven practices to ensure that offshore outsourcing is successful for both client and supplier organizations.

4. *Exploring Virtuality within and beyond Organizations* by Niki Panteli and Mike Chiasson argues that there has been a limited conceptualization of virtuality and its implications on the management of organizations. Based on illustrative cases, empirical studies and theorizing on virtuality, this book goes beyond the simple comparison between the virtual and the traditional to explore the different types, dimensions, and perspectives of virtuality. Almost all organizations are virtual but they differ theoretically and substantively in their virtuality. By exploring and understanding these differences, researchers and practitioners gain a deeper understanding of the past, present, and future possibilities

of virtuality. The collection is designed to be indicative of current thinking and approaches, and provides a rich basis for further research and reflection in this important area of management and information systems research and practice.

5. *ICT and Innovation in the Public Sector* by Francesco Contini and Giovan Franceso Lanzara examines the theoretical and practical issues of implementing innovative ICT solutions in the public sector. The book is based on a major research project sponsored and funded by the Italian government (Ministry of University and Research) and coordinated by Italy's National Research Council and the University of Bologna during the years 2002–2006. The authors, along with a number of coauthors, explore the complex interplay between technology and institutions, drawing on multiple theoretical traditions such as institutional analysis, actor network theory, social systems theory, organization theory, and transaction costs economics. Detailed case studies offer realistic and rich lessons. These case studies include e-justice in Italy and Finland, e-bureaucracy in Austria, and Money Claim On-Line in England and Wales.

6. *Outsourcing Global Services: Knowledge, Innovation, and Social Capital* edited by Ilan Oshri, Julia Kotlarsky, and Leslie P. Willcocks assembles the best work from the active participants in the *Information Systems Workshop on Global Sourcing* which began in 2007 in Val d'Isere France. Because the quality of the contributions was exceptional, we invited the program chairs to edit a book based on the best papers at the conference. The collection provides in-depth insights into the practices that lead to success in outsourcing global services. Written by internationally acclaimed academics, it covers best practices on IT outsourcing, business process outsourcing, and netsourcing.

7. *Global Challenges for Identity Policies* by Edgar Whitley and Gus Hosein provides a perfect fit for the series in that the authors examine identity policies for modern societies in terms of the political, technical, and managerial issues needed to prevent identity fraud and theft. The scale of the problem exceeds political boundaries and the authors cover national identity policies in Europe and the rest of the world. Much of the book provides in-depth discussion and analysis of the United Kingdom's National Identity Scheme. The authors provide recommendations for identity and technology policies.

8. *E-Governance for Development* by Shirin Madon examines the rapid proliferation of e-governance projects aimed at introducing ICTs to improve systems of governance and thereby to promote development. In

this book, the author unpacks the theoretical concepts of development and governance in order to propose an alternative conceptual framework which encourages a deeper understanding of macro- and micro-level political, social, and administrative processes within which e-governance projects are implemented. The book draws on over fifteen years of research in India during which time many changes have occurred in terms of the country's development ideology, governance reform strategy, and ICT deployment.

9. *Bricolage, Care, and Information Systems,* edited by Chrisanthi Avgerou, Giovan Francesco Lanzara, and Leslie P. Willcocks, celebrates Claudio Ciborra's legacy in information systems research. Claudio Ciborra was one of the most innovative thinkers in the field of information systems. He was one of the first scholars who introduced institutional economics in the study of IS; he elaborated new concepts, such as "the platform organization," "formative contexts;" and he contributed to the development of a new perspective altogether through Heideggerian phenomenology. This book contains the most seminal work of Claudio Ciborra and work of other authors who were inspired by his work and built upon it.

10. *China's Emerging Outsourcing Capabilities* edited by Mary C. Lacity and Leslie P. Willcocks marks the tenth book in the series. The Chinese government has assigned a high priority to science and technology as its future growth sectors. China has a national plan to expand the information technology outsourcing (ITO) and business process outsourcing (BPO) sectors. Beyond the hopes of its leaders, is China ready to compete in the global ITO and BPO markets? Western companies are increasingly interested in extending their global network of ITO and BPO services beyond India and want to learn more about China's ITO and BPO capabilities. In this book, we accumulate the findings of the best research on China's ITO and BPO sector by the top scholars in the field of information systems.

In addition to the books already published and under contract, we encourage other researchers to submit proposals to the series, as we envision a protracted need for scholars to deeply and richly analyze and conceptualize the complex relationships among technology, work, and globalization. Please follow the submissions guidelines on the Palgrave website (http://www.palgrave-usa.com/Info/Submissions.aspx). Stephen Rutt (email: s.rutt@palgrave.com) is the publishing director for the series.

Leslie P. Willcocks
Mary C. Lacity
April 2009

Preface

In many ways the life of an academic is normally little different from that of any other professional worker. We all have periods of intense work pressure, we all experience occasional frustration when our ideas are dismissed, and we all are thrilled when our contributions are recognized by our peers.

As information systems academics in a Department of Management within a world class social science institution, we are delighted when our research is accepted to be published in the top outlets in our field and discouraged when our proposals for research are rejected because of concerns about how the research might not advance the social science understanding of the political effects of technologies.

The "normal" academic life, however, stopped for us in 2005 when we became involved in the identity policies surrounding the UK government's proposals to introduce biometric identity cards. Our teaching (both individually and jointly) emphasizes the importance of understanding technology when trying to make sense of society, an understanding that becomes particularly significant when considering policy issues such as privacy, inequality, development, and the transformation of government. The importance of understanding the political effects of technology had formed the basis for a number of earlier publications and (unsuccessful) grant proposals, and so we sought to apply this perspective to the developing area of identity policy.

As key players in the LSE Identity Project we sought to inform the policy-making process by contributing detailed analysis of the proposed policy. Our intention was to enhance the deliberation of this significant policy initiative and yet the government saw it simply as a politically motivated attempt to discredit the policy. As a result, it singled out one of our friends and subjected him to unprecedented personal attack. This was no longer academic life as we had come to know it.

We feared for our jobs and we feared for our reputations. Both the quality and integrity of our research was questioned by government officials and many of our contacts in industry and the public sector began to avoid us. At the same time, all areas of the media began to contact us on a daily basis, seeking our opinion on the government's behavior and its proposals.

Although much academic research has a significant impact on the policy process, it is rare for the research itself to have a significant presence in the specialist media, let alone the mainstream press. For some reason, however, our work on identity cards has retained a high profile in the years since the LSE *main report* was issued and the report itself generated far more media coverage than the LSE press office had experienced previously.

Despite our best efforts to emphasize the detailed work that had been involved in the 300 + page report we had issued, all too often the coverage focused on the "war" we were having with the government and the difference between our estimate for the costs of the Scheme (between £10.6 and £19.2 billion over ten years) and those of the government (£5.8 billion over ten years).

One consequence of this was that we were invited to participate in almost all the public and private meetings about the topic; an opportunity we took up as far as possible. This gave us unique access to the key players in the policy-making process. We were invited to brief Parliamentarians both from the Labour party and from the opposition parties. We were invited to sit in on key Parliamentary debates as "special advisers."

We were sent and read just about everything that was published relating to the Scheme. Whilst most of this material was publicly available on newspaper websites, Parliamentary web pages etc., we would occasionally be sent materials that were not yet publicly available. As such, as a result of the particular role we were playing in the development of the policy debate, we developed one of the most comprehensive sets of resources about the proposals.

The madness surrounding our involvement did not let up once the Identity Cards Act received Royal Assent in March 2006. Indeed, the research became the gift that kept on giving as the implementation of the Scheme faced a number of problems almost immediately and, once again, we were being called upon to provide independent analysis of the government's revised plans.

Over time, aspects of a more normal life (dogs, marriage, family, teaching, marking, publishing etc.) returned although the Identity Cards Scheme was never that far away. We began reflecting on our experiences and the lessons learned began appearing in academic papers. It became clear that what had happened to us was not an isolated incident that would be forgotten or overshadowed by events such as the cancellation of the Scheme. Instead, there were important lessons for the policy-making process, lessons that were specific to identity policies but which would apply globally.

This book represents the distillation of our insights into the challenges of developing effective identity policies. Although drawing heavily on issues raised by the UK Scheme, many are much more widely applicable and highlight the particular challenges that democratic processes face when attempting to scrutinize and implement policies that leverage the unique capabilities of information and communications technologies.

The book covers the period from the introduction of the Identity Cards Bill to Parliament (2004) through to the first applications for biometric residence permits by certain classes of non-European Economic Area (EEA) foreign nationals (November 2008). This period is placed in a broader historical and global context.

We continue to watch this space avidly, with all the friends and colleagues we've made over these years. It has led to amazing opportunities. One day we found ourselves advising a number of governments on what had to be learned from what we had seen and the next day we found ourselves in refugee camps pushing our knowledge to the limits in the hope of helping to advance a cause. Looking back, we will probably never know for sure whether we were right, but we can rest assured that we knew what we were doing and we were doing it with care, because we knew it really mattered. That is exactly what you should expect from academics.

EDGAR A. WHITLEY AND
GUS HOSEIN
LONDON, 1 May 2009

CHAPTER 1

The challenge of identity policies

> We are all familiar with the increasing need to be able to prove who we are in a secure and convenient way. (UKIPS, 2008a)

With these words, Home Secretary Jacqui Smith introduced the 2008 Delivery Plan for the UK's controversial National Identity Scheme (the Scheme). The Delivery Plan was the most recent statement of intent about the Government's identity policy, the third such statement since Parliament began debating this issue in 2004. The UK seems no closer to being able to address the challenge Jacqui Smith articulates, despite five years of effort and vast amounts of public expenditure. In 2008 alone, the Identity and Passport Service (IPS) spent nearly £32 million on external consultants [Written Answers – WA 267452].

The UK experience highlights the difficulties of transforming a policy ideal into an effective solution. Academic studies of policy-making processes have revealed the many complexities that any public policy faces in moving from principle to practice. It might seem reasonable to assume that policies relating to information and communication technologies (ICT) would fall neatly into a subset of the larger policy-making field. If this were the case, many of the insights from policy analysis would apply equally to ICT-related policies.

This book, however, shows that this is only partially true. By focussing on a subset of ICT policies, namely identity policies, it demonstrates the range of unique challenges that these policies introduce – challenges that require distinct skills from key policy-makers.

It is no longer the case that technology simply supports the implementation and administration of policy decisions; instead technology can now be a key driver of innovative practices. As an illustration, in the UK, the process of paying car tax has moved beyond simply being able to download and print off the official form, to a situation where the online system also allows payment after it has checked the vehicle's details in other databases to ensure that the car has valid insurance and has been officially certified as roadworthy. In this case, the innovative use of technology leverages the process to mitigate the need to present and authenticate various paper documents before paying the tax.

Beyond data-sharing, technologically leveraged policies can take advantage of advances in technology including encryption, digital signatures, and remote authentication to develop innovative practices. The potential of these advances should be maximized to develop technologically-leveraged identity policies.

Despite the opportunities for technologically leveraged identity policies, the UK Scheme fails to take advantage of the opportunities that new technologies present, suggesting a limited understanding of the challenges and opportunities they afford. It also suggests a very traditional view of technology.

Technology can no longer be understood as an artefact that either acts autonomously of human control or can be shaped to achieve any desired policy objective. Instead, key technological design decisions, often political choices, made in the early stages of policy development can effectively lock-down the resulting systems and hence determine the overall shape of the policy initiative. If these initial decisions are ill informed, they can prove incredibly costly (both economically and politically) to unravel, leading to the potential of legacy systems that fail in their primary policy objectives, or abandoned systems that exist as reminders of poor policy-making decisions.

Information and communication technology policies are therefore policies that involve “things”: technological devices such as telecommunications exchanges, databases, computers, and mobile phones, which themselves can be broken down into component elements like algorithms, networks, applications, and processes. More specifically, it is not just the things in themselves that matter, but also the way these “things” are inextricably linked to the social and political life of the society we live in. These things are involved in our communications with others (both in terms of the nature and the content of the communication), our social relationships and the digital footprints we leave behind. Again, depending on the nature of the systems we use, these linkages between systems may be ephemeral, instantaneous, moved, copied, shared, or kept for an eternity.

This book focuses on technologically leveraged identity policy as a specific example of ICT policies. That is, it examines the policy decisions that shape how individuals and organizations can identify and authenticate themselves to third parties. Identification is a process whereby someone’s identity is revealed (“This is Jo Bloggs”), while authentication is a process that results in a person being accepted as authorized to engage in or perform some activity (“I am allowed to withdraw money from this bank account," or "I am old enough to buy alcohol"). The next section examines how identification and authentication raise particular challenges for contemporary life.

Identity policies for a modern society

The advent and widespread adoption of digital information systems has caused many governments to develop, reassess, and transform their identity policies. The problem of identity assurance, that is, securely providing information about you to other parties, is particularly challenging in a mediated, electronic social space where traditional face-to-face mechanisms cannot operate.

Identity assurance policies therefore seek to address the trust-related issues that arise from such interactions. Thus, individuals may wish to confirm that they are over 18 to access particular "age-restricted" resources or services, or may need to confirm that they are entitled to particular government services or benefits. Such situations are easy to imagine in the online and offline world.

For many years, identity assurance *tokens*, that is cards, have proven to be quite effective when making age-restricted purchases (e.g. for alcohol or tobacco) or gaining access to particular services or facilities in the real world. However, as the global problem of voter registration has shown, policies for verifying the identity of individuals for even the most noble of causes can lead to intense political concerns about social exclusion and disenfranchisement, and still result in ineffective and inefficient public policy solutions.

Online, the challenges of authentication and identification are even more troubling and remain unresolved: after nearly twenty years of policies geared toward regulating the internet we are still nowhere nearer to solving the policy problems of, for example, preventing children from accessing pornography. Similarly, electronic commerce transactions can be undertaken more smoothly if the transacting parties are aware of whom they are dealing with.

There are global pressures on policy-makers to implement or enhance existing identity policies for both the online and offline world, frequently using some form of state-issued "identity card" to provide this functionality. Technology policies are not the preserve of national governments, however, and industry-led initiatives, for example tying identity assurance functionality to devices like mobile phones, are also possible. In such cases, the role of government might be limited to regulating the market, or providing a supportive environment for the development of such services.

A common illustration of the potential for an identity policy based on identity cards is the use of the cards to provide "proof of age" services for both young people (wishing to have access to age-restricted services and locations) and older people (wishing to claim age-related benefits). For example, the IPS website (UKIPS, 2009c) gives the following vignettes:

> Ella is 18 and wants to buy some wine from an off-licence to take to a party. Cynthia is a youthful 70 and is keen to claim an "over-65" discount offered at her local garden centre. In each case the retailer could ask for proof of age. As both Ella and Cynthia have an ID card, they do not need to show:
>
> - birth certificate
> - pension book
> - driving licence
> - or any other documents that might be requested to prove identity.
>
> Instead each of them can simply hand over their ID card. In this case the retailers will simply:
>
> - look at both sides of the card checking for the security features, then
> - compare Ella or Cynthia with their photograph on the card.
>
> If the retailers are satisfied that the ID cards are genuine and that they each belong to the person using them, they will then check the dates of birth to confirm their ages. It takes just moments for the check to be completed so that Ella can buy the wine and Cynthia can claim her discount.

And the document Introducing the National Identity Scheme (UKIPS, 2008e) gives this illustration:

> Sita's gone out with a group of friends after college. They're all celebrating and Sita offers to buy a round. When she gets to the bar the barman asks for proof that she's over 18. Sita laughs and says she's 19, but the barman is new and demands proof of age. Sita digs in her bag and pulls out her identity card. She hands it over which confirms that she is in fact 19. As she puts the card back in her purse she is relieved that she no longer has to hand over documents with her address on them to prove her age. (p. 6)

At first sight, a solution based on the presentation of an identity card provides a straightforward mechanism for verifying one's age so that suitable access to age-related services and discounts can be received and prevents the necessity of carrying multiple identity-related documents that can be easily mislaid or stolen.

However, a more sophisticated understanding of the “things” involved in such an identity policy, in this case an identity card, reveals issues that some policy-makers may wish to avoid. Verification of age does not require the disclosure of someone’s date of birth, full name, or any other identifying information that might be found on the face of an identity card. Access to age-related services and content only needs to be dependent on a simple Yes/No assertion linked to the identity of the person about whom the assertion is being made.

This means that in the case of an enhanced, electronic identity card there is no need for the service provider to have access to all the information presented on the card and, moreover, not even a need for the service provider to have access to the individual’s date of birth – personal data that are often used as a security mechanism to prevent identity fraud. Thus an identity policy that actively encourages individuals to present their date of birth without restriction becomes a political issue, particularly if citizens are compelled to have identity cards.

Political drivers of identity policies

It may be a surprise to traditional policy experts that the politics of identity policy can be just as fierce as the politics of taxation policy. However, both call equally on political ideologues and political parties to question the very foundations of the relationship between the individual and the state. Unlike taxation policy, however, few policy-makers have a real idea about the issue they are legislating and regulating. They may not understand the complexity of the problem and may not appreciate the technological issues around alternative solutions to address the problem some examples of which are given below. The policy processes around identity policy need to incorporate fast-moving scientific and technological landscapes that alter not only the nature of available technologies, but also the nature of the problems that the new policies are hoping to solve.

At different times and at different locations, there have been different drivers for identity policies. These include

- the need to combat terrorism (e.g. it has been argued that a third of all terrorists use multiple identities);
- the need to combat fraud (e.g. to ensure that only those who are entitled to government services may actually receive them);

- the need to combat identity fraud (e.g. the growing concern about fraudulent use of identities to open accounts in other people's names);
- the need to manage borders (e.g. the implementation of biometric visa schemes to combat illegal working);
- the need to support the private sector with an adequate regime of identification (e.g. to support customer management and reduce fraud);
- the need to aid the development of electronic government services (e.g. to enable citizens to gain access to government services on-line will require some form of authentication in order to file taxes, etc.);
- the need to provide a consumer-led scheme that minimizes the amount of personal data exchanged between parties (e.g. by storing and exchanging minimal personal data); and
- the need to manage particular populations (e.g. refugees or immigrants with temporary leave to visit or remain in a country).

Each stated purpose, together with its advocates, influences the eventual shape of the policy and the eventual design of the resulting technological schemes. For instance, if the overriding goal of the identity policy is to adhere to international obligations for travel documents, then this will have deterministic effects on the form of the policy: it will need to involve the use of biometrics and "contactless chips" containing specific information regarding the individual, in accordance with international standards. If the purpose is to combat fraud and identity fraud, the solutions might be focused on minimizing the amount of personal data held and exchanged.

However, the nature of the technological "things" listed above is not necessarily unambiguous. Indeed, it is probably unsafe to assume that all those "things" itemized above, such as "biometrics" and "contactless chips" and even "amount of personal data" are the product of clear and stable agreements on their constitutions. "Biometrics" for instance, is a shorthand notation for a complicated domain that is still evolving in terms of scientific, technological, and human factors. Biometrics might be understood to include novel measures of physiological features like fingerprints and iris scans, knee prints and DNA, but also include digital images of the face that we are more familiar with. Contactless chips are even less understood from the perspective of technology, security, and privacy. Even if agreement can be reached on what these technologies might be, there is further disagreement about how they should be used: which biometrics should be used, should they be stored on a centralized database, or only on a local device under user control? Should the original biometric be used or is it feasible to use a "template" taken from the biometric? How much knowledge about people, such as their biometrics, is required for an effective identity assurance scheme to operate?

Comprehensive identity policies therefore involve creating or adapting schemes for the collection and processing of individual-specific data that will be shared across services, both within and beyond government, often for a variety of purposes. Choices to be made include decisions about

- the kinds of technologies involved in implementing the processes;
- the role of the private sector in any identity assurance scheme;
- the balance between the rights and concerns of the citizen and those of government;
- the scope of identity assurance; and
- the drivers underlying any proposals (including technical issues of system interoperability and legal issues of convergence and coherence).

Each stated purpose and associated solution, however, also has a different cost profile. Questions of costs (both economic and political) are likely to influence policy deliberations and public support for the resulting identity policy. Some of the cost profiles that arise from technological design decisions include

- costs attributed to design decisions (whether to establish a central registration centre to where all individuals must report every few years, or an application process that can be conducted through intermediaries such as banks, or by post);
- management of costs (which government administrative department will administer and pay for the scheme? Will others have to pay for access to the scheme?);
- opportunity costs (could the funds and effort be expended elsewhere to greater benefit society through more proportionate solutions?);
- costs burden (who actually pays for the scheme? Tax-payers, industry, public sector, subscribers?); and
- liability costs (who is liable if problems with the scheme cause someone to fail to be identified properly or if someone is incorrectly identified?).

We take as a fundamental assumption the assertion that there is no “obviously best answer” to any of these issues and, indeed, will show that identity policies vary significantly across countries, legal cultures, and historical time periods. Despite the thrust of globalization where citizens and consumers around the world may face similar concerns, and despite the calls for standardization and convergent solutions, we argue that identity policy is such a delicate domain that it requires individualized and culturally sensitive solutions.

This becomes more complicated when differing policy drivers and associated technological choices interact. Once again, this is not an uncommon problem in the analysis of policy-making but it is a problem that is exacerbated by technological considerations, especially given the infrastructural qualities of any system underpinning an identity policy.

This book therefore examines the process of policy-making in a technologically sophisticated area by examining the development of identity assurance policies. It draws particularly on the analysis undertaken by the authors in relation to the UK government's proposals to introduce an identity policy in the form of biometric identity cards for all UK nationals and foreign nationals. In so doing, it examines the limitations of parliamentary and democratic institutions to undertake effective, detailed consideration of complex legislative proposals with a significant scientific and technological element. It makes specific recommendations about the risks of policy laundering, about the consequences of not appreciating the nature of technology, and about the ways in which technological issues should be debated in a democratic environment. The book uses the challenges of identity policies that the UK has faced to suggest the design of innovative and effective identity schemes.

To illustrate some of the complex issues that the formation of an identity assurance policy needs to address, the remainder of the chapter examines one of the policy drivers listed above, namely identity fraud, and its interrelationship with the other drivers. The fraudulent use of identities in both the online and physical world is a growing problem that many governments are seeking to address. In the UK, addressing identity fraud is frequently cited as one of the key reasons behind the introduction of biometric identity cards.

Illustrating the challenges of identity policy: The case of identity fraud

Many governments around the world are now trying to reassess their identity policies in light of technological changes. What used to be simple tasks like opening bank accounts or paying for items over the phone are now threatened by the rise of identity-related fraud. These incidents range from the fraudulent use of an individual's identity to open credit accounts, withdraw cash, or purchase goods to fraudulently using corporate identities and registered details. In extreme cases, individuals may be held in jail because crimes have been committed by someone matching “their” identity (Whitley and Hosein, 2008). Identity fraud may then turn into a terrorism risk when terrorists are able to get identity documents in the names of other people or travel between countries using multiple identities; into an immigration risk as illegal immigrants can assume the identity of a citizen; into a risk to commerce and e-government as organizations cannot have confidence in the identity of the individuals with whom they are dealing; and into a drop in consumers’ and citizens’ confidence when their identities are at risk of abuse.

Many explanations have been offered as to the nature and causes of identity-related fraud. Some see the problem as one that is best addressed by the public sector or state, others see the problem as one best addressed by the private sector. In each case, some form of policy to address the problem is proposed. Others again see the problem of identity-related fraud as a private, individual responsibility, one of the many consequences of a prevailing era of consumption. Unsurprisingly, the responses proposed to the problem of identity-related fraud vary according to the perspective adopted: these include government-issued biometric identification documents and regulations regarding notification of any data breaches, best practice guidelines for secure data handling for organizations, and the use of personal shredders.

In addition to these three areas of intervention (public, private, and personal), the policy responses to identity fraud can also be understood at the level of principles and/or policies and at the level of practices. Many policy initiatives include feedback features that link the practice of policy implementation back to the principles underlying the policy, to ensure that the policy is complied with.

There are therefore many complexities that an identity policy to address identity fraud might face, particularly as interventions in one area might “overflow” (Callon, 1998) into other areas. For example, in response to concerns about the ways in which discarded bills might result in identity-related fraud, a utility company might introduce the practice of encouraging customers to replace printed utility bills with online-only statements (i.e. they check their statements online). Whilst such a practice might result in fewer paper statements being discarded by customers, the practice might overflow into other areas. For example, with customers increasingly encouraged to access online resources via passwords and PINs, there is growing evidence that good practice about password security is not being followed. Individuals often end up using the same password/PIN for many if not all of their accounts. If this password is disclosed, the individual is potentially at risk of increased fraud, as many of their accounts can be compromised.

Other issues arise in both the public and private sectors. In the case of many interactions with government and private organizations, individuals need to identify themselves, for example to set up a relationship with the organization. At present, such identification is often based on the presentation of a series of documents, typically including a recent utility bill. If, however, the individual has moved to using online-only statements, then the best that they can provide is a printout of the online statement. Such printouts are, of course, easily forged. Until practices are updated to involve alternative forms of identification there is a significant risk of identity-related fraud arising in the opening of such new relationships.

Moreover, there are different kinds of relationship that might be created that require different levels of identity assurance (and have different levels of associated risk) (Cabinet Office, 2006). There is a relatively low-level of risk associated with some interactions such as paying a parking fine, where the identity of person paying the fine is not important, only that it is paid for the specific parking offence. Indeed, in some cases, the parking fine might be paid by someone other than the car owner. Other interactions raise far more risks. Disclosing personally sensitive medical records to someone other than authorized medical staff could lead to embarrassment, while incorrectly identifying someone as a suspected criminal could result in misplaced vigilantism. In an organizational context, unauthorized disclosure of information could result in reputational harm. Here there is a requirement for strong initial proof of identity and strong authentication in service delivery (Cabinet Office, 2006 Supplement B: Definition of Service levels).

Identity fraud, identity theft, and the scale of the problem

It is increasingly recognized that personal identities may be as valuable as material possessions. A case of identity-related fraud, perhaps resulting from the abuse of discarded utility bills and credit card statements, can result in large-scale financial loss, distress, and inconvenience for individuals. In addition to any financial burden incurred, there is often a considerable temporal and emotional burden associated with resolving the issue. It has been estimated that individuals can spend an average of between 25 and 60 hours restoring their records. In addition, they may find themselves coming to terms with being the victim of a crime (Privacy Rights Clearing House, 2007). However, the exact nature and extent of the problem is not clear.

Some of the best studies of the phenomenon known as *identity theft* emerge from the United States. One recent study reports there were 8.4 million U.S. adult victims of identity theft in 2007, down from 10.3 million in 2003 with identity theft costing the economy $49.3 billion in 2007 (Privacy Rights Clearing House, 2007). In response, the U.S. Government has developed laws to prevent and investigate identity theft and numerous individual states have also passed laws that provide assistance in recovery from identity theft. In the U.S., identity theft is the responsibility of the Federal Trade Commission (FTC) and a new industry has emerged in the U.S. to protect individuals from identity theft. These firms monitor their clients' credit records and other data records to actively protect them from fraud. Interestingly, these firms often operate for profit and some even offer packages covering the whole family.

In the UK, primary responsibility for identity-related fraud issues resides with the Home Office (equivalent to Interior or Justice departments in other countries), taking over responsibility for the issue from the Cabinet Office (Cabinet Office, 2002). There have been three government assessments of the extent of identity crime in the United Kingdom. The first was produced in 2002 (Cabinet Office, 2002) suggesting that the minimum cost to the UK economy was £1.3 billion. Updated figures issued by the Home Office in 2006 (Home Office, 2006) suggested a new figure of £1.7 billion, although £400 million of this can be attributed to items "not included in the 2002 study." In 2008, a new set of figures was produced based on a new methodology that included operating costs of the Identity and Passport Service for "carrying out identity checks, investigating suspected identity fraud cases, implementing systems and processes to detect and prevent fraudulent applications of passports, including costs relating to the introduction of face-to-face interviews for all adult, first-time applicants for a UK passport" (Home Office, 2008 p. 5). Using this new methodology the annual cost fell to £1.2 billion.

The discrepancy between the figures and the introduction of a new cost calculation methodology highlights two key issues: first, we still do not know how to define identity-related fraud and second, we still do not know how to measure it. In terms of definitions, legislation in the U.S. defines identity theft as taking place when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law" [Identity Theft and Assumption Deterrence Act 1998 (ITADA), enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028)].

The UK uses slightly different definitions, with the Cabinet Office report noting that there is no offence of identity theft per se, but rather that identity crimes arise in conjunction with other offences (e.g. concealing an existing identity, accruing a financial benefit, or avoiding a financial liability), thus suggesting the use of the term identity *fraud* rather than identity *theft*. Noting that identities can be "attributed" (name, date, and place of birth), "biographical" (more detailed personal history, including details of education and employment, address history as found on credit records and electoral rolls etc.), and "biometric" (physical attributes associated with the individual), the report argues that attributed identity is the easiest to assume, often based on fabricated or stolen documents while biographical identity requires much more detailed knowledge of a person's life history. A biometric identity, it is often suggested, cannot be as readily assumed by another. In this context, identity theft occurs "when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead" and identity fraud occurs "when a false identity or someone else's identity details are used illegally: for commercial or monetary gain; to obtain goods or information; or to get access to facilities or services (such as opening a bank account)" (Sir James Crosby, 2008 § 4.1, § 4.2).

It is widely recognized that there are considerable problems in measuring all kinds of fraud with identity fraud being particularly difficult to pin down. For example, Levi and Burrows (2008) do not even consider identity fraud as a distinct category of fraud because of problems of how it might be defined and calculated. Indeed they note that many fraud studies, "particularly those conducted by professional consulting firms with marketing aims," lack the kind of detailed presentation of methodology found in academic research, resulting in findings based on loose methods with limited value for aggregation purposes (p. 296).

More generally, Levi and Burrows identify six key concerns with existing sources of data about the extent of fraud:

- Weaknesses and inconsistencies in defining "fraud";
- Data collection undertaken for different purposes and with poor response rates;
- Neglect of some forms of fraud;
- Imprecision about the unit of analysis (such as companies and their subsidiaries as well as transnational organizations);
- Insufficient concern about the implications of the variable time between the commission of the offence and awareness, reporting and recording of the crime; and

- Weak disciplines applied to the aggregation of the data (adapted from Levi and Burrows, 2008, p. 298).

Despite the problems of definition and measurement of the scale of the problem, fraud losses are undoubtedly growing and costs run to the billions (Sir James Crosby, 2008). Identity fraud is therefore one of the drivers for identity policies in most global economies.

Who should be responsible for addressing identity fraud?

In general, the question of where responsibility lies for tackling identity fraud can be found at three distinct levels: the private individual, the private sector firm, and the public sector (government). This section reviews some of the existing literature that views identity fraud at each of these levels and relates them to the practice/policy–principle distinction.

Private individuals

Perhaps the least immediately intuitive level for responsibility for identity fraud is that of the individual citizen. However, in a recent review, Donncha Marron (2008) argues that much of the legislation on identity fraud, particularly in the U.S., is framed around the idea of the consumer. For example, U.S. policy including ITADA enshrines the principle that the primary victim is the consumer. This, he suggests, did not occur in a vacuum – rather it arose in a context of neoliberalism that makes consumers "responsible for their own condition," responsible for the "establishment and maintenance of an individualized sense of self or one's life as coherent narrative or biography" (p. 23). In particular, he suggests that this should be understood as part of a wider notion of consumption, meaning that identity fraud has the potential to affect an individual's ability to consume, (e.g. by denying them credit if their credit history has been abused), hence undermining their ontological security as well as their emotional and financial well-being.

From this perspective, therefore, it is hardly surprising that much of the onus for preventing and responding to identity fraud lies with the individual. As Marron notes, the advice offered by organizations like the U.S. Federal Trade Commission encourages individuals to be "entrepreneurial," they must actively canvass credit reference agencies, creditors, and debtors if they discover their identity has been used fraudulently. Similar emphasis on the individual can be found in the UK "Identity theft" website, which has specific pages entitled "protecting *yourself*" (Identity Theft, 2009a, emphasis added) and “What if it happens *to you*” (Identity Theft, 2009b, emphasis added).

Private sector companies

With most identity fraud associated with financial institutions it is arguable that much responsibility for preventing identity fraud lies with private sector companies. Their handling of personal and identity data plays a key role in preventing identity-related fraud from taking place. They have particular responsibilities for the management of personal data that might be used to perpetrate identity crimes. In addition, they normally have a statutory duty to properly identify individuals before undertaking high-value transactions.

Information collection and processing is regulated in the United Kingdom under the Data Protection Act 1998 (DPA). This law limits the amount of personal information that may be collected by an organization to information that is proportionate to its stated purposes. Although the DPA, and its European equivalents, are based on data protection principles first articulated in the United States (U.S. Department of Health Education and Welfare (HEW), 1973) before being adopted by the Organisation for Economic Cooperation and Development (OECD) and the Council of Europe, there are no direct equivalents in the U.S. for mainstream data handling.

What does exist in the U.S., however, is specific legislation that, amongst other requirements, states that companies must notify their employees and/or customers if data held by them is breached (Holtfreter and Holtfreter, 2006), which is supposed to help consumers minimize the risk of identity fraud. What is less clear, however, is the effectiveness of this approach to the problem (Binder and Gill, 2005; Holtfreter and Holtfreter, 2006). Thus, in the UK, there has been resistance against introducing such requirements for fear of causing undue worry in individuals who may not be able to evaluate the notifications appropriately (Romanosky et al., 2008). In addition, it may prove necessary to issue periodic “nothing to worry about” messages if no problems arise so that individuals can be reassured that they have not missed out on important notification of problems (Marron, 2008).

Government and the public sector

As was noted above, there is a general recognition that public policy has an important role to play in addressing issues of identity fraud. This can range from specifying legislation about identity fraud to encouraging best practice in industry. Moreover, as a holder of significant personal data for most aspects of policy delivery (Dunleavy et al., 2006), the public sector has the opportunity to "lead by example" with respect to the secure handling of personal data.

Government may also assist by helping those who are the victims of identity fraud, as they try to re-establish control over their personal information and identity. In this sense, the government could act as a supporting resource.

In addition, in most countries government tends to be a guarantor or issuer of identity documents. This is enabled by the fact that the state often holds the monopoly over recording key details about individuals' "life events" such as births, marriages, and deaths. Governments also tend to oversee many of the activities that require identity documents and so, in turn, issue official documentation such as driving licenses to authorize driving, passports to identify its citizens to other governments, etc.

Many governments oversee some form of a social security net and issue targeted unique identifiers such as the Social Security Number in the U.S., or the National Insurance Number in the United Kingdom. In some countries, governments issue unique identifiers and identity cards that are cross-purpose identifiers. The difference is that the targeted identifiers are often limited in purpose to a specific task, for example the administration of national pensions, while a cross-purpose identifier can be used across government services and the public sector.

Identifiers and records management can play a role in reducing the risk of identity fraud. For example, a government could require that large financial institutions verify the identity of new account holders by also checking their identity card, or by verifying the given address and contact details against the records held by government departments.

A technological policy to address identity fraud

Despite there being a strong case for public policy in addressing the problem of identity fraud, an ill-informed or poorly implemented policy could potentially make the problem worse rather than better. For example, the malicious use of Social Security Numbers (SSN) in the U.S. has been at the root of many plots to perpetrate identity fraud (Berghel, 2000; Garfinkel, 1995). The SSN was originally intended for very specific applications and yet now it is being used across many public and private sector services and it was never designed for such an eventuality.

A typical response to such a failing public policy is to attempt to differentiate between the policy and its underlying principles and the practice and implementation of the policy. That is, to apportion the blame not to problems of principle but to questions of practice (cf Collins and Pinch, 1998a, ch. 3).

Many of the traditional responses to poor policy implementation, for example enforcement and monitoring powers built into the policy itself, may themselves be problematic. For example, Froomkin (2007) explores the challenge of enforcing a "viral" privacy standard for government-issued identifiers like the SSN, where, for example, the government could mandate that the use and storage of tax-payer funded credentials be limited to those organizations who agree to be bound by national privacy rules. He notes, however, that in the U.S. context there may be some First Amendment limitations on Congress's powers to regulate the repetition of "true" statements, which a government-issued identifier would certainly be.

Similar problems of poor enforcement of principles in practice can also be found in the private sector (Verizon Business, 2008), where it is unclear how effective published security manuals and training programs are at addressing practices of end users who may be unaware or uninterested in the security implications of their actions (BBC News, 2008b).

Technologically-leveraged policies, however, offer innovative opportunities for addressing some of these enforcement and implementation issues. It is possible to design systems that regulate normal behavior to follow the particular norms and ideals of the system designers (Lessig, 1999; Mlcakova and Whitley, 2004), for example by using cryptographic methods to limit the effectiveness of just presenting the identity credential for visual inspection; so called "flash and go" usage.

A state-issued identifier might be designed so that it is not directly accessible from an identification token, but instead might require technological means to access a (changing) decryption key allowing access to the identifier. It would therefore be feasible to limit access to the decryption key to duly authorized organizations who commit to upholding the policy principles every time they access it. Such a policy, however, introduces the business need to provide round-the-clock support to enable access to the decryption key at all times and in all eventualities, or fall-back measures and liability constraints if the service is unavailable.

Another technological policy response to identity fraud might be to introduce a policy of data minimization (Home Affairs Committee, 2008; Sir James Crosby, 2008) whereby "as a matter of principle, the amount of data stored should be minimized." This means that "in the design of its policies and systems for collecting data, the Government should... collect only what is essential, to be stored only for as long as is necessary" as data that are not held cannot be breached and cannot lead to problems of identity fraud. Implementing data minimization, however, will require extensive redesign of both systems and work practices and so may be better suited to the design of new systems rather than existing systems.

Technologically-leveraged policies like these highlight the importance of understanding these practical issues that underlie a policy implementation. For example, questions of costs and public confidence in the technology become significant.

In the U.S., when Congress approved the REAL ID Act there was near unanimous approval for the scheme that would require all states to issue *secure* driver's licenses. When the costs of the scheme were finally calculated (with estimates of between $17bn and $23bn) and Congress issued no funds to support the implementation of this scheme opposition to the proposals grew significantly.

Costs sometimes act as a grounding mechanism, bringing policy-makers with lofty dreams of new technological infrastructures down to reality when faced with detailed implementation challenges. Dreams of combating foreign terrorism through the use of biometric passports are easy to come up with, and the standards for these documents were quickly approved. Yet the implementation of these passports around the world is expected to take over a dozen years on average as governments grapple with the idea of building biometric enrolment centers and securing information on contactless chips.

The substantial associated costs of a comprehensive identity scheme go some way to explaining why, if the solution appears so clear, there are so few successful comprehensive identity assurance implementations. For instance, online verification of credit card purchasing is recommended to assure that a credit card presented for a transaction is in fact a valid credit card, but the facilities for online verifications of billions of transactions a year, with a commercially reasonable "response time," is very difficult to implement technologically. A similar practical concern may apply to the question as to why some banks have tested, but have declined to implement, biometric verification for banking transactions: the opportunity and management costs may be too great and may place too much emphasis on the relatively low-level employees working on the front line of transaction processes. Liability costs also explain why private sector identity assurance initiatives have been slow to emerge, where a financial institution might not be willing to be held accountable for a high profile error in an authenticated identity based on a bank card they had issued.

Public confidence in the implementation of technologically-leveraged policies also becomes important (Pieri, 2009; Whitley, 2009). Since 2007, there have been a series of high profile cases of government mismanagement of personal data. The most significant was probably the announcement of a data breach involving the loss of the personal data for 25 million individuals and 7.25 million families. The incident, which is discussed in more detail in Chapter 3, arose when a civil servant at Her Majesty's Revenue and Customs sent a full copy of the data on two password-protected compact discs to the National Audit Office. They never arrived and have still not been recovered (and probably never will be). The discs included the names of recipients and the names of their children as well as address details and dates of birth, child benefit numbers, national insurance numbers and, where relevant, bank or building society account details.

In light of the seriousness of the breach, an announcement was made in Parliament on 20 November 2007 by the Chancellor of the Exchequer and the story made the front pages of all newspapers for a number of days, with many emphasizing the risk of identity fraud.

One media commentator, Jeremy Clarkson, writing in *The Sun* tabloid newspaper, said that he could not see what the fuss was all about, as it would not be possible for the leaked information to be used for fraudulent purposes – at best individuals would only be able to make payments into his account. To make his point, he published his bank account details, along with information about how to locate his home address from publicly available sources. A week or so later, he published a shame-faced apology. Someone had used this information to create a monthly direct debit for £500 to a charity he was known to support, demonstrating that this information could be used to perpetrate identity fraud (BBC News, 2007a).

Issues of data management also apply in the private sector, where there have been a series of high profile data breaches in recent years (e.g. Nationwide Building Society, TJX/TK Maxx). A recent industry-based study by Verizon Business (2008) identifies a number of important themes in relation to data breaches that they were called in to assist with – most data breaches are the result of a series of events, rather than any one factor. This suggests that, for example, a policy for installing "patches" and updates to the operating system needs to be combined with a similar regime of updates for application software such as email and web browsers. A second area of concern that the study notes is the large number of breaches associated with data that the organization did not know it was holding. This means that the data that are being unknowingly held are often less secure than data that are known to be sensitive (Verizon Business, 2008).

Implications

A traditional policy analysis would be hard-pressed to understand the problems with establishing a comprehensive identity policy. A policy of this type would have to bridge the public and the private sectors, to establish new centers of information collection, and to use advanced technologies that have not been tried and tested on a large scale under intense public scrutiny.

In fact, public scrutiny is increasing, particularly because of the lack of confidence in the processing of personal information by both the public and private sectors. The creation of another new store of "knowledge" about the citizenry or all consumers would thus give rise to considerable concern (FIPR, 2009). This would be particularly true of the use of new technologies and these technologies have implications on the choice of design and the likely costs that will be incurred. Amongst these costs are the liability costs of designing a system that could be used across the public and private sectors for a wide variety of services.

Of all the ICT policy challenges, identity policies therefore pose a particularly perplexing case. Like more traditional policies, these policies are driven by agendas set by powerful bodies. But unlike traditional policies, the policy is also driven by technological aspirations, where new techniques will enable a policy that was previously impossible (Fishenden, 2009). The key point is that these are the very same reasons why this policy domain is fraught with challenges.

Policy-makers continue to believe that technology is the source of the solution. Our contention is that technology introduces new issues for consideration within the public policy deliberative process. Sadly, however, policy-makers have yet to greet these new challenges as issues worthy of further study. Instead, technologies are "things" to be plugged into older solutions to make them more effective.

At a time when the problems are so serious, such as the growing concerns about terrorism, illegal immigration, identity fraud, amongst a myriad of others, this book will show that the zeal to find new solutions has not been matched with an interest to understand how to effectively introduce identity policies. Only an informed policy process can understand how to make this work, but unfortunately all that has been seen to date is "politics as usual," building a house of cards.

Overview of the book

In order to understand and appreciate the challenges of identity policies in a global world, this book focuses on the UK proposals to introduce a National Identity Scheme (the Scheme) based on biometrically based identity cards linked to a centralized National Identity Register (the Register). The Scheme arises from the Identity Cards Act 2006 (the Act). An analysis of the extensive Parliamentary and wider public discussion about the proposed Scheme reveals limitations of the abilities of our policy-makers to review technologically-leveraged policies.

The book begins with a review of national identity policies in Europe and the rest of the world. Chapter 2 reveals the wide variety of identity policies and the need to disentangle the idea of having "an identity card" from underlying identity policies. It also reviews the contexts in which many of these policies were introduced and the forms of oversight and scrutiny they involved.

Chapter 3 presents the life cycle of identity policy in the United Kingdom, from the earliest forms of identity cards introduced during the two World Wars, to the Parliamentary passage of the Act. It highlights the role of the LSE Identity Project's assessment of the proposals and the key events since the Act was passed.

The key features of the UK National Identity Scheme, as presented to Parliament, are described in Chapter 4, which also includes an overview of the claimed benefits of the Scheme as well as details of how the Scheme would be funded and used in practice.

A key argument used to justify the proposals was that the UK was obliged to upgrade its existing passports to comply with international obligations on machine readable travel documents. This claim is critically reviewed in Chapter 5, which shows that while the UK may have chosen to upgrade its passport documents it was under no legal compulsion to do so.

Chapter 6 reviews another way in which Parliamentary due process was overridden, in this case, due to the way in which knowledge of science and technology are conventionally conceptualized as being distinct from politics. The chapter argues that effective scrutiny of technologically-leveraged policies requires a due process for considering the perplexities about technological issues introduced by informed advocates.

In Chapter 7, the Parliamentary debate about the Scheme is analyzed, focusing particularly on the intentionally ambiguous statements made by the government about the costs and voluntary nature of the Scheme. The intentional use of ambiguous statements again limits the effective scrutiny of identity-related policy proposals.

The language used to describe the Scheme is further evaluated in Chapter 8 where consideration is given to the espoused certainty that the Scheme would deliver exactly as promised and on budget. Experience with large projects has repeatedly demonstrated that such technological certainty is misplaced, especially for long-term developments. It suggests that for a technologically-leveraged policy to progress, confidence in the ability to deliver the policy, rather than misplaced certainty, is required.

Chapter 9 reviews the Scheme five years after it was first introduced, showing how it is likely to be delivered and demonstrating how significantly it has changed from the version presented to the UK Parliament. This again raises important questions about the role of democratic scrutiny in high profile, technology-based policies.

The book ends with a review of the implications from the study of identity policies in the UK, making recommendations for Parliamentarians and academics about the effective scrutiny and oversight of identity policies and technologically-leveraged policies more generally.

Chapter 2

A review of national identity policies

To many governments, a national identity policy is an obvious requirement as they have long had policies and laws that require some form of identification or formal identity document and some policy for when that identity is necessary. These policies may be decades, if not centuries, old developed as the nation-state developed, linked to taxation, instituted to regulate the flow of peoples, or developed due to imperial requirements (Amoore, 2008).

In the modern nation-state, the question of identity policy needs revisiting and for those who have not yet established comprehensive policies, proponents of policy change often argue that the time for a formal identity policy has finally arrived. These policies are generally quite limited, however, as they tend to imagine the institution of a new identifier such as a national tax number, or a new identity document such as an identity card.

With new technologies and new opportunities such as using government services on-line and the deployment of biometrics, a new generation of policies are slowly emerging that are taking national identity policies to new levels, leveraging the opportunity for innovation that new technologies offer the nation-state (Fishenden, 2009). The policies of yesterday of simple cards and single, universal identifiers are being replaced by comprehensive registration and administration schemes. Even in those countries where national identity policies might be referred to as obvious there is often little understanding of the ramifications of more innovative identity policies.

This chapter reviews the international landscape for identity policy. In a number of national identity policy debates, as most recently seen in Australia, Canada, and the United Kingdom, proponents of national identity policies point to other countries with identity cards to show that their own governments are far behind the rest of the world. Reality is actually quite different, however, as many of these other countries have not even begun to think of new, technologically-leveraged identity policies and so the nascent proposals often go well beyond what is deemed the cultural norm in these other countries. The introduction of technologically leveraged identity policies goes much further than the mere existence of an identity card or a single unique number for administrative purposes.

Technology is not the only difference, however. The nature of the policy debate that led to the establishment of a national policy is also noteworthy and cannot be easily dismissed with the simple claim that every other country has identity cards and so must we. For example, is it appropriate to compare a scheme being introduced in the twenty-first century following a full parliamentary debate with one that was introduced in a time of war? Questions of scale and population also become important as the implementation of an identity scheme for a small country with a small, homogenous population may face very different issues from those of a country with a large, cosmopolitan or geographically dispersed population.

Countries also vary in the extent to which their cards are voluntary or compulsory (to obtain, carry, or present the card), the legal frameworks that oversee them, the cost of the card itself, whether they are used for identification purposes only, or are intended for wider use in society.

In such circumstances, the richness of experience in identity schemes across the world becomes apparent and makes straightforward comparison between cases much more problematic, a common problem for academics drawing on case studies. The data in this chapter present a snapshot of the current diversity of global identity schemes and policies, based on information accessible from the UK in early 2009. Inevitably, some of the detail presented here will change over time. However, the underlying principles behind each scheme and the concerns that have influenced their development and oversight mechanisms are less likely to vary significantly over time.

Identity cards in Europe

Mainland Europe is well known for its identity card schemes. This can be related to the establishment of civil law (Froomkin, 2009), whilst others claim it is linked to the earlier oppressive regimes in many of these countries. More interesting than the possible explanation for the existence and acceptance of identity cards in these countries is the diversity even within these countries about the nature of their national identity policies. For instance, in 2004 the UK House of Commons 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. (Home Affairs Committee, 2004, §22)

As is shown below, there is indeed a wide variety of identity systems in Europe, just as there is a wide array of concerns regarding the systems. Each country's domestic politics varies, just as their cultural values differ. German privacy law, for example, prevents the Federal government from creating a centralized 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 (Standing Committee on Citizenship and Immigration, 2003). In addition, according to Arora, the historical background for existing schemes influences the rate at which they are capable of incorporating new technologies and hence the interoperability of systems within Europe (Arora, 2008).

Among the more noticeable differences between schemes within Europe are whether they are compulsory or voluntary and how much an identity card typically costs.

Table 2.1 shows that, in general, compulsory schemes are cheaper for the citizen than voluntary ones (LSE Identity Project, 2006a), which suggests that for the voluntary schemes to be successful, citizens must find it worth their while to purchase the cards. The next sections describe the identity policies and associated identity schemes in many European countries to draw out the variances amongst the policies, as well as the commonalities, claimed and observable benefits.

Austria

The Austrian identity system presents novel solutions to the question of cross-agency referencing. For historical reasons, Austrians have been wary about the ability to link personally identifiable information across government departments. Therefore, when its new electronic identity card was introduced in 2004, specific technological measures were introduced to limit the use of a single identification number.

Table 2.1 Identity schemes in Europe (2009 prices)

Country	Requirement	Charge (€)
Austria	Voluntary	57
Belgium	Compulsory	15
Bulgaria	Compulsory	n/a
Cyprus	Compulsory	8
Czech Republic	Compulsory	4
Denmark	No card	n/a
Estonia	Compulsory	n/a
Finland	Voluntary	40
France	Voluntary	Free
Germany	Compulsory	8
Greece	Compulsory	Nominal
Hungary	Voluntary	5
Ireland	No card	n/a
Italy	Voluntary	20
Latvia	No card	n/a
Lithuania	Voluntary	0
Luxembourg	Compulsory	3
Netherlands	Voluntary	21.50
Portugal	Voluntary	5
Romania	Compulsory	2
Slovakia	Compulsory	4.50
Slovenia	Voluntary	12
Spain	Compulsory	10
Sweden	Voluntary	37
Turkey	Compulsory	2

The Austrians maintain a Central Register of Residents with an associated registration number. This number is used to generate an associated identification number stored on the citizen's card. From this one number, which is not itself used, the card is able to generate unique sector-specific (e.g. tax, health, education, etc.) identification numbers (Otjacques et al., 2007). This use of modern technology, therefore, explicitly prevents automated linking of data between government departments (and hence the creation of a de facto single national identification number).

Belgium

In Belgium, cards were first issued in 1919 to anyone over the age of 12. They were renewable every 10 years. In recent years, the Belgian

Government has announced a new "electronic" card that will cost almost three times as its predecessor – up to €15 per card. These new cards will have to be renewed every five years, again leading to a rise in costs.

The Belgian Personal Identity Card (BELPIC) is a relatively sophisticated card and makes Belgium the first country in Europe to include a digital certificate in an identity card (Van Alsenoy and De Cock, 2008). A digital certificate, put simply, is a digital representation of a credential and permits identification and authentication transactions to be performed at a distance and on-line. It is supported by cryptographic protocols to ensure some levels of mathematical assurance that the transactors are legitimate. In turn, the certificates permit digital signatures, which is the equivalent of an individual signing a piece of paper, but again backed up with cryptographic protocols.

The Belgian Government's goal is to enable citizens to carry out on-line secure transactions with government agencies, to access e-government applications and to perform e-banking, or other private 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 (EPIC and Privacy International, 2004).

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 identity card by the end of 2009 (Expatica, 2004).

Though much can be said about including cryptographic protocols on the card, the security of the card deserves scrutiny. In an interesting development, it appears that the Belgian Government is intentionally making spelling mistakes on its cards in order to confuse fraudsters (Libbenga, 2005), which leads to the conclusion that they accept that the card can be forged. In addition, a cryptography research team from the Catholic University of Louvain disclosed serious weaknesses in the Belgian biometric passport (Avoine et al., 2007). The Belgian e-ID cards do not implement any access control mechanisms. This means that it is difficult to prevent others from reading identity information from the chip. Moreover, there is no way for the citizen to choose what information will be released (De Cock et al., 2008).

Estonia

The Estonian identity card ("small in size, big in content") (Republic of Estonia, 2009) is the country's primary identification document. Its virtues have been promoted by the former UK Home Secretary, Charles Clarke, in a Channel 4 television documentary on fighting identity fraud, telecast in March 2007.

The card contains the holder's name, sex, citizenship, date of birth, place of birth, personal identification code, photo, signature, date of issue and date of expiry, and document number. The personal identification code is widely used in government and private sector databases. For resident aliens with valid papers, the card also contains residence and work permit data. In addition to many security features, the card has a machine-readable code and a chip which contains both copies of the visual data on the card and two security certificates to verify the individual and supply digital signatures (Estonia Citizenship and Migration Board, 2009).

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 civil liberties grounds in the Third 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 and the CGT Union (the General Confederation of Labour) (Noiriel, 2005). 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 (Piazza, 2005).

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," i.e. "Jew"). The central records-file was also abolished. In 1974 the Government decided to phase out the collection of the fingerprint and began moving toward an optional card. This gradual reduction in the regime represents a stronger regard for civil liberties with regard to identity cards.

A first attempt to introduce a digitized identity 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" (Decret n87–178, 1987). This is the form of the current national identity card. It is not mandatory and while a fingerprint is taken it is not digitized and does not appear on the card. It is stored securely and only on paper. While a judge, in a specific case where the police already have a suspect, can access that paper with the fingerprint, conditions for access are tightly regulated (Decret n55–1397, 1955, Article 5).

A central database was eventually 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, that is when it was issued and presumably if it was reissued; but there is no audit trail of each transaction done with the card. 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 and only in circumstances involving an offence (Decret n55–1397, 1955, Article 11). 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 (Decret n55–1397, 1955, Article 12). To this day, in France there are continued negative responses to the centralization of personal information (Noiriel, 2005).

On top of a long history, it is essential to understand evolutionary or revolutionary proposed policy changes. For instance, research in 2005 found that there were two separate innovations planned for the French card. One is emerging from the Ministry of State Reform, the other from the Interior Ministry. Each had very different goals and in turn very different implications.

France I: E-government strategic plan

The French Minister for State Reform wished to oversee a strategic plan to provide services to citizens, the private sector, and the public sector supported by e-government initiatives (French Government, 2004). The plans emphasize 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 aimed 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 minimized to increase the confidence of users. The Ministry acknowledged that e-government gives rise to two contradictory requirements:

- simplifying formalities for the users, which entails 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; and
- upholding the protection of personal data, which may in fact restrict the interconnections between government departments. (French Government, 2004, p. 13)

The French Ministry of State Reform developed its solution to this conflict:

> Government guidelines are clear: do not authorise uncontrolled generalised exchanges between departments. However, the development of e-government must grant citizens more transparency in the monitoring of their administrative papers and better control of their personal details (confidentiality, right to access and correct data regarding them). (French Government, 2004, p. 13)

To enable this, the Government promised to provide tools and services which will enable citizens and professionals "to exercise their rights more simply and completely" (French Government, 2004, p. 13). These tools and services include:

- **Decentralized storage of data:** The French Ministry of State Reform is aware that there are several options available, including centralizing 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" (French Government, 2004, p. 13). The French Government proposes instead that all data will remain decentralized 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. (French Government, 2004, p. 15)

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, which would include a listing of all relevant identifiers, "would probably not go down too well in our country" (French Government, 2004, p. 15). 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. (French Government, 2004, p. 15)

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 departments. At the same time, the French Ministry of State Reform stated its intent to preserve the ability of users to not identify themselves to government departments unless necessary.

The French Ministry of State Reform chose 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 and no centralized list of identifiers.

France II: The Ministry of Interior proposal

The interior ministry was at the same time proposing a completely different identity policy. The project, entitled "Identité national électronique sécurisée," or the "INES" project, was officially announced in February 2005 (Piazza and Laniel, 2008).

This system in many ways mirrors the UK Home Office's proposals. In this policy, the card contains facial and fingerprint biometrics (two fingerprints from the six 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 to adopt a biometric passport and adds that it should comply with the European Union standards, in particular the EU Council decision of 13 December 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.

Civil liberties groups voiced numerous concerns regarding the proposal (Various, 2005), asking for clarification of the nature of the "international requirements" and recalling imagery from the Vichy regime (Marzouki, 2005).

Identity theft and fraud, particularly by terrorists, are given as some of the principal reasons for the new card system. A coalition of civil liberties groups, among them unions of attorneys and of magistrates, responded to the government's claims 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 U.S. and the UK.

The coalition of groups 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 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" (Bauer, 2005).

The proposal faced 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 was placed under review by the Commission Nationale de l'Informatique et des Libertés, the national privacy regulatory commission.

In June 2005 a consultative report was released by the Forum for Civil Liberties on the Internet (Anonymous, 2005). This NGO was asked by the 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); and
- a clear Parliamentary debate on the obligatory nature of the card.

A law implementing the system was due to be introduced into the French Parliament in September 2005. In October/November 2005 identity checks that target minority communities disproportionately were said to be the basis for widespread rioting (Wadham et al., 2006). At the time of writing, neither policy has moved forward.

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 identity 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.

Instead, any information that is collected for the identity 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 are deleted and destroyed (Standing Committee on Citizenship and Immigration, 2003).

No federal agency or private sector organization can use the identity card number for registration. The scheme is organized at the level of the Länder (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 (Home Affairs Committee, 2004).

Slowly, Germany has moved toward biometric identity cards. The German Prevention of Terrorism Act of 2002 includes a specific provision that biometric data in passports and identity cards may only be stored on the cards and not in centralized databanks. It took many years for a political solution to be found to deal with concerns over privacy.

Data Protection authorities are concerned that a biometric system must meet some basic criteria. First, the biometric data must not be used to gain other information about personal attributes (for example, reviewing photos in order to determine race). Second, individuals must know which biometric data will be stored and how they will be used. Third, 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 (Various, 2002). 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 centralized 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 € 22 million to € 700 million for implementation and from € 4.5 million to € 600 million for annual maintenance of systems for passports and identity cards (eGovernment news, 2004a).

In 2007 a political solution finally emerged and the German Parliament authorized two fingerprints and a photograph of the individual's face on the card. The primary safeguard against abuse and the solution to the political challenge set by the second-largest party in the Parliament was that the biometric data should reside only on the card and could not be stored elsewhere. The Social Democrats concluded that because the storing of the data elsewhere had been "ruled out completely," the Social Democrats could finally support the initiative (Heise Online, 2007).

Later, further safeguards emerged when the German government noted that the smart identity card would support pseudonyms for electronic transactions. In one example, the Government promised that an individual card number is used to generate a pseudonym that cannot be reconverted mathematically to the original card number, which could be used to register at a site on-line (eHealth Europe, 2008; Heath, 2008).

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 (EPIC and Privacy International, 2004).

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, 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 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 (Standing Committee on Citizenship and Immigration, 2003). 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 in 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 to 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 compulsory recording of 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” (Greek Data Protection Authority, 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 (eGovernment news, 2003).

Hungary

The emergence of strong privacy safeguards in Hungary reflects those encountered in Germany and Greece. The most notable development in privacy protections was the Hungarian Constitutional Court decision in 1991 regarding the collection of census information.

At the time, 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 or 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 (Decree, 1986) 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 organizations (Hungarian Constitutional Court, 1991).

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 was determined to be unconstitutional. Therefore, a general and uniform personal identification mark (personal number) for unrestricted use was ruled to be unconstitutional (Hungarian Constitutional Court, 1991).

Ireland and the Common Travel Area

A particular complication of the UK National Identity Scheme is its likely effects on Ireland, particularly as a result of the Common Travel Area (CTA) that exists between the UK and Ireland.

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. Moreover, there are proposals for increasing the amount of "ad hoc immigration checks" on vehicles to target non-CTA nationals (Holder, 2008).

The rights to free travel (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 UK government has not signaled any intention to repeal these provisions.

Speaking in the House of Commons during the first debates about the Bill, 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. [20 December 2004: Column 1990][*]

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

> The principle of the Common Travel Area will be unchanged by the introduction of identity cards. All third country nationals who have

[*] All these are references to Hansard – "the edited verbatim report of proceedings in both Houses" – available at http://www.publications.parliament.uk/pa/pahansard.htm

> 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. [WA 204527]

This position was confirmed by the then-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" [WA 149931].

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, 2004)

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.

A report by the Northern Ireland Human Rights Commission (Holder, 2008) highlights particular problems that are likely to arise because of the specific arrangements found in Northern Ireland. In particular, British and Irish citizenship and identity rights are enshrined in the terms of the Belfast (Good Friday) Agreement. This recognizes:

> the birthright of all the people of Northern Ireland to identify themselves and be accepted as Irish or British, or both, as they may so choose and accordingly confirm that their right to hold both British and Irish citizenship is accepted by both Governments and would not be affected by any future change in the status of Northern Ireland. (Paragraph 1(vi) Belfast (Good Friday) Agreement)

It is estimated that 400,000 Irish passports have been issued to Northern Ireland residents in the last 10 years. Many of these people who see themselves as Irish are likely to be resistant to carry British Identity Cards and register on the British National Identity Register, particularly if the card identifies them as British Citizens and carries British symbols (see also Enterprise Privacy Group, 2008).

If many individuals choose not to carry a (British) identity card, there is an increased risk of discrimination amongst this community. If instead of a British Identity Card, they enrol for an Identification Card that will have "to be issued to EEA nationals or to British nationals not eligible for a travel document" (UKIPS, 2008g, Appendix 2) there is a risk that they will either be discriminated against, or the incorrect inference that they are ineligible for a travel document may be made. There may also be knock-on effects as to the utility of the identity card in Northern Ireland where a significant proportion of the population may choose not to have one (Holder, 2008).

It is perhaps unsurprising that the Government is reviewing the rules and operation of the Common Travel Area to explore how border security can be strengthened [WA 168405].

Italy

In Italy, citizens must agree to have their fingerprints taken and recorded in a database in order to be issued with a national identity card; however, a ministerial decree states that the association between the identity card and the fingerprint can be made only if expressly requested by the citizen (Decree, 2000).

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 ... 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 told that almost no one provides an imprint. Using fingerprints as the biometric identifier could provoke a negative response in Italy. (Standing Committee on Citizenship and Immigration, 2003)

A decree from the Council of Ministers in February 2004 called for a smart "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, 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 (eGovernment news, 2004c).

This smart card is not the same as the electronic identity 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: first, the process of standardizing the smart card without recourse to proprietary solutions; second, overcoming difficulties caused by the fragility of the microchips on the card; third, 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 centralized 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 identity 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 identity 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 drivers' license will be used instead. All three are valid identity documents. Drivers are warned that they should also carry their passport or identity cards with them at all times, as their license may be confiscated after a car accident, leaving them vulnerable to fines if they are stopped.

The costs of the regime are complicated. Many people are forced to buy an identity card, particularly if they do not have a passport or a driver's license. This applies particularly to younger and older people. Anyone losing their identity card must pay a fine of €30. In addition, in order to ensure possession of a card at all times, it is necessary to pay €30 for next-day service. As the card itself costs €30, losing a card can cost €90. The government froze the cost of the card for the first three years of operation.

According to reports, the compulsory identification 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 criticized 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 identity 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 allowing the policy to verify identities of individuals at soccer matches. (EDRIGram, 2005)

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

> The main rule is there will be few escapes available for people who cannot immediately present their ID. There is no right to an easygoing treatment, because it will in the end undermine the value of mandatory ID for law enforcement. (Openbaar Ministerie, 2005)

Under the law, the police can demand an identity card 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 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 identity of possible witnesses;
- identifying an unknown, new member in a group of known drug dealers;

- youths causing nuisance in public space;
- suspecting a person amongst a crowd to have started the fire, in the event of a fire;
- events such as football and demonstrations in case of riots or the threat of riots; and
- 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 (Anonymous, 2004).

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 identity card. Because she could not produce it, she received two fines; one for cutting the twigs, one for not showing her identity card. She burst out in rage and was given a third fine: for insulting an officer in the course of his duty (De Volksrant, 2005).

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 identity card when asked. During the following two months, the average rose to 5,300 individuals per month fined for being unable to produce their identity card. After three months in operation, 15,984 fines had been applied, generating €800,000 in revenue for the Government (Parool, 2005).

The law was due to be evaluated in 2008, including a consultation of all those with the power to demand identity cards, including the police, park-wardens and environment control staff. 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. (Ministerie van Justitie, 2005)

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.

In 2008 the Dutch government decided to go a step further and proposed a national biometric database. Under this proposal, all individuals over the age of six will be fingerprinted. The government argued that biometric information is already collected for passports and other purposes and rather than having all this information stored in separate databases they could be merged into a single national database. Access to the database would be restricted to cases where "serious crimes" have been committed (Houtekamer and Verkade, 2008).

Spain

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

In 2003 it was reported that the Spanish were also trialing a social security smart card, containing a microchip with national identity number, medical information. Information on the chip could be accessed by health professionals using a special reader. The project to develop and distribute 8 million cards was originally estimated at €55 million.

A Canadian Parliamentary Committee that traveled 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. (Standing Committee on Citizenship and Immigration, 2003, p. 25)

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 digitized photograph of the holder;
- A digitized image of the holder's handwritten signature; and
- All the data that is also printed on the card (date of birth, place of residence, etc.) (eGovernment news, 2004d).

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 €100 million over the next four years. The launch of a pilot system was delayed by one year and the first cards were issued in late 2007 (eGovernment news, 2004b).

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.

Although there is no compulsory card in Sweden yet, all individuals must have a personal number and a record on the national register and can choose to be issued a "certified identification card." Access to the register is tightly regulated. It has existed since the seventeenth century and, according to one report, was run by the Church until 1990.

There are plans to introduce identity cards with biometrics on them when the passports are updated, but plans keep on being delayed. 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 the card will not be linked to the register because of opposition on grounds of civil liberties (Home Affairs Committee, 2004).

In 2007 foreign nationals living in Sweden began to have problems being issued with identity cards. They were previously issued to foreign citizens by state-owned Svensk Kassaservice and by banks. In January 2007, however, it is reported that Svensk Kassaservice stopped issuing identity cards to people who are not Swedish citizens or who are not closely related to a Swedish citizen. Some banks have taken the same line. At the same time, many foreigners legally resident in Sweden, including EU citizens, say they have had their passports refused as identification documents when using credit cards, picking up parcels, and trying to prove their age (The Local, 2007).

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 (Myhr, 2008).

The European Union is working to minimize this variety. Through a number of initiatives, the EU is hoping to standardize cards of all types. All too often, this is effected with minimal debate and even less awareness regarding the proposed policies. EU/Schengen passport policy is a prime example of this practice. As discussed in Chapter 5, 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 International Civil Aviation Organization (ICAO) standards but also the EU requirements that were decided with minimal scrutiny.

EU driving license

The EU is working to standardize the 110 different types of driving licenses that are issued within Member States for Europe's 200 million license holders. The new license will involve a photograph on a smart card. The policy was supported quite strongly by the European Parliament (Billings, 2005), 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. (Kubosova, 2005)

Some significant disagreements led to a simpler license than what was originally envisaged. For example, some countries were keen to standardize policies on drivers aged over 65. The new standard will be rolled out over next twenty years with the first cards being issued in 2013 (BBC News, 2006a).

The Hague Programme's standardized identity

The most significant program will also be the most influential. In November 2004, the European Council adopted a new multiannual program, 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. (Council of the European Union, 2004)

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 harmonize 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" (Council of the European Union, 2004, p. 16). 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. (Council of the European Union, 2004, p. 17)

The European Commission then had the responsibility to develop an action plan; it identified ten priority policy areas (Communication from the Commission, 2005). 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. (Communication from the Commission, 2005)

Most of these decisions took 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 had the task of harmonizing and standardizing identity cards across Europe. It was all 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 standardized identity documents.

An initiative that began as an EU policy of ensuring a coherent standard for driving licenses has expanded incrementally to include visas, passports, and residence permits for third-country nationals (European Commission Justice and Home Affairs, 2009). It has now reached a point where it is likely that the EU will decide not only whether any given member state will have identity cards, but also their form and structure.

Identity cards 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 identity cards. Following a visit to the UK, they moved on to mainland Europe:

> The relationship between the individual and the state in Canada, the U.S., 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. (Standing Committee on Citizenship and Immigration, 2003, p. 32)

It is difficult to explain exactly why there are such cultural differences between European countries and those countries identified by the Canadians (Froomkin, 2009). 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 identity card. South Africa, which has a mix of legal systems including common law and Dutch civil law, does have a national identification system project (HANIS) replacing the earlier apartheid based pass laws and identification cards (Bowker and Star, 1999, ch 6; Breckenridge, 2008).

It could simply be an aspect of "our culture" to reject identity cards. The Australian (Clarke, 1987) and New Zealand public have rejected similar proposals outright. Following widespread criticism (Elliott, 2003), Canada abandoned its proposed biometric identity card system in early 2004, opting to focus its efforts on enhanced border security. National identity 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 identity cards, similar to the oft-quoted 80 percent in support of the UK card in 2004.

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 identity cards is symptomatic of the restraint expressed in both the unwritten and written constitutions of these countries. Wadham et al. (2006) express this in terms of the Diceyan notion of "residual liberty," that is "that everything the citizen does is legal unless explicitly made illegal by government" (p. 11).

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

Australia

Australia has an exceptional history with identity cards. The debate on proposals to introduce a card in the late 1980s provides significant insights into the whole issue of identity cards in every country (Wadham et al., 2006).

Identity cards are not alien to Australia. 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 (Rule, 1974).

Thirty years passed before the idea of a national identity card was again raised. Three reports, The Asprey Report of the Taxation Review Committee (1975), the Mathews Report on inflation and taxation (1975), and the Campbell Report on the Australian Financial Systems (1975), suggested that the efficiency of the Commonwealth Government could be increased and fraud better detected, through the use of an identity 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 (Graham, 1990).

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 (Clarke, 1992)) 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:

- **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, multipurpose 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 organizations to demand the card, to 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; and
- **Cross-notification:** Agencies using the system would be required to notify each other of changes to a person's details (Clarke, 1992).

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 percent of the public supported the scheme.

Not everyone was enthusiastic about the plan: a few journalists ran occasional stories raising questions about the proposal and the official Parliamentary opposition party was against 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 centers, civil liberties councils, academics, and advocates joined in opposition to the identity card plan and over the next two years, a strong intellectual foundation was developed (Davies, 2004).

Australian data protection expert Graham Greenleaf, one of the pioneers of the anti-identity 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. (Greenleaf, 1987)

Advocates pointed out that, although it is true that some civil law countries (such as Spain or France) have an identity 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 identification cards in other countries by creating a central information register that would touch many aspects of a person's life.

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 (Joint Select Committee, 1986). The fact that no common law country has accepted an identity 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 did 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 identity 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 identity card issue. In the opinion of the media, the identity card was simply not on the agenda as neither the Government nor the opposition raised the identity card as a key issue during the election campaign. The government was reelected and promptly resubmitted the identity card legislation.

Within weeks, a huge and well-organized movement was underway. Rallies were organized 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 (Davies, 2004).

On the night of 14 September 1987, 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 organized 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 percent 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 impositions rather than take the road of broadening national freedoms. (Australian Financial Review, 1987)

By mid-September, the Government was facing an internal crisis. The left of the party had broken ranks to oppose the card, while right wing members (particularly those in marginal seats) were expressing concern within caucus. Deputy Prime Minister Lionel Bowen urged the Party to tread with caution and suggested that a rethink might be necessary (Davies, 2004).

Within weeks, in the face of mass public protests, a party revolt, and civil disobedience, the government scrapped the identity 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 reintroducing the legislation but did not 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 toward a national identity system.

Australia is imposing basic biometrics into passports, but this will be limited to a digital photograph. It will result in an AU$19 increase in the cost of passports (Riley, 2005a). 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, drivers' licenses, and passports through a central data exchange hub (Riley, 2005b). The Government is opposed to the introduction of a single number to identify every Australian.

Around the time that the UK government introduced its Identity Cards Bill, the Australian government renewed its interest in an identity card for Australia. In January 2006, a formal enquiry was announced by Attorney General Philip Ruddock. This investigated whether Australia needed an identity card and how much it would cost. Shortly thereafter, however, the proposals were revised to take the form of a health and welfare services card, or “Access Card” (Wilson, 2008). As part of the preparation for these plans, Professor Alan Fells was given the task of reviewing other proposals and his visit to the UK coincided with the leaked e-mails and review of the Scheme that resulted in the Strategic Action Plan.

The Access Card was intended to be compulsory and near-universal although it would not be compulsory to carry it (Greenleaf, 2007). The roll-out of the card was intended to be rapid (1–3 years) which would lead to problems as there would then be a period of low enrolment until another peak coinciding with the expiry of the first cards.

These proposals were among the first policies dropped following the election of a new government, previously in opposition, in November 2007 (Arnold, 2007).

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 an identity system, it might instead be imposed upon Canadians because of U.S. 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 our own scanners, we can say we will take care of our own people with our own scanners. (Clark, 2003)

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 (Standing Committee on Citizenship and Immigration, 2003).

The Committee held a number of consultation sessions, met with local leaders, and traveled 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, overreliance on a single card, identity theft generated by the card, costs, and race relations.

The interim report concluded by stating that:

> 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. (Standing Committee on Citizenship and Immigration, 2003, p. 40)

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

At the same time, however, further policy changes were afoot in the realm of drivers' licenses. Every province in Canada is responsible for issuing drivers' licenses. Increasingly these licenses 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. And there is pressure from the U.S. to implement contact-less chips and collect further information including immigration status into the "Enhanced Drivers Licences" (EDLs) in order to permit their use for crossing the U.S. border.

In the case of George Bothwell, whose license 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 license from being entered on a database. He considered that this was not in accordance with his religious beliefs (with reference to the Book of Revelation 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. (Makin, 2003)

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 (CBC Online, 2003). Clearly, Bothwell was concerned with his right to privacy. According to Canadian jurisprudence:

> 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. [R *v* Dyment 1988 2 S.C.R. 417]

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 identity cards, the Canadian Government is moving to implement biometric passports. Although the national identity 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 that Canada will deploy facial recognition biometric technology on the Canadian passport, in accordance with international standards.

The Canadian Government justified this change, like most other countries, as necessary "to maintain our reputation as a First World nation" (Schick, 2004).

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. 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. (Privy Council Office, 2004, p. 53)

There are no plans to compile a searchable electronic database of the images or other data encoded on the chip although there are reports that the Passport Office has been considering the idea of screening applicants' photos against images of suspects on terrorist watch lists.

There are further developments under the Smart Border Agreement. This is an agreement with the U.S. Government on data-sharing and common standards between the two countries at border points. The "Smart Border Declaration" (Foreign Affairs and Trade Canada, 2003) 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 identity initiative. The two countries continue to work on methods of sharing data and standardizing policies and technologies, including through the Western Hemisphere Travel Initiative.

United States

Although the United States has no national identity card, it is implementing a variety of schemes that share many of the attributes of identity cards. These include the "REAL ID" policy for Enhanced Driver's Licenses and the Transportation Worker Identification Credentials (TWIC). In addition, it has been a forerunner in recording face and fingerprint biometrics from foreign nationals entering the country.

REAL ID

Though Americans are generally opposed to identity cards and have rejected all prior proposals to implement such a system, in February 2005 the U.S. House of Representatives approved the REAL ID Act. It became law in May 2005 following unanimous approval in the Senate. 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 U.S. driver's licenses and for identification document security standards (Froomkin, 2009). The law requires the United States to deny driver's licenses to undocumented immigrants. This requirement is seen as moving the license into the realm of a de facto "national" identity card (Gates, 2008).

The first step lays the foundations by requiring that federal agencies refuse any driver's license that does not meet minimum document requirements and issuance standards, including verification of immigration status and federal antiterrorism standards. As a result, temporary residents in the U.S. will only get a driver's license that is valid until their authorized period of stay expires. For all other noncitizens, 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 U.S.-issued driver's licenses to board the planes on September 11; they had foreign passports that allowed them to board airplanes. Use of foreign passports to board airplanes would still be permitted under this provision. (American Immigration Lawyers Association, 2005)

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

The database that is generated under this regime will also be shared with Mexico and Canada. The 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 country.

In an interesting development, the state of Georgia has prohibited the use of fingerprints in driver's licenses. This followed concerns regarding identity theft and acknowledgment by the law enforcement community that the fingerprints were not being used for combating crime. The state assembly of Georgia responded by passing a law, by a wide majority, 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. (Georgia, 2005)

State-level opposition is strong. As of 2008, eleven State Congresses have enacted legislation that prohibited its government from implementing REAL ID. Another nine State Congresses have passed resolutions denouncing REAL ID. A further six Congresses have approved anti-REAL ID legislation in one chamber and eleven have introduced anti-REAL ID legislation (ACLU, 2009).

Implementation issues associated with complying with the Act mean that all 50 states have applied for extensions to the original implementation date of 11 May 2008, effectively extending the deadline to 31 December 2009 (although the states have until 11 October 2009 to request a further extension (Department for Homeland Security, 2008)).

After the 2008 elections, President Barack Obama appointed Janet Napolitano as the new Secretary of the Department of Homeland Security (DHS). When she was Governor for Arizona, Napolitano was critical of the REAL ID law and her state had passed anti-REAL ID legislation. There are emerging reports that she proposes to limit the deployment of the Act, though more to consider cost issues rather than on civil liberties grounds (Modine, 2009).

Transportation Worker Identification Credential (TWIC)

Transportation workers have been identified by the DHS as a particular class of individuals with special status in relation to transportation security. This arose in response to the Maritime Transportation Security Act of 2002 (MTSA). This Act requires the use of a biometric identification credential for those who need unescorted access to secure areas of maritime facilities and vessels. As a result, the process requires a security threat assessment before a TWIC card is issued. The applicant then submits fingerprint biometrics and a digital photograph. As such, "TWIC is a secure, verified credential that can be used in conjunction with the owner/operator's risk-based security program that is required in security regulations issued by the Coast Guard" (TWIC, 2009). These cards currently cost $132 and are valid for five years. They can also be used as valid state-issued identification documents for airport checkpoints.

There have been reports about initial enrolment problems associated with capturing fingerprint biometrics with between 4 percent and 8 percent failure to acquire rates being reported. In addition there are issues of integrating the TWIC cards with existing infrastructures. Full roll-out and evaluation of the effectiveness of TWIC has not yet been undertaken although 1 million workers were enrolled by March 2009 (Congress Daily, 2009).

Biometric border controls for foreign nationals

Since 30 September 2004, all visitors to the United States have been fingerprinted and had a photograph taken at the border. These measures are part of a huge 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 U.S. Visitor and Immigration Status Indication Technology (U.S. VISIT) collects and retains biographic, travel, and biometric information on all visitors, except Canadians applying for admission to the United States as B-1/B-2 visitors for business or pleasure and those specifically exempted. The purpose of this collection is to identify people who are believed to potentially pose a threat to the security of the U.S., are known or believed to have violated the terms of their admission to the U.S., or who are wanted in connection with a criminal act in the U.S. 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."

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

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, treaties or regulations and assisting other Federal agencies to protect national security and carry out other Federal missions. (Department of Homeland Security, 2003)

This information will then be shared with other government departments and used in other surveillance programs. The U.S. 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.

The Government Accountability Office (GAO) assessed U.S. 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. (Government Accountability Office, 2004)

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 U.S. Government has commissioned a $15 billion contract to fully develop U.S. VISIT into a system that creates detailed dossiers on all visitors to the U.S. (even though DHS had originally budgeted $7.2 billion).

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. (Lichtblau and Markoff, 2004)

In its Privacy Impact Assessment, the DHS has contended that U.S. VISIT actually protects the privacy of foreigners. When U.S. VISIT was first put into operation, however, there were no rights of redress for individuals who faced any sort of adverse consequences. 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. This found that a security risk assessment had not yet taken place and that the privacy impact assessment was lacking. The problems arose particularly because U.S. VISIT is made up of various preexisting systems, operated in different ways by various DHS organizational components. The GAO found conflicting protections under the Privacy Act for information that came from a variety of sources, arising from the fact that U.S. 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." This was considered to be symptomatic of the wider problems with U.S. 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 nonmatch rate for fingerprinting can be extremely high – up to 36 percent. With 300 million visitors to the U.S. every year, the potential for mass error increases, yet little attention had been paid to these issues.

From 29 November 2007 the DHS has begun collecting ten fingerprints from international visitors at selected locations, with the intention that this will become policy at all points of entry. This extension comes despite a GAO report that found "security control weaknesses that place sensitive and personally identifiable information at increased risk of unauthorized and possibly undetected disclosure and modification, misuse and destruction" (Government Accountability Office, 2007).

The GAO also reports problems with the methodology used to match records of foreign nationals leaving the country with prior arrivals data (Government Accountability Office, 2008a).

Identity cards in other countries

China

Since 1985 the Chinese Government has issued an identity card to every citizen. This card originally held relatively simple information, including nationality, birth date, identification 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 identity 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. (Chen, 2003)

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 (Best, 2003), 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 in any case they doubted the reliability of the technology. According to an official at the Chinese National Registration Centre:

> Such an effort to introduce biometrics, [given] the huge quantity (of cardholders), [it] is not feasible to start. (Balaban, 2003)

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 and verified on-line (Chinaview, 2008).

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, "our security officials already have all the information about us, anyway, so this is not a big change" (Chen, 2003).

From 2004 the Government began issuing a "second generation" mandatory identity card involving contact-less chips (Brown, 2008). 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 (People's Daily, 2004).

Hong Kong

Hong Kong residents have carried identity cards since 1949. In 2002, the Government introduced a new card that would include a smart card, the Hong Kong Smart ID card (HKID) (Bailey and Caidi, 2005). These are being deployed as part of a seven-year plan costing $400 million. The territory-wide card replacement exercise was completed on 31 March 2007.

The new card contains basic information on the individual, a fingerprint image, and an identity number. The data are stored only on the card, not in a government database, but the legal regime behind the card allows the unrestricted use of identification numbers, thus still permitting the profiling of activities of individuals across the public sector (Greenleaf, 2002). The Hong Kong Privacy Commissioner's smart card Code does provide limited controls on the private sector use of the number.

The card system was designed from the outset as a multiuse card, with few limits and safeguards on its uses (Greenleaf, 2008). 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 nonimmigration related applications will be kept at back-end computer systems of the concerned government departments. None of the proposed nonimmigration 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. (Yau, 2002)

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 and posted the Privacy Impact Assessment for smart cards on its website. As the card is designed for multiple purposes, there is nothing restricting the Government from placing this information back on the policy agenda.

India

India has recently announced plans to implement biometric identity cards (Mehmood, 2008). A group of Indian ministers has approved the establishment of a Unique Identity Authority that will issue unique identity numbers to all citizens from 2010. This identifier would be a permanent identifier from birth to death, obviating the need for multiple documentary proofs. The roll-out will begin with all voters on the current electoral roll and will roll-out to include under-18s who are not part of the voter lists. In due course it is intended that photographs and biometrics will be added to the register (The Hindu, 2008).

In a similar manner to the UK proposals, it is intended that the biometrics will be stored in a central database (Espiner, 2008).

Japan

The Government of Japan approved the 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 known as "Juki Net." In essence, Juki Net is a network of registries, each run by local governments (Ogasawara, 2008).

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 (CardTechnology.com, 2004), 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 (Kallender, 2005). 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 (The Sydney Morning Herald, 2005). 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 (InfoWorld, 2005).

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 that was decided on 30 May 2005, the court in Ishikawa prefecture ruled that individuals may not be required to pass 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 favor of the system. Similar lawsuits have been filed in 13 different courts across Japan, challenging the collection of data for Juki Net. The confusion has yet to subside and according to some reports, the system is hardly used (Ogasawara, 2008).

Malaysia

Malaysia has long had a national identity card, but in 2001 moved toward a smart card scheme to replace both the older identity card and the driving license. 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 (Unisys, 2009). However, banks have dissuaded customers from using the card for banking purposes (New Straits Times, 2004). The chip on the card originally had 32k of memory storage, but the next generation card consists of a 64k chip, which permits the storage of multiple certificates, issued for specific government services and can run over 30 applications.

The card is issued at age 12 and reissued at age 18. Children under age 12 are issued with a "MyKid" card which currently does not contain a biometric, although the Government has considered the collection of biometrics from new-borns (Oates, 2005). There is now also an “iKad,” an identity card for foreigners.

Malaysia recognizes 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:

> A lot of governments including the U.S. 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. (Knight, 2001)

In October 2007, it was announced that paperless applications for international passports would be accepted by simply submitting a thumbprint and passport-sized photograph as the remaining information for the passport could be verified from the National Registration Department (The Star Online, 2007).

Middle East

Throughout the Middle East, governments are introducing identity cards, with Oman, UAE, Saudi Arabia, and Israel in the process of issuing “smart” identity cards. In so doing, they are coming across issues of identity exclusion (BahaiRights.org, 2008; Carr, 2009).

Oman was one of the first countries in the region to have a card programmed. The cards will store a single fingerprint and the police will be supplied with fingerprint readers to verify the cards (Balaban, 2004). 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 digital certificates and digital signatures. Interestingly, information held on the card cannot be released to all government agencies, or to the private sector.

In 2006 the United Arab Emirates (UAE) created a single, national identity card. This included fingerprint biometrics and smart card capabilities such as digital signature and authentication certificates. Its use is managed by the Emirates Identity Authority (EIDA) (Karake-Shalhoub, 2008). Registration is currently open for UAE nationals, Gulf Cooperation Council citizens working or residing in the UAE, expatriate government staff, and professionals in the private sector. The EIDA has announced a deadline of

31 December 2008 for all of the above categories. The UAE is also a forerunner in the use of iris biometrics for border control purposes, where the technology is used to screen all individuals who require a visa to enter the country against a watch-list. An estimated 10 billion real-time comparisons are performed at the border crossing each day (Kabatoff and Daugman, 2008).

Philippines

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

One plan involved requiring Muslims in Manila to carry an identity 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. Some sections of the Muslim community may have supported such a plan as a reaction to the constant harassment Manila Muslims have had to endure from police in their hunt for members of Abu Sayyaf.

An earlier plan attempted to establish a national identity 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 authorize 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, 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. (Hearing, 1998)

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 identity card, one of the main arguments for such a system usually being its benefit in countering terrorism. Skeptics 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 identity card bill.

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 counterterrorist 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. (Privacy International, 2005)

Besides the biometric data in the form of thumbprint templates and facial biometrics 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.

After a terrorist attack in February 2005, plans were reintroduced for a national identity 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 of civil liberties. When terrorists attack, that's when civil liberties are curtailed. (Guinto, 2005)

Although the exact details of the card remain to be known, it is believed 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 issued from 1 July 2005. In accordance with a 1997 Household Registration Law, these new cards include a fingerprint of all citizens over the age of 14. Premier Frank Hsieh argued that the program 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. (Engbarth, 2005b)

The fingerprinting program 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 9,000 fingerprint scanners at an estimated cost of NT$500 million (Engbarth, 2005c).

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. (Engbarth, 2005c)

The Vice President was also concerned that the adoption of a fingerprinting program 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 hundred human rights groups formed to oppose the program. The ad hoc "Movement to Refuse Fingerprinting" included as members the Taipei Bar Association and the Judicial Reform Foundation. Supporters were planning to apply for identity cards but would refuse to be fingerprinted. They would then lodge formal complaints with their local governments if they are not issued with a card.

Opposition parties claimed that the majority of Taiwanese supported the fingerprinting program. According to one party leader, 70 percent of respondents to polls agreed with the program (Engbarth, 2005b).

In June 2005, the Council of Grand Justices issued a temporary injunction to halt the program. This was the first time that the Council had used this power (Engbarth, 2005a). 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.

In 2008 the city of Taipei decided to scrap all the fingerprints it had collected between 2003 and 2005, after presuming that the system would not ever be operational again. Though it had collected the fingerprints of more than 700,000 citizens, the hard drives were "cut and smashed." According to the City Government, the biometric data was scrapped "mainly in response to requests by the public, aiming at preventing possible leaks of personal data" (China Post News, 2008).

Another interesting innovation occurred in 2008 when the Government decided to ensure that Taiwan's identity card numbers will not have more than one occurrence of the number "4." In Taiwan the number "4" is believed to bring bad luck because its pronunciation resembles the word "death." The Government had to previously stop issuing identity cards ending in 4 (Monsters and Critics, 2008).

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 the provincial and district levels (Ramasoota, 1998).

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 identity cards in January 2004, it announced that the first major batch of the cards would be issued to citizens in the three provinces of Patani, 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 a 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. The government claims to be on track for issuing cards to its 64 million citizens.

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 and 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 proposed to create a DNA database of all suspected militants in the region and of all teachers at private Islamic schools. Both the Thai Law Society and the National Human Rights Commission have expressed concerns and pointed out that the collection of DNA samples must be on a voluntary basis.

From 1 July 2005, individuals over the age of 14 applying for new cards would have to submit a full set of fingerprints when applying (Lin, 2005).

Disentangling identity cards from identity policies

It is all too easy to suggest that because many countries have identity cards there is a commonality to their identity policies, a commonality that implies that identity cards are "an idea whose time has come" (Blair, 2005). As the examples in this chapter have shown, this form of argument is fundamentally flawed: the existence of an identity card in a particular country gives no indication as to the kind of identity policy in that country and no indication as to whether these experiences can be applied in another country (cf Home Affairs Committee, 2004 §38). Instead, it is necessary to disentangle identity cards from a broader understanding of the identity policies in these different countries.

For example, in many cases, there was limited, if any, discussion of the identity policies underlying the identity schemes in existence. Many identity systems have been inherited from prior regimes of a completely different kind: identity cards under Franco in Spain, registration by a Nazi Government, national identity 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 the United Kingdom. In a significant number of cases, identity cards have been implemented by decree rather than through a national law, thus avoiding the national legislative process. This was the chosen method in Spain, Greece, Italy, the Philippines, and Thailand.

Where a debate about an identity policy does occur, there is usually initial broad support for identity cards, support that ebbs away when the flaws of the system are seen, the penalties of noncompliance are noticed, costs are disclosed and reviewed, and the implications are considered in detail (Davies, 2004; Wadham et al., 2006).

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 identity cards, was compelled to remove this by its national regulator. In Italy, officials have stated that, although Italians like their identity cards, the implementation of a fingerprint biometric would provoke a negative response.

Putting aside the issue of acceptance or rejection of identity cards, it is increasingly clear that not all systems are built equally. That is, there are significant variations in underlying national identity policies even though there are common instances of an “identity card” across countries. 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. Some have considered and yet rejected biometrics. Registration processes vary from registering at police stations to registering at banks; from requiring the presence of a live witness to the submission of a photograph signed by a referee; from the central storage of biometrics to distributed systems that delete the biometric once a card has been issued.

The reasons for this variety are largely attributable to national legal culture. The fact that a country has a national identity card does not mean that its populace supports all forms of identity systems. Identity 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 driver’s licenses, China has abandoned biometrics and Taiwan came close to declaring its fingerprinting program as unconstitutional.

Another interesting variation exists in relation to the nature of any “national identification number” used. Some countries use a single identification number for all purposes; others issue sector-specific numbers.

In some cases, specific legislation explicitly prevent the issuance of single identification numbers, while in others, methods are used to create sector-specific numbers that can only be (re)linked cryptographically (Otjacques et al., 2007).

The form of the number varies as well. In some cases, the form of the number has particular semantic properties: in Cyprus a prefix is used to distinguish Cypriots from non-Cypriots, Malta has a different structure of the number for Maltese citizens and foreigners. The Swedish "personnummer" includes the person's date of birth and, until recently, the county of their birth. Finally, the ninth digit in the number is odd for males and even for females. In the UK, in contrast, draft secondary legislation suggests that the National Identity Registration Number (NIRNo) will be designed to prevent the derivation of individuals' characteristics. According to the UK Government:

> By reading the number alone without other information, it will not be possible to deduce any other personal information about the individual – for example, this means that the number cannot be designed in such a way as to impart information about an individual's age, gender or nationality.

and

> If reading any such number along with another such number and no other information, it will not be possible to deduce any connection between the individuals to whom they have been allocated, other than that they both are registered on the National Identity Register. (UKIPS, 2008c)

The review of the practices of other countries reveals further insights into the issues surrounding identity policies. For example, the experience in Japan with the weak security surrounding the Juki Net highlights the risks to networking and creating a central registry. The Malaysian MyKad experience has resulted in banks advising that the cards should not be used to their full capabilities to access ATMs (cf BBC News, 2009b). Hong Kong conducted a Privacy Impact Assessment before moving forward with its card and rejected the implementation of a central database. Germany also deletes registration information from central stores when they are no longer needed and data are only collected locally. A number of countries do not have onerous enrolment procedures, reducing costs and also minimizing the inconvenience for individuals. Some countries restrict the use of identification numbers, Taiwan going so far as to try to gain acceptance for the numbers by adhering to local superstitions by minimizing the use of the number "4." 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 functionality offered as part of the national identity policy, whether in the form of digital certificates as found in the Belgian e-ID card (De Cock et al., 2008; Van Alsenoy and De Cock, 2008), or various applications found on MyKad or extra data and uses such as medical data proposed to be held on the Spanish card, again reveal differing legal and cultural attitudes underlying the implementation of the identity policy.

While countries differ on detailed issues, this review has shown that there is no natural design for an identity scheme and that the development of identity assurance mechanisms are as amenable to social (political, popular, legal) influence as they are to any notion of the inevitability of technological "progress" or modernization in any particular direction.

It also highlights the important role that the sponsoring department can play in the shape of the eventual scheme (Whitley and Hosein, 2008). Thus, once the UK and French proposals are tied to the Home Office and Interior Ministry the other policy agendas of these departments are likely to play significant roles in shaping the proposals brought forward before parliament. For example, the UK Home Office and the French Interior Ministry also have responsibility for crime prevention, policing, passports, and immigration. This makes certain decisions, like the inclusion of fingerprints into the register more understandable. They are no more, and more likely much less, effective than other biometrics for tying a person to a particular identity but have an opportunity to link the identity policy to the other policy agendas of the sponsoring department. Thus, in the UK, in an e-mail to those who had signed a petition against the introduction of identity cards, the then-Prime Minister Tony Blair repeated an earlier claim about the benefits of the scheme (Home Office, 2005d p. 3) by stating that:

> The National Identity Register will help police bring those guilty of serious crimes to justice. They will be able, for example, to compare the fingerprints found at the scene of some 900,000 unsolved crimes against the information held on the register. (Blair, 2007)

Most if not all countries are dealing with the issue of introducing or updating their identity policies, whether in the form of a card, an e-government initiative, or a policing initiative. As such, many of the issues associated with technologically-leveraged identity policies may arise in many countries. Enrolment challenges, conflicting costs estimates, technology failures, problems of public confidence, and the need for safeguards may yet be universal issues. As the Canadian Parliamentary committee's interim report concluded, changes in identity policy include transformations in the relationship between the individual and the state, the need to consider data protection and privacy issues, the worry about function creep and expansive use of the identity policy beyond its original scope, challenges in the use of advanced technology, confusion over the use of a single token or multiple systems, problems introduced by the "new solution," dynamics around costs and governance, and issues regarding social cohesion and race relations.

Thus even if identity cards are untangled from identity policies, there are still many generalized issues that the effective introduction of such policies need to address, revealing the limitations of existing policy analysis and policy process for the study of technologically-leveraged policies.

CHAPTER 3

The life cycle of identity policy in the United Kingdom

There are many stages to the life cycle of any policy and identity policy in the UK is no different. There are questions about when the approach to the identity policy arose and in response to which problems. There are the details of the policy's deliberative process, its eventual approval, its deployment, and enforcement. As this chapter demonstrates, the story of the UK identity policy became increasingly personalized moving away from any neutral, evidence-based norm that policy-making might be intended to follow. Each stage in the life cycle of a policy provides opportunities for the policy to be deflected or translated to address other stakeholders or policy agendas. Nevertheless perhaps the most surprising feature of this case is the way the policy has doggedly tried to keep to a simple narrative of problem, policy, and implementation.

The chapter begins by reviewing the two identity policies introduced in the First and Second World Wars, before assessing the background to the current legislation. Next the chapter outlines the Parliamentary passage of the proposals as the Identity Cards Act (the Act) became law in 2006. It then presents a series of further key events that have influenced the on-going life cycle of policy as it moves toward implementation.

Two wartime cards

Identity policy is not new in the United Kingdom, potentially being traceable back to the Doomsday book that in 1086 registered all the possessions of the new King of England upon the landing of William the Conqueror. In fact, the current National Identity Scheme (the Scheme) is the latest incarnation of a national identity register that has appeared and disappeared in the United Kingdom since the First World War. However, there is something relatively unique about the UK amongst all of its European partners, in that until recently it did not have a sustainable identity policy involving a national identity card.

Reflecting on the experiences associated with the introduction and termination of these wartime cards will help place the reaction to the current Scheme in a historical context and may explain some of the popular and administrative responses to the Scheme's implementation.

According to Agar (2005) before the introduction of identity cards during the First World War, it was possible to find personal information listed on eighteen disjointed, localized registers. This lack of clear data about the UK population led to the development of the first National Registration Bill during the First World War. In particular, there was a perceived need to determine whether the UK could draw on a "patriotic population" that was sufficiently large to support voluntarily both the military and industrial requirements of the country in wartime. If the UK did not, then it would need to consider conscription as an alternative (Elliot, 2006).

As a result, rather than simply undertaking a census of the adult population, the wartime government proposed a National Register listing the adult population aged between 15 and 65, including their employment details and requiring the State to be kept informed if they changed their address. The implementation of the Register was based in the General Register Office for England and Wales and the General Register Office for Scotland.

At an administrative level, the smooth running of the Register would directly influence the reputation and effectiveness of the proposals and raised questions about the administrative processes associated with their implementation. For example, allocating every adult a unique identification number, which could be used across the regions, required the creation of a central index. Another concern faced by the Register Offices was their classification of the employment categories of the individuals, as this could determine who was to be exempted from military recruitment and hence was potentially a matter of life and death, a decision that these civil servants had previously never faced (Elliot, 2006).

Once the register was in place, the War Cabinet was soon informed of the number of men in England and Wales still available for national service: 1,413,900. As Agar (2005) notes, once this figure was determined, political interest in National Registration (and the associated identity cards) waned.

During the Second World War, a second Register was introduced but this time it was given a variety of purposes: coordinating national service, national security, and the administration of rationing (Thompson, 2008).

In particular, it was the linking of the identity card with rationing that made it a more significant part of public life during the Second World War and beyond, as the absence of an identity card meant no legal access to food.

This scheme continued beyond the end of the Second World War, until Clarence Willcock was stopped by a policeman in 1950 and asked to present his identity card. He challenged this request and, in court, argued that as a piece of wartime legislation the carrying of an identity card should no longer be enforced in peacetime. Though the court reluctantly agreed that the card was legal at the time, the court also argued that a card could antagonize the relationship between the citizenry and the police. In 1952 the scheme was scrapped.

Whilst the 1939 Act had three purposes for the register, by 1950 thirty-nine government agencies were using the records. Although keeping track of potential bigamists was suggested as one of the additional benefits of the Scheme, Agar (2005) argues that this problem was not a particularly prevalent issue at the time.

The new Bills and the Identity Cards Act 2006

Ever since the Second World War Identity Cards were scrapped, various Home Secretaries are believed to have considered reintroducing some form of national identity document, but each of these proposals had been abandoned after the amassed expertise in the Civil Service had been presented to them. The current Scheme has its origins in proposals for "entitlement cards" that were first proposed by the then-Home Secretary David Blunkett in 2002 (Office of Government Commerce, 2003).

In the consultation document for the proposals (Home Office, 2002) the core design of the Scheme is presented. It would entail

- establishing a secure database which could potentially hold core personal information about everyone who is lawfully resident in the UK;
- implementing rigorous procedures to ensure that the information held on the database was accurate and protected from unauthorized access;
- linking the core personal information to other databases which held service entitlement information. This would allow service providers to deliver their services more efficiently and effectively and in a way which made it simpler for people to gain access to the services to which they were entitled; and
- issuing entitlement cards to everyone on the central database so they had a convenient way to access services (Home Office, 2002, §1.3).

In the consultation, the government sought the public's opinion on "the principle of establishing an entitlement card scheme as a more efficient and convenient way of providing services, tackling illegal immigration and illegal working and combating identity fraud" (Home Office, 2002, §P1), whether the card should be universal or targeted (§P2) and whether they should be voluntary or compulsory (§P3). Views were also sought about practical issues associated with the cards including the content and scope of any associated legislation (§P5), incentives and sanctions to "help ensure universal coverage" (§P6), the form of any personal identification number associated with the scheme (§P7), and the potential development of a national population register (§P8).

As the Office of Government Commerce (OGC) Gateway 0 Review (2003), undertaken in June 2003, shows the Home Secretary saw the introduction of Entitlement/Identity cards as essential to reduce identity fraud and improve our immigration controls (Office of Government Commerce, 2003, p. 3).

The review also noted that

> The scope and objectives of an Entitlement Card scheme must be precisely defined at a very early stage and all opportunities and desires to change or grow these requirements must be resisted;
>
> The implementation risks must be minimized through the optimum use of existing capabilities, skills and expertise; and
>
> Entitlement Cards should represent a program of projects, as the lowest risk implementation strategy will involve building on existing operations and future initiatives in the Driver and Vehicle Licensing Agency, Passport Service, Immigration and Nationality Directorate and Citizens Information Project and possibly other areas as well (Office of Government Commerce, 2003).

The report recommended that the Entitlement Card program be managed by a single empowered organization. A second OGC Review was undertaken in January 2004 (Office of Government Commerce, 2004). It noted that

> The combination of greater mobility and advancing technology is making it increasingly difficult to protect and authenticate people's identity. As a result British citizens are facing growing threats to their security and prosperity from illegal migration and working, organized crime and terrorism, identity theft and fraud and fraudulent access to public services. (Office of Government Commerce, 2004)

The review also noted that biometric passports were already being developed in the UK and that the U.S. would shortly require a biometric from foreign nationals entering the U.S. It understood that the Government's plans were to build a compulsory Identity Card Scheme in an incremental fashion to "protect people's true identity against fraud and to enable them to prove their identity more easily without unnecessary intrusion by the State." This would involve establishing a National Identity Register (the Register), proceeding toward more secure passports and driving licenses based on biometric technology with personalized, specific identifiers, or a stand-alone identity card for those who do not need a passport or driving license (Office of Government Commerce, 2004).

The OGC Review made a number of detailed recommendations including the continued requirement "to recognise the need of partner Departments to make a success of their own businesses alongside their participation in the Identity Cards scheme" and the requirement "to identify the preferred solutions to each of the main technical issues by the start of the procurement phase."

The Review also urged that "new costings and sensitivity analyses be prepared, together with financial modelling, alongside the work on structures, standards, deliverables and technical issues discussed above" and stated that the "CIP facility will need to be ready in time and to the required standard if it is to be used to support the Identity Card programme" (Office of Government Commerce, 2004).

On 29 November 2004, following a two-and-a-half-year gestation and a name change from *entitlement cards* to *identity cards*, the Government introduced and published its Identity Cards Bill. The Bill outlined an identity policy that was very similar to that envisaged in the original consultation document and the OGC Reviews, based on a central register and the use of biometrics. These components are discussed in more detail in the next chapter.

The Bill was debated (in Second Reading) in the Commons on 20 December 2004 and was then considered in Committee in mid-January 2005. For details of how a Bill becomes law, see House of Lords (2008). The Bill reached Third Reading on 10 February 2005 when it passed by 224 votes to 64. The Second Reading debate in the House of Lords took place on 21 March 2005, after which the Bill was suspended pending the General Election.

During the 2005 election, the Labour Party included proposals for identity cards in its election manifesto. Labour won the election, although with a much weakened majority in the House of Commons. A revised version of the Bill was promptly presented to the House of Commons on 25 May 2005 as one of the main items on the new policy agenda.

It is important to also note a few more political dynamics. In 2003 a new nongovernmental organization established itself to fight the Government's policy, called NO2ID (www.no2id.org). In the ensuing years it became significantly larger with greater resources to provide briefings to Parliamentarians. Other human rights groups also emerged as opponents to the Scheme and these groups played a significant part in raising public and political interest in the issue.

A second and very significant development was that after the election, the leader of the opposition party, the Conservative Party, resigned. Michael Howard had been a strong proponent of identity cards when the Conservative Party was in power and as Home Secretary he had also considered a national identity card in the mid-1990s. So when the Bill went through the House of Commons in late 2004 and in early 2005, the opposition party did not offer a concerted effort to fight the Bill. In a famous moment, when the Bill was receiving its Second Reading in December 2004, many Conservative MPs were nowhere to be found and the explanation that emerged was that they had all "gone Christmas shopping" (Kite and Freinberg, 2004).

When Mr Howard announced that he was stepping down as leader of the Conservative Party, other members of the party began voicing stronger opposition to the Bill. The party's leadership contest ended up between two strong opponents to the Bill, David Cameron (who, as a member of the Home Affairs Committee that had looked into the Bill, had previously spoken about his unhappiness with the policy, particularly the way it changed the relationship between the citizen and the State (Cameron, 2004)) and David Davis (who was appointed as the lead member of the Opposition on the Bill in the Commons). With Cameron's appointment as Party Leader the Conservative Party position on the Bill became stronger, particularly on practical grounds. Meanwhile, the third party of British politics, the Liberal Democrats, consistently held strong beliefs that the Bill was contrary to civil liberties.

The LSE Identity Project Report

As the first version of the Bill was being considered by Parliament it became apparent that there was very little deliberation about the details of a Bill that could fundamentally alter the relationship between the citizen and the State. Moreover, it became clear that many of the government's claims about the science and technology behind the Scheme (i.e. the design of the Register and the use of biometrics for verification purposes) were being accepted at face value with the prevailing discourse presented to the media being one of *progress* (Gamson and Modigliani, 1989). For example, in June 2005 the then-Prime Minister, Tony Blair, said that identity cards were "an idea whose time has come" (Daily Telegraph, 2005). Sometime later, Tony Blair (2006) associated identity cards with modernity, former Home Secretary John Reid (2007) related identity cards with civilization and Home Office minister Liam Byrne (2007) argued that the Scheme could become "another great British institution."

From an academic perspective this view of the success and benefits of the Scheme would appear to reduce the intimate intertwining of society and technology to a simple cause-and-effect sequence. The deterministic focus on technology's effect on society neglects the many ways in which people can affect the role that technology plays in society. Politically, such a view seems "to encourage a passive attitude to an enormously important part of our lives" (MacKenzie and Wajcman, 1999, pp. xiv–xv).

Inspired by this insight, a group of researchers based at the London School of Economics and Political Science (LSE) decided to undertake research into the government's proposals. The intention behind this work was to enhance the policy debate. As Giandomenico Majone notes:

> Good policy analysis is more than data analysis or a modelling exercise; it also provides standards of argument and an intellectual structure for public discourse. Even when its conclusions are not accepted, its categories and language, its criticism of traditional approaches, and its advocacy of new ideas affect – even condition – the policy debate. (Majone, 1989, p. 7)

The LSE "Identity Project" decided to present a thorough analysis of the government's proposed identity policy, taking into consideration both issues of principle and concerns about practicalities.

The LSE team released an *Interim Report* (LSE Identity Project, 2005a) in March 2005 to coincide with the Second Reading debate in the House of Lords. The purpose of this report was to present many points of views on aspects of the Scheme, to begin to inform the debate, and to seek feedback on the analysis presented.

On 27 June 2005 the LSE Identity Project released its *Main Report* (LSE Identity Project, 2005c), the day before Parliament revisited the Bill upon the reopening of Parliament after the general election. This report was over 300 pages long and concluded that while an identity card system could offer some public interest and commercial sector benefits, there were a number of areas of major concern with the Government's plans. These are summarized in Table 3.1.

Table 3.1 Key conclusions of LSE Identity Project

Multiple purposes: The UK scheme has multiple rather general rationales, suggesting that it has been "gold-plated" to justify the high-tech scheme.

Will the technology work? No scheme on this scale has been undertaken anywhere in the world. Smaller and less ambitious schemes have encountered substantial technological and operational problems that are likely to be amplified in a large-scale national system. The use of biometrics creates particular concerns, because this technology has never been used at such a scale.

Is it legal? 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.

Security: The National Identity Register will create a very large data pool in one place that could be an enhanced risk in case of unauthorized accesses, hacking, or malfunctions.

Citizens' acceptance: An identity system that is well-accepted by citizens is likely to be far more successful in use than one that is controversial or raises privacy concerns.

Will ID cards benefit businesses? Compliance with the terms of the Identity Cards Bill will mean even small firms are likely to have to pay for specialist readers which, together with other requirements, will add to the administrative burdens firms face.

Shortly before the LSE *Main Report* was published, newspaper reports at the end of May 2005 suggested that the LSE analysis was indicating that the likely cost of identity cards could be of an order of £300 per person (BBC News, 2005b; Doward, 2005; Pascoe-Watson, 2005).

The government responded robustly to these reports, with Ministers stating that the likely costs of the card were nowhere near that presented by the draft LSE report (Adams, 2005). By the following week, press coverage was including details of the alternative Scheme being proposed by the LSE Report, which was likely to be less costly than the government's proposals (Harrison, 2005).

The Government's opposition to the LSE report escalated on 16 June 2005, when the then-Home Secretary (the head of the Home Office) went on the BBC Radio 4 Today program to describe the LSE's costings as "simply mad," saying that the reports were "completely wrong" and that the kinds of figures "that have been talked about in the media based on their briefings are total nonsense." He also accused the LSE of running "scare stories" (BBC News, 2005a). At this stage, the Government's plans were to have the first identity cards issued to UK citizens by the end of 2007 (Arnott, 2005).

Unsurprisingly, the Home Secretary's outburst received extensive media coverage raising public awareness of the cards considerably (Freeman, 2005; The Sun, 2005; Tempest, 2005; Whitley, 2009).

The Home Secretary acknowledged that the report had not been officially released and had not been seen by Home Office officials. The LSE had frequently sought to engage with the Home Office, offers which had repeatedly been turned down. The LSE Director Howard Davies told The Times

> The researchers involved have offered to discuss this work with the Home Office several times. Charles Clarke may not like the conclusions, but he has no basis to question the integrity of the LSE or those conducting the research. (Freeman, 2005)

As a result of the attacks on the integrity of the LSE as well as on the research itself, the launch of the LSE report was rescheduled to 27 June 2005 (the day before the Second Reading debate) so that LSE Director Howard Davies could introduce the launch of the report.

Speaking on 28 June 2005, the Home Secretary again attacked the LSE research, calling it "technically incompetent" and singling out one of the project mentors, Simon Davies, for being a "partisan" academic (Crace, 2005), a claim repeated by the Prime Minister in January 2006 (Davies, 2006).

The reason for Howard Davies's support for the LSE report became clear in a letter he wrote to the Times (Winnett, 2005). In it, he accused the Home Office of using "bullying and intimidation" in its attempt to suppress a study about identity cards. He had received an aggressive phone call from Sir John Gieve, Permanent Secretary at the Home Office (the chief civil servant responsible for that department), who was said to have been delivering a "political message." Howard Davies said that he was "genuinely shocked" by the experience. LSE Governors also claimed that the Home Office had tried to delay publication until after the House of Commons Second Reading debate. Lord Grabiner, chairman of the LSE governors added: "We don't take very kindly to interference with academic freedom. Also, we think the work was done independently and objectively and in the good academic tradition" (Winnett, 2005).

Howard Davies later wrote to a member of the House of Lords saying "we have had some extraordinary responses to our work from the government, who appear to think that they can deal with a Report from a group of academics from a University in the way they would a submission from the official opposition" [Quoted by Lord Phillips of Sudbury, 19 December 2005, Column 1552].

In late July 2005, the Home Office issued a response to the LSE "alternative blueprint" for an identity scheme (Home Office, 2005b) giving further details about the logic underlying its own proposals including the largely automated nature of the biographical enrolment check, the "common sense" underlying the approach of using a centralized database and the claim that the approach "complies with industry best practice." The Home Office response to the LSE report also suggested that the LSE's costings of the Government's plan had allocated between £500m and £1bn in marketing costs and questioned the validity of this amount. Responding to this analysis of the LSE's costings of the scheme's likely marketing costs, the LSE Identity Project pointed out that "the LSE report did not set out an estimate for marketing costs or indeed for any line item of that nature. Such a figure would, however, most likely be somewhat higher than the range suggested in HO's [Home Office's] response document" (LSE Identity Project, 2005b). Moreover, in the *Research Status Report* issued in January 2006 (LSE Identity Project, 2006c) the LSE Identity Project offered a possible explanation for the confusion: "Another report from another organization, Kable, included marketing costs within their estimates, following the example of a Home Office commissioned-study. Though we collaborated with Kable on the costings models used, even a superficial analysis of the two reports would note the absence of the £1bn line item from the LSE report" (LSE Identity Project 2006c, fn10).

Parliamentary progress of the Bill

Details of the Parliamentary debates about the revised Bill are given in Table 3.2. Even with Labour's reduced majority, the scrutiny of the Bill in the House of Commons was relatively limited. However, when the lower House approved the Bill in October 2005, it was then sent to the House of Lords where its passage became more problematic for the Government. In particular, in the Lords the Labour party was the minority party and faced effective, coordinated opposition from the other two main parties (Conservatives and Liberal Democrats).

In early 2006, the Lords approved a number of significant amendments to the Bill. These included a proposal that the Act only commence after a report on the costs and benefits of the Scheme had been delivered to Parliament, that citizens be offered a choice about whether their details be recorded on the Register when they are issued with designated documents, deleting a clause to ensure that the transition from a voluntary to compulsory system needed to be made by primary legislation and changes to the appointment and reporting line for the Scheme Commissioner. As the Bill had been modified by the upper House, it had to return to the lower House for further consideration.

When the Bill returned to the House of Commons, the Government continued to attack the LSE Identity Project's reports, focusing particularly on the question of the "marketing costs." The Home Office minister responsible for the Bill in the Commons Andy Burnham MP, wrote to members of the Parliamentary Labour Party repeating the claim that "The LSE also allocated an inflated £1billion marketing budget and assumed a much

Table 3.2 Parliamentary passage of the Identity Cards Bill after the May 2005

Date	House of Commons	House of Lords
25 May 2005	Introduction to House (First reading)	
28 June 2005	Second reading	
05 July–21 July 2005	Committee Stage	
18 October 2005	Remaining stages	
19 October 2005		First reading
31 October 2005		Second reading
15 November–19 December 2005		Committee stage
16 January–30 January 2006		Report stage
06 February 2006		Third reading
13 February 2006	Consideration of Lords' Amendments	
06 March 2006		Consideration of Commons' Amendments
13 March 2006	Consideration of Lords' Amendments	
15 March 2006		Consideration of Commons' Amendments
16 March 2006	Consideration of Lords' Amendments	
20 March 2006		Consideration of Commons' Amendments
21 March 2006	Consideration of Lords' Amendments	
28 March 2006		Consideration of Commons' Amendments
29 March 2006	Consideration of Lords' Amendments	
29 March 2006		Consideration of Commons' Amendments
29 March 2006	Consideration of Lords' Amendments	
30 March 2006	Royal Assent	

higher loss/theft ratio than is the case for existing documents. In that way the research generated headlines of the kind that read "£300 for an ID card" which some may say was the object of the exercise" (Burnham, 2006).

The Lords' amendments about the Scheme Commissioner were overturned in the House of Commons. The question of costs and commencement were addressed by an amendment introduced by Frank Dobson MP that was accepted by the Lords when the Bill returned there after its reconsideration by the lower House.

The issue of voluntary versus compulsory enrolment was more problematic and the Bill "ping ponged" between the two Houses on five occasions in February and March 2006 on the issue of linking the issuing of identity cards to the renewal of passports before a compromise amendment was accepted on 30 March 2006 (Whitaker, 2006). This amendment was proposed by the former Cabinet Secretary Lord Armstrong and offered the concession that, for a period until the next general election, a person could choose not to be issued with a card although obtaining a passport would remain conditional on biometric enrolment on the Register. The Bill received Royal Assent shortly thereafter and on 1 April 2006, a new agency – The Identity and Passport Service (IPS) – was created from the former Passport Agency. Chapter 7 examines the debates about compulsion and costs in more detail.

Identity Cards Scheme or the National Identity Scheme

Throughout the deliberations about the Act, the resulting Scheme was referred to as the Identity Cards Scheme and the requirement to report on costs is labeled as a "Report to Parliament about likely costs of ID cards scheme." The Act also, however, refers to the National Identity Scheme Commissioner, which suggests the National Identity Scheme might be something different from the Identity Cards Scheme.

This confusion is not helped when the first s.37 cost report ("about the likely costs of the ID card scheme") states that the Act "establishes in statute the framework for a National Identity Scheme" (UKIPS, 2006a). All later IPS reports use the language of the "National Identity Scheme." For example, the 2006 Strategic Plan states:

> The National Identity Scheme will be governed by the Identity Cards Act 2006, immigration legislation, the secondary legislation (regulations and orders) made under the Identity Cards Act 2006 and approved by Parliament, and other legislation (e.g. the Data Protection Act, etc.). (UKIPS, 2006b, §72)

The "immigration legislation" that is referred to is the UK Borders Act 2007, which had not been proposed at the time that the Identity Cards Bill was being debated. The same document states that:

> The National Identity Scheme is the term used to describe the Government's plans to improve the way that identity can be verified so

> as to provide greater convenience for individuals as well as improved protection for the public. It will provide a new way to do this – more securely, and more conveniently. It has three key elements that improve on current systems:
>
> - a single National Identity Register,
> - the recording of fingerprint biometrics,
> - the issue of biometric identity cards. (UKIPS, 2008c, §1.16)

Under the UK Borders Act 2007, "there will remain a separate system for issuing identity cards to foreign nationals by the UK Border Agency" (UKIPS, 2008c, §1.19). "At a later date the identity cards issued to foreign nationals will be designated as ID cards under the Identity Cards Act. From that point onwards identity details of foreign nationals will also be held on the National Identity Register together with the identity details of British and EEA nationals issued with identity cards" (§1.19).

This suggests, therefore, that until details of these identity cards issued to foreign nationals are entered onto the Register, they are not technically part of the National Identity Scheme. Furthermore, according to the Strategic Action Plan:

> Appointing a commissioner to oversee the operation of the National Identity Scheme is a key safeguard of the Identity Cards Act 2006. The Commissioner will be recruited by means of an open competition, which will begin significantly before the first ID card is issued. (UKIPS, 2006b, §74)

The first biometric identity cards for foreign nationals were issued in late 2008 but the recruitment process for the National Identity Scheme Commissioner did not begin until early 2009 and the Commissioner is due in post in mid-2009. The holders of these first cards will also not have any of the protections of the Scheme Charter, which sets out the rights and responsibilities of individuals, businesses and of the Government related to the Scheme, as this will only be published in the second half of 2009.

This suggests that there is still not yet a "National Identity Scheme" in operation in the UK despite some biometric identity "documents" having been issued. This point is reinforced by statements like: "The National Identity Scheme (NIS) is arriving over the next few years" (UKIPS, 2008e, p. 3) and "This document sets out how the Government *will* deliver the National Identity Scheme (NIS or "the Scheme"), how the Scheme *will* work and be operated" (UKIPS, 2008a, p. 6 emphasis added). However it is also contradicted by the statement in the Delivery Plan that "the first step in implementing the National Identity Scheme *has been* the introduction of fingerprint visas through the UKvisas Biometrics Programme, which is making a real impact overseas" (UKIPS, 2008a, p. 9 emphasis added).

Given this ambiguity, the Scheme referred to in this book refers to the more broadly defined National Identity Scheme.

Other key events

Although the Bill received Royal Assent in March 2006, since then there have been a number of key events that have shaped the development of the Scheme. As an understanding of these is needed for the later chapters, each of the key events is presented.

In this case, the period covers a number of "critical incidents" (Pettigrew, 1990) in the life of the Scheme. Each of these incidents reveals new data associated with the relationship under study and each can best be understood in relation to the previous events as a form of longitudinal case study (Milne and Culnan, 2002; Organization Science, 1990; Walsham, 2006).

Science and Technology Select Committee inquiry

The question of the government's use of scientific and technological advice in developing the proposals for identity cards formed a key part of a House of Commons Science and Technology Select Committee inquiry. The inquiry looked at three areas of government policy: the classification of illegal drugs, the use of MRI equipment, and the technologies supporting the Government's proposals for identity cards.

The inquiry into identity cards took place after the Bill had become law and received written and oral submissions from the Home Office as well as representatives from industry and academia (Science and Technology Select Committee, 2006).

Leaked e-mails and the Strategic Action Plan

On 9 July 2006 a leading Sunday Newspaper ran a front page headline story entitled "ID cards doomed" based on leaked e-mails sent between senior officials from the Office of Government Commerce and the Identity and Passport Service. These e-mails had been exchanged on 8 and 9 June 2006.

The first e-mail, from OGC Mission Critical Director David Foord, warned:

> even if everything went perfectly (which it will not) it is very debatable (given performance of Govt ICT projects) whether whatever TNIR [Temporary or Tactical National Identity Register] turns out to be (and that is a worry in itself) can be procured, delivered, tested and rolled out in just over two years and whether the resources exist within Govt and industry to run two overlapping procurements. What benchmark in the Home Office do we have that suggests that this is even remotely feasible?
>
> I conclude that we are setting ourselves up to fail. (The Sunday Times, 2006)

The response, from Peter Smith, Acting Commercial Director for the Identity and Passport Service indicated what was likely to happen next:

> The procurements we will (we hope) launch in the next few months – not the TNIR but things like APSS and contact centre – are all necessary (essential) to sustain IPS business as usual and we are designing the strategy so that they are all sensible and viable contracts in their own right EVEN IF the ID Card gets canned completely. So also less dependence on business case approval etc. (The Sunday Times, 2006)

Following these leaks the recently appointed Home Secretary John Reid delayed all aspects of the procurement process and ordered a full-scale review of the proposed Scheme. As a result of this review, a new Strategic Action Plan (UKIPS, 2006b) was released in December 2006 on the last day before the Christmas Parliamentary Recess. This proposed a redesign of the Scheme, for example by dropping the mandatory use of iris biometrics and reusing three existing government databases rather than designing a new National Identity Register from scratch.

Procurement and supplier short listing begins

In late October 2007, following a Pre-Qualification Questionnaire stage (which solicited 11 responses) IPS announced a long list of suppliers who would be invited to participate in a Competitive Dialogue with IPS, prior to seeking final tenders for the Framework Agreement. This “long list” consisted of eight suppliers: Accenture; BAE Systems; CSC; EDS; Fujitsu; IBM; Steria; and Thales.

The procurement approach is based around a "Framework Agreement" that will involve a small group of suppliers (the "Strategic Supplier Group" (SSG)) who will work with IPS to deliver capabilities for the Scheme. According to the NIS Strategic Supplier Framework Prospectus, the majority of components for the Scheme will be bought as managed services by running "mini-competitions" among members of the "Strategic Supplier Group" (UKIPS, 2007b). For example, two projects were described as having received approval at the time that the prospectus was issued:

> The replacement of core Application and Enrolment processes for passports and the provision of desktop infrastructure for IPS; and
>
> The replacement and upgrading of the existing systems for fingerprint matching and storage in connection with immigration and visa requirements and transition to the replacement service. (UKIPS, 2007b, p. 17)

Members of the SSG would therefore compete to implement these projects for IPS and the contracts for these systems were issued (to CSC and IBM respectively) in April 2009 (Collins, 2009b). Other projects that are envisaged include:

- Biometric recording, storage and matching needs, including the systems integration of new and existing services;
- Biometric support;
- Further development of Application and Enrolment solutions to meet future needs (which may include business process, people, systems, and premises);
- Data sharing services;
- Biographical Background Checking Services (for the purposes of confirming identity);
- Identity Checking Services;
- Production, Management, and Distribution of passports, ID Cards, and other products;
- Biometric Enrolment Services; and
- Other capabilities including entitlement checking services and associated case management services (UKIPS, 2007b).

However, in January 2008 two major companies (Accenture and BAE) withdrew from the Competitive Dialogue process (Palmer and Burns, 2008b) and in February 2008 Steria also withdrew from the process (Grant, 2008). This left only five suppliers in the Competitive Dialogue process and all five were appointed to the Strategic Supplier Group in May 2008 (UKIPS, 2008f).

Leaked plans

In January 2008, the lobby group NO2ID leaked what it claimed were updated plans for the Scheme, based on the outcomes of an Options Analysis process (NO2ID, 2008). According to this document, a "tactical solution" for implementing the Scheme was proposed, including targeting particular groups for early enrolment. These include those in trusted relationships, where it was claimed that there was a "strong narrative" for linking identity assurance, vetting and Criminal Records Bureau checks. Examples included airside transportation workers and young people (who could use them as identification when opening bank accounts or applying for student loans and accessing age-restricted locations such as bars and nightclubs). The analysis suggested a two-phase approach, with the targeted groups enrolled in the first half of 2009 and a "high level" approach for enrolment from 2012 onwards. The plans also suggested downplaying the role of biometric identifiers ("we should *eventually* work toward a Scheme including a *high proportion* of fingerprint enrolment" (emphasis added)).

HMRC data breach

Perhaps the most significant external event was the announcement by the Chancellor Alistair Darling, on 20 November 2007, that a data breach involving "personal data relating to child benefit" had arisen in Her Majesty's Revenue and Customs (HMRC) [20 November 2007, Column 1101–]. On 18 October 2007, in response to a request from the National Audit Office (NAO) for data in relation to payment of child benefit, a civil servant at HMRC sent a full copy of the data on two password-protected compact discs, using an obsolete version of compression software with weak encryption. The discs were sent using the HMRC's internal mail service, operated by TNT. The package was not recorded or registered and failed to arrive at the NAO. When the requested discs did not arrive, a further set of discs were sent, this time by recorded delivery. These did arrive. Senior management at HMRC was not told about the lost discs until 8 November 2007.

The discs, containing details of all child benefit recipients, records for 25 million individuals and 7.25 million families, have still not been recovered. The records included the names of recipients and the names of their children as well as address details and dates of birth, child benefit numbers, national insurance numbers and, where relevant, bank or building society account details.

Following this statement, the Chancellor appointed Kieran Poynter, Chairman and Senior Partner of PricewaterhouseCoopers LLP to review the circumstances surrounding the data breach and to make recommendations on urgent and longer-term changes required to ensure such breaches do not recur. Poynter issued a first report, addressing what exactly happened and what urgent measures should be taken, on 14 December 2007 (Poynter, 2007). Poynter issued his final report in June 2008 (Poynter, 2008) at the same time as a slew of other government reports on data handling and security (Cabinet Office, 2008a, b; IPCC, 2008).

Unsurprisingly, the news of a breach of this scale immediately renewed concerns about the government's plans to store the personal details of the entire UK population on the three logically distinct databases that would comprise the Register. There was renewed interest in alternative, more secure means of storing this data in such a way that minimizes the risk of similar large-scale breaches (LSE Identity Project, 2008).

The Crosby Review of Identity Management

When Gordon Brown was still Chancellor of the Exchequer, he appointed Sir James Crosby to chair the Public Private Forum on Identity Management. The forum was asked to review evolving technologies used for identity management and consider how public and private sectors can work together to maximize efficiency and effectiveness (Brown, 2006). Crosby began his work in September 2006, consulting widely with government, industry, and civil society. He presented his preliminary report to the Chancellor in March 2007 and was invited to produce a fuller report for later that year. Crosby's review was mentioned in the leaked NO2ID report and in the 2008 Delivery Plan and the government has claimed that it has benefited greatly from the review and is incorporating key elements of it in their plans, a claim that has been challenged by others.

Introducing the concept of identity assurance, Crosby states that "the key element in common between the public and private sectors is the consumer" (§1.2) and he therefore defines identity assurance as "a consumer-led concept in which people prove who they are to others, be they retailers, financial institutions, domestic or foreign governments etc." (§1.3). In this context, identity is "an informational representation of the chain of life events that is defined by who they are" (§1.4). For Crosby, the consumer focus in identity assurance makes it distinct from identity management which, although utilizing many of the same technologies, he sees as being designed "to benefit the holder of the information," whereas identity assurance "is focused on bringing benefits to the consumer" (§1.6).

In terms of biometrics, Crosby notes that they provide "no 'silver bullet' in identity assurance" (§1.19) and pure biometric images are irreplaceable once compromised. He therefore suggests that *if* biometrics are taken, "the database need only store one of a number of nonunique digital representations (a collection of points on the print) which can, if needs be, be replaced by another nonunique representation" (§1.20). That is, from an identity assurance perspective, full images of biometric data should not be held on government databases although, from an identity management perspective, other government departments (such as the police with their collection of unmatched crime scene prints) may find the storage of full images beneficial (Whitley and Hosein, 2008).

In order for the public and private sectors to benefit from an identity assurance scheme, Crosby recognized the importance of widespread and fast consumer adoption. He noted that "low-cost schemes have found it easier to persuade citizens of the scheme's benefits and have demonstrated higher take up" (§3.5) where low-cost might involve cheap or free tokens and low cost enrolment. According to Crosby, an effective identity policy has to involve the private sector in the roll-out of any identity assurance scheme and the scheme should be built on existing infrastructure and resources.

On the question of reliability Crosby notes that "it is technically impossible for any identity scheme to provide 100 per cent assurance" (§4.7) and argued that a quick and efficient repair of identity is also required. Such a process would also help secure public trust in the scheme.

In summary, Crosby presents 10 key principles that, he suggests, will lead to a consumer-led assurance scheme that has "universal status" (these are summarized in Table 3.3) and a scheme that would provide significant benefits to both the public and private sectors. Reading between the lines, it is clear that Crosby is no fan of the National Identity Scheme as many of the principles he proposes are not currently found in the Scheme.

Delivery plan 2008

On 6 March 2008, on the same day as Sir James Crosby issued his report on identity assurance the Home Office issued what it called the "Delivery Plan" for the National Identity Scheme (UKIPS, 2008a). This document confirmed much that had been foreshadowed in the document leaked by NO2ID.

Table 3.3 Sir James Crosby's ten principles for the design of any identity assurance scheme

1. The purpose of any scheme should be restricted to that of enabling citizens to assert their identity with ease and confidence.
2. The scheme's governance should be designed to inspire the highest level of trust among citizens.
3. The amount of data stored should be minimized. (In this context, Crosby recommends that only nonunique digital representations of biometric images should be stored and that any additional data accessed during enrolment should not be retained.)
4. Citizens should "own" their entry on any register. (In particular, Crosby suggests that the verification of identity should be performed "without the release of data," that is, it should not be possible to "push" data to other public or private sector organizations).
5. Enrolment processes should vary between individuals and change over time.
6. The scheme should be capable of being rolled out at pace.
7. The scheme's systems should be closely aligned to those of the banks.
8. Citizens should be able to rely on their cards being replaced and their identity being repaired quickly and efficiently.
9. Enrolment and any tokens will have to be provided free of charge.
10. The market should provide a key role in delivering a universal ID assurance scheme.

Source: Sir James Crosby, 2008, pp. 7–8.

In particular, it noted a "twin track" approach to delivering the Scheme, beginning with those who are employed in sensitive roles or locations and in 2010, for young people on a voluntary basis. The second track would involve, from 2011/12, high-volume enrolment of British citizens, offering a choice of receiving a separate identity card, a passport, or both (UKIPS, 2008a, p. 7). The plan also suggests that the widespread availability of personalized, joined-up services will be available in 2015. On 1 August 2008, French company Thales was awarded the contract to implement the Temporary or Tactical Register (UKIPS, 2008l).

The 2008 Delivery Plan represents the third significant delivery option for the UK's National Identity Scheme. It presents a far slower roll-out of identity cards to the UK population than the initial 2007 roll-out and significantly changes the nature of the Scheme, including its enrolment and verification functionality. The changes to the Scheme and the consequences that result are examined in detail in Chapter 9.

Home Affairs and Constitution Committees

In March 2007 the Home Affairs Select Committee announced an inquiry into "A surveillance society?" focusing on Home Office responsibilities 'such as identity cards', the Committee's report, including detailed discussion of the Identity Cards Scheme was published on 8 June 2008 (Home Affairs Committee, 2008).

In April 2007, the House of Lords Constitution Committee launched its own investigation into the impact of surveillance and data collection, which was set against a series of proposals including identity cards. Its report, "Surveillance: Citizen and State" was published on 6 February 2009 and also included detailed consideration of the implications of the Identity Cards Scheme (Constitution Committee, 2009).

Secondary legislation

In June 2003, the OGC Gateway Review of the Scheme had recommended that "the key accompanying secondary legislation, will need to proceed alongside the work on project definition" once a decision to proceed had been taken in principle (Office of Government Commerce, 2003). However draft secondary legislation was only presented for consultation in November 2008 (UKIPS, 2008c).

This legislation included details about enrolling "Wave One" airport workers, National Identification Number (NIRNo) Regulations (including the decision not to have the NIRNo on the face or the chip of the card), and detailed regulations and penalties associated with the issuance and update of data on the Register.

Evolution of the political opposition

As described above, over the course of the debate about the government's proposals for identity cards, the political parties in Britain eventually drew clear lines in the sand over the issue. In the 2005 election the Labour Party was insistent in its support for a voluntary identity card scheme, with a statement in its party manifesto stating as much. The Conservative Party was a bit more confused at the time, but as a result of the leadership battle after the election, the Conservative's position became more clear.

In fact, by the time the Bill was revisiting the House of Commons the Shadow Cabinet was offering emphatic opposition to it. When David Cameron was elected as Conservative Party Leader one of his first policy announcements was that, should he win the next election, he would abandon the proposals for identity cards. His opponent in the leadership campaign, David Davis, was appointed as the Shadow Home Secretary, making him responsible for continuing the opposition to the Scheme.

After the Bill became an Act, the political opposition continued and, if anything, increased. Notably, David Davis took the unprecedented action of contacting the Cabinet Office and the IT industry to warn them about the procurement process for the Scheme, reminding the firms that if the Conservatives were to win the next election their intention would be to terminate all the contracts relating to the Scheme.

David Davis eventually stepped down from his position and called a by-election to get reelected with a mandate on protecting civil liberties in Britain, including repealing the Identity Cards Act (Raab, 2009). He won that by-election but was not reappointed as Shadow Home Secretary. To date the Conservative Party continues to state its strong opposition to identity cards (Cameron, 2009).

With the possibility of a hung Parliament after the next election, the continued opposition to identity cards by the Liberal Democrat “third party” suggests that a coalition alliance between these parties would result in the Scheme being scrapped.

CHAPTER 4

The proposed National Identity Scheme for the United Kingdom

It is widely appreciated in policy analysis that any given policy is much more than the legislative language that authorizes it. What is more difficult to capture, however, is the full picture of a policy, as the creators of the policy themselves may not fully appreciate its long-term version. When this policy enshrines itself in a technology or an infrastructure it becomes essential, for the purpose of policy analysis, to understand both the proposed legislative language and also the descriptions of the "full picture." Details of the full picture, as much as the policy makers themselves know them, tend to leak from the reports and formal documents issued by the creators of a policy, but they also emerge through probing amendments, careful questioning and, occasionally, by accident.

In parliamentary and open debates, such "prodding" is commonplace and can often be a useful research device. That is, when policy-makers are compelled to answer specific questions they must move away from carefully worded, general statements about the virtues of a scheme and disclose some of its proposed characteristics.

This chapter reviews the National Identity Scheme (the Scheme) as it was put to Parliament during the Parliamentary scrutiny of the Identity Cards Bill (the Bill) and as outlined in the final Act that received Royal Assent in March 2006 (the Act). The government always claimed that the Identity Cards Act 2006 was "just" enabling legislation as there was "much still to be done in terms of detail, regulations and all the other elements" [28 June 2005,: Column 1253] and the first batch of draft secondary legislation that provided this detail was finally issued in November 2008. Nevertheless, this "enabling" legislation still coded into law many key aspects of the Scheme as the Home Office envisaged it would be implemented (cf Home Office, 2002; Office of Government Commerce, 2003).

This chapter reviews the key aspects of the Scheme as "enabled" by the legislation, the key issues that Scheme was due to address, the way in which the Scheme was intended to operate, the costs and benefits of the Scheme and the proposed roll-out strategy.

Overview of the Scheme

There is great irony that the Act is only partially about identity cards. That is, the card is only one part of a much larger integrated scheme. The Government's vision involves a multifaceted and far-reaching scheme that collects and processes substantial use of personal information within a complex legal and technological environment, yet it chose to present the legislation surrounding the Scheme in an Act named after an age-old technology.

The Act outlines an identity system that has seven components:

- **The National Identity Register (the Register):** This element is the information hub of the system. Clause 1 of the Act 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. The Register will also record "information about occasions on which information recorded about him in the Register has been provided to any person" (i.e. an audit trail of every time an identity is formally verified against the Register).
- **The code:** Clause 2 (5) requires that every individual must be given a unique number, to be known as the National Identity Registration Number (NIRNo). In the same way in which the U.S. Social Security Number has become a de facto identification number in many sectors (Garfinkel, 1995) this number could become the "key" for government and private sector organizations to access information on the Register and, in certain circumstances, to share information.
- **Biometrics:** Clause 5 (5) requires individuals to submit to fingerprinting and "other" means of physical (biometric) identification. Clause 42 (1) specifically lists the features of an iris as an example of biometric information.
- **The card:** Clause 6 establishes the actual identity card, generated from and containing part of the information in the Register.
- **Legal obligations:** Clauses 13 and 14 establish the ways in which it may be necessary to produce the card in order to obtain public services.
- **Administrative convergence:** The number and the Register will be used by a variety of agencies and organizations both for access and disclosures and in the future as a possible administrative base. Schedule 4 (1)

lists those registration numbers (e.g. National Insurance, passport, drivers license, etc.) that might be stored on the Register for a particular person.
- **New crimes and penalties:** The Act establishes a large number of new crimes and offences to ensure that people comply with the legislation.

Objectives of the Scheme

The statutory purposes of the Scheme are to facilitate, by the maintenance of a secure and reliable record of registrable facts about individuals in the United Kingdom,

- the provision of a convenient method for such individuals to prove registrable facts about themselves to others who reasonably require proof; and
- 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 (Clause 1(3)).

For the purposes of the Act, something is necessary in the public interest if and only if, it is

- 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 unauthorized working or employment; or
- for the purpose of securing the efficient and effective provision of public services (Clause 1(4)).

The last subclause is potentially so broadly worded as to permit virtually any government activity to be covered by the catch-all phrase "efficient and effective provision of public services," with further ambiguity introduced by the pluralized "services."

According to the Government's Identity Cards website, the Scheme aims to

- help protect people from identity fraud and theft;
- strengthen our security and improve public confidence;
- tackle illegal working and immigration abuse;
- disrupt the use of false and multiple identities by organised criminals and those involved in terrorist activity; and

- ensure free public services are only used by those entitled to them (UKIPS, 2009d).

The same site gives the following list of benefits of the National Identity Scheme. It will

- help protect cardholders against identity theft and fraud;
- provide a reliable way of checking the identity of people in positions of trust;
- make travelling in Europe easier;
- provide a secure way of applying for financial products and making financial transactions, including those made over the internet;
- offer a secure and convenient way of proving your age;
- help to confirm your eligibility for public services and benefits – and reduce fraud relating to these services and benefits;
- help in the prevention of organised crime and terrorism;
- help combat illegal working and reduce illegal immigration to the UK; and
- allow the police more quickly to identify suspects and people they arrest (UKIPS, 2009a).

It is interesting to note that many of the aims and benefits of the Scheme have a strong government rather than citizen-centric perspective, with very different technological infrastructures underlying them. For example, a government-centric identity policy which addresses border control issues would need a very different on-line, identity-checking facility from a user-centric one for enabling secure electronic commerce transactions on-line.

On many occasions, the government has been challenged about the key aims and purposes of the Scheme with one Home Office minister admitting that the benefits of the Scheme had been "oversold" (Woolf, 2005). Moreover, following the terrorist attacks in London on 7 July 2005, the then-Home Secretary admitted that identity cards would have made little difference (Clarke, 2005), particularly as the attackers turned out to be UK citizens who would have been entitled to hold a UK identity card.

With each goal or objective, however, the scheme must take on new burdens. It must, for instance, be able to "make travelling in Europe easier," but in order to do so, it takes on the burdens of complying with international standards for travel documents, which entail both technological and procedural challenges. In the case of helping police to prevent crime, the burden becomes more financial as the police must have scanners to identify individuals based on their cards or their biometrics. As the Scheme becomes the solution to more and more problems, practical issues of scope creep become significant.

How the Scheme is expected to work

The operation of any identity scheme involves two distinct stages of operation. First, individuals must be enrolled, which involves the registration of some information about them. Registering for a driving license or a passport requires the provision of personal information including details relating to the entitlements associated with the identity document, for example, "I have the right to drive" or "I am a citizen of this country." This information is typically stored on database. Second, the scheme must permit verification of identity-related data. When someone is stopped by the police or passes through a border control point their identity needs to be verified, which is normally done by checking the associated identity document. In the case of passports, the integrity of the document is checked (see UKIPS, 2007a) and the passport photo is compared with the person's face. In the case of driving, this verification process could also involve a check against the database of driving licenses to ensure that the license is valid.

With the advances in technologies, policy-makers are considering ways to make these processes more thorough and, as a result, more complex, potentially involving more data collection, generation, and sharing.

Enrolment

The UK Government has long promised that its Scheme would provide the "gold standard" of identity. That is, it would be much more reliable than existing systems and practices (Office of Government Commerce, 2003). To support this claim, the Government has repeatedly emphasized the care by which citizens would be enrolled into the Scheme. In particular, the Government is concerned that individuals cannot enroll into the Scheme more than once and hence have more than one "official" identity. In order to achieve this goal, the enrolment process would involve two forms of checks.

The first of these is a *biographical check*, whereby biographical details about the citizen are checked against information held against them on various public and private sector records. This would involve interviews lasting 30 minutes. "It will be conducted in a friendly manner and will consist mainly of asking applicants to confirm facts about themselves, which someone attempting to steal their identity may not know" (UKIPS, 2009b). For individuals with a reasonably extensive biographical footprint, this could include details about their date of birth, address history, their bank details, details about their children, national insurance number, etc. News reports suggested that the questions could be drawn from a list of 200 possible questions (Johnston, 2007). This enrolment would take place at specially designated "enrolment centres" that would involve no more than one hour's travel for most citizens (with special alternative arrangements put in place for rural communities, such as the Highlands and Islands).

In light of the vast data breaches amongst the public sector in the UK and particularly the HMRC breach, there are some obvious concerns with the way in which the biographical check would take place. "Applicants will be asked to confirm facts about themselves which someone attempting to steal their identity may not know but to which the *interviewers already know the answer.* Mr Herdan (executive director of the Identity and Passport Service) said there would be no pass or fail mark but officials would make a judgment on the basis of the whole interview whether an applicant was telling the truth" (Johnston, 2007 emphasis added). This means, at the very least, that the interviewers will have access to a lot of personal information about each individual enrolling in the Scheme. A likely practical implementation of this process would involve collating this information at the interview location, before the interview begins. It appears that this collated information will be destroyed after use although the details of the particular questions asked and answers given would need to be stored on the Register.

The biographical check, however, is not necessarily perfect as a determined individual could learn many of the details of another person and potentially pass the biographical check element using the other identity. Therefore, in addition to the biographic check, the Scheme also involves a *biometric check*. That is, the biometrics of individuals who enroll into the Scheme will be checked against all the other biometrics from individuals who have already been enrolled. If the biometrics match those of someone already on the Register, this would mean that the person has already enrolled in the Scheme under a different identity.

The effectiveness of this process is dependent on the type of biometrics chosen, the quality of the biometrics collected and the methods used to compare the submitted biometrics with those previously recorded. Different biometrics have different performance parameters in terms of ease of enrolment and likelihood of mismatching or not-matching against existing records. At a technical level, the differences between various biometrics can be understood in a variety of ways. These include

- false match rate – the probability that a person's biometric matches the enrolment template of another person;
- false nonmatch rate – the probability that a person's biometric fails to match their own enrolment template; and
- failure to acquire rate – where the submitted biometric is too poor for the system to make a reliable decision (Science and Technology Select Committee, 2006, Section 17 and Appendix 2).

For example, the failure to acquire rate for fingerprints is affected when taking fingerprints from people with no fingers, or whose fingerprints have been damaged through manual labor. Moreover, not all biometric systems are built equally. There may be performance differences between two implementations of the same biometric. Environmental issues such as lighting and usability issues such as user-interfaces that cater for individuals with disabilities can have dramatic implications for the effectiveness of the system. The quality of the technologies used to collect and compare the biometrics also varies widely. For instance a simple photograph of the face from a mobile-phone camera could collect good images while a high resolution scanning technique using 3-D technology would offer greater opportunities to differentiate between individuals. The consequences of these issues are discussed in more detail in Chapter 6.

There is also some uncertainty about the feasibility of the proposed biometric checking. Although one-to-one checks are increasingly common (i.e. do the biometrics being presented by this person match the biometrics we have on record for this person?), the one-to-many checks (i.e. do the biometrics being presented by this person match any of the biometrics that we have on record) required for the Scheme are less common, particularly at the scale proposed for the UK. That is, once the Scheme is fully rolled out, each new biometric would need to be checked against upwards of 50 million other records.

In order to match the promises made regarding the objectives and goals of the scheme, such as running uniqueness searches against a database of 50 million other biometrics and fulfilling European travel requirements, the Home Office decided to require facial scans, fingerprints, and iris scans. Each biometric would meet a different need. The facial scans are universal in that everyone has a face and they are commonplace and already part of the international standards for travel documents; facial scans would not provide reliable results when searching against 50 million other facial images as there is a high risk of error (Introna and Nussenbaum, 2009). Fingerprinting would match European travel document standards and the data would provide lower error rates, but as mentioned before, fingerprint collection is not necessarily universal as some people have "thinner" fingerprints, or missing fingers. Searches against large databases are somewhat problematic as searches may take quite some time depending on the choice of system. Iris scanning is unprecedented in that there is no international standard for the technology but would permit a unique identification of nearly every citizen. In addition, system performance to date suggests that it offers an effective search capability across large databases. These three biometrics were offered to Parliament as the most effective means of identifying the entire British population.

Verification

Once an individual is successfully enrolled into the Scheme and their data are held on the Register, the Scheme is intended to provide a variety of verification services. At the simplest level, in some circumstances, all that may be required is for an individual to present his identity card when asked. Such a "flash and go" check would involve checking that the card appears genuine (cf UKIPS, 2008d), has not been obviously tampered with, and that the person presenting the card "looks like" the person whose image appears on the card.

More sophisticated verification processes also exist, particularly considering the advanced technologies foreseen for the Scheme. Biometric checks could be done, where police and other agencies could use biometric scanners to take an individual's fingerprints and/or photograph and verify that biometric data against the data that is kept on the card or perhaps on the Register to ascertain technologically that the individual presenting the identity card is the same person who was present at the enrolment stage. For a scheme like this to work, however, biometric scanners would have to be near-ubiquitous; although scanners are increasingly found at airports around the world, their deployment is progressing far more slowly across government systems and the private sector, mostly due to costs and infrastructure development challenges.

Verification could take place *on-line* or *off-line*. An on-line verification could be as sophisticated as comparing a biometric of the individual with the biometric stored centrally in the Register; or as simple as scanning the card and checking against the database that the card is indeed valid. Off-line verifications can also be sophisticated, where the biometric is compared only to the biometric on the card; or as simple as merely doing a "flash and go" check, though it is also possible to verify the integrity of the card, that is, that it has not been tampered with, that it has the "distinctive sound when flicked" (UKIPS, 2008d). On-line checks, particularly of a biometric nature, are costly and burdensome tasks for all forms of verification, making them unlikely to be used for minor operations.

The government's position on whether most checks would be done online or off-line has varied markedly. In 2004, the Home Office stated: "We are proposing to make on-line checks against the register the norm, except in those low risk/low value cases where a visual check is judged to be sufficient" (Watson, 2004). Responding to a question of whether libraries and video rental shops might require the card the then-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" (Home Affairs Committee, 2004, Answer to Q653).

Department of Work and Pensions documents released following a Freedom of Information request (DWP, 2007) gave detailed assumptions about different on-line and off-line verification models.

Critics then began to wonder why such an expensive and sophisticated enrolment scheme was being implemented if the use of the Scheme would frequently result in simple "flash and go" verifications, which were particularly susceptible to the existence of fake cards that appeared to be genuine.

During the later stages of Parliamentary deliberations, the government came forward with proposals for an alternative infrastructure for verification that could address this risk of excessive "flash and go" verifications. This would be enabled through the use of a Chip-and-PIN process, whereby the individual puts their card in a specialist card reader and enters their secret PIN to confirm that the card is theirs. This may also be combined with a visual check of the card. It is unclear whether the PIN would be checked against encrypted information held on the card or if the PIN would be checked against a central server as the DWP document gave processing times for each of between 15 and 30 seconds. Most bank cards allow both a local check (for low-risk transactions) and a remote check, for high-risk transactions, which can include confirmation that the card has not been marked as lost or stolen.

There is growing evidence that PINs are not particularly secure as people often use the same, memorable PIN for all their cards and PINs can be divulged. These numbers are deemed inappropriate for access to high-impact level applications (Cabinet Office, 2006).

A third level of check would involve checking the card and the biometric details of the individual whose identity is being verified. Thus, in addition to entering their PIN an individual might also be asked to present their biometric (again, it is unclear at this time whether the biometric would be checked against a local copy held on the card, or against the biometric stored on the Register). This is an implementation of the computer security "ideal," of requiring individuals to provide, for the purpose of authentication, something they "know," for example a PIN, something they hold, for example the card, and something they "are," for example their biometric.

Costs issues continue to plague even this solution. In order to do these more sophisticated verifications, organizations would need to be suitably accredited, would need to invest in appropriate card readers (although, presumably, there is a possibility that the existing Chip-and-PIN infrastructure including card readers could be used) and, if required, suitable biometric readers. These would need to be connected to the identity verification services using appropriate secure communication links. Depending on the verification services offered, it may also be possible to integrate the verification process with existing organizational systems. For example, trusted organizations might be able to combine identity verification with a data push whereby the individual's current address details (as held on the Register) could be delivered to the organization's internal systems to populate their databases.

The issue of on-line verification also gives rise to a further issue. According to the Act, each time a formal verification of information held on the Register is made, an audit trail record is kept, which logically would include data about when and where the verification took place (e.g. "Elizabeth Yap had her identity verified by a bank in May 2008," although it is likely that the audit trail would be much more detailed than this: "Elizabeth Yap had her identity verified by bank ABC, branch 123, using terminal xyz, at 10.13 on 1 May 2009. She entered her PIN and presented a fingerprint biometric for her right thumb. The verification took 0.13 seconds to process"). The assimilation of all this data is similar to a credit card company accumulating a list of all financial transactions, for billing purposes.

One consequence of this data aggregation in the case of the credit card company is that it has records of a good proportion of a person's financial transactions and is able to spot unusual transactions that might indicate that the card is being used for fraudulent purposes. Similar aggregation could arise in the case of the Register where the audit trail is of "live events" and is to be implemented for universal use in the United Kingdom.

As such it could provide a log of all of an individual's interactions with the State and the private sector.

In the context of the government's plans for the retention of communications data (Whitley and Hosein, 2005) and crime prevention, a Home Office spokesman described the benefits of being able to "examine their contacts, establish relationships between conspirators and place them in a specific location at a certain time."

If the same logic of the usefulness of inferring relationships between individuals that places them at specific locations at a certain times applies, then many of the privacy concerns about the audit trail on the Register become understandable.

Rolling out the Scheme: The link with passports

An integral part of the strategy behind the Scheme has been the close link between identity cards and passports. From the first consultation on entitlement cards (Home Office, 2002) the government has decided to link the issuing of identity cards with the issuing of passports. The Identity and Passport Service was formed from the existing Passport Service immediately after the Bill completed its Parliamentary passage.

The government gave a number of reasons for this strategy. First, it argued that it was compelled to update the passport-issuing process to include biometric identifiers. Second, as a result of this close linkage between passports and identity cards, the government was able to claim repeatedly that 70 percent of the cost of identity cards would need to be spent "anyway" to enable the new passport-issuing process, as much of the necessary infrastructure, systems, and processes would apply to both. Third, with passports issued with a ten-year validity period (the same as was proposed for identity cards), the roll-out of the Scheme could be linked to the issuance of passports. Finally, with approximately 80 percent of the adult population having passports, linking the issuing of identity cards with passport renewals would give a clear timescale for the government's plans to make registration on the Register compulsory (even if the carrying of an identity card would not be).

The government's claim that it was obliged to upgrade passports to include the same biometric identifiers as it was proposing for identity cards is a complex and arguably inaccurate one. It is discussed in more detail in Chapter 5.

The claim that 70 percent of the costs of the Scheme would be incurred for the upgrade to the passport service depends critically on the claim that the proposed changes to the passport service are in fact mandatory rather than desirable. The government's strategy was to lump more changes into the passport infrastructure than was strictly necessary, while claiming that they were necessary, so the costs of the new infrastructure would be reduced (Collins, 2009a). One consequence of the claim about necessarily incurred costs was the Government's statement that the first identity cards would cost no more than £30 given a passport fee (at that time) of £65.

The link to the passport was not just to conceal the costs – it was a carefully considered strategy for the deployment of the Scheme. That is, by issuing identity cards alongside passports, the government could address a key issue of load-balancing for the delivery of the Scheme. Given the size of the UK population, around 60 million people, and a registration process involving both biographical and biometric enrolment, it would be sensible for it to be staggered. Otherwise, a "big bang" approach of having everyone do so in a single period (say the first year) would mean that the enrolment centers would have very little to do for the next nine years (apart from enrolling those individuals who turn 16 – approximately 3,000 a day).

Such a staggered roll-out means that it is possible to predict the likely take-up of identity cards (assuming there is not a rush of individuals who want to register for a card in advance of the renewal of their passports). However, during the Parliamentary debates it proved to be tricky to obtain definitive numbers of passports that were due to be issued each year and hence to infer the likely number of identity cards that would be issued over any particular period.

In December 2005, Home Office minister Baroness Scotland informed the House of Lords of the number of new passports and passport renewals that were reported/foreseen for the period 2003/04 to 2010/11 [WA HL2359]. She also noted the current best estimate for the number of enrolments on the National Identity Register for 2012/13 and 2013/14. Table 4.1 presents the total number of passports to be issued until 2010/11 and adds the estimated number of NIR enrolments for 2012/13 and 2013/14. The cumulative number of passports (and hence identity cards) from 2005/06 indicates the likely roll-out of the Scheme assuming enrolment starts shortly after the Scheme receives Royal Assent. Interestingly, there appears to be a significant jump in the number of individuals enrolled on the Register in 2011/12. This would suggest plans for making enrolment compulsory at that time. Further confusion arose when Home Office minister Meg Hillier reported that "The number of estimated passports to be issued in the year 2007–08, as reported in the Identity and Passport Service (IPS) Business Plan, is 6.2 million" [WA 164091], a figure significantly higher than previous statements had suggested.

Figures for the number of "products issued" by IPS were presented in the November 2007 and May 2008 cost reports (reflecting the changes proposed by the Delivery Plan that had been launched in March 2008). Table 4.2 and Table 4.3 take these figures and assume that once identity cards begin being issued, half of the total products issued will be identity cards.

Taking the earlier figure of around 4 million citizens who will receive a new passport and a new identity card each year and assuming a total UK population of around 52 million citizens, this suggests that calculating on passport-based enrolment alone, over ten years around 40 million citizens will have been issued with passports and identity cards (i.e. approximately the 80 percent of the adult population who have a passport). This also means, however, that it will take seven years (when 28 million citizens have enrolled) for over 50 percent of the adult population to be enrolled on the Register and be issued with an identity card. This means that the government's ultimate desire to make enrolment in the Scheme compulsory can only realistically take place after at least six years of operation of the Scheme. This has important implications for the viability of the Scheme,

Table 4.1 Likely enrolments (millions) drawing on statements made to Parliament in December 2005

	2003/04	2004/05	2005/06	2006/07	2007/08	2008/09	2009/10	2010/11	2011/12	2012/13
Passports issued (new and replacement)	3.7	3.7	3.7	4.7	4.3	4.1	3.8	4.0		
Cumulative passports			3.7	8.4	12.7	16.9	20.7	24.7		
NIR enrolments									31.3	40

Table 4.2 Likely enrolments (millions) as presented to Parliament November 2007

	2007/08	2008/09	2009/10	2010/11	2011/12	2012/13	2013/14	2014/15	2015/16	2016/17	2017/18
Total products issued	5.8	5.6	5.9	9.4	10.2	11.2	11.6	11.7	11.8	10.4	11.3
Identity cards	0	0	0	4.7	5.1	5.6	5.8	5.85	5.9	5.2	5.65
Cumulative identity cards	0	0	0	4.7	9.8	15.4	21.2	27.05	32.95	38.15	43.8

Source: Data taken from third s.37 Cost Report (UKIPS, 2007c).

Table 4.3 Likely enrolments (millions) as presented to Parliament May 2008

	07/08	08/09	09/10	10/11	11/12	12/13	13/14	14/15	15/16	16/17	17/18
Total products issued		5.6	5.5	5.4	5.9	7.9	10.5	12.5	12.9	13.1	12.3
Identity cards		0	0	0	0	3.95	5.25	6.25	6.45	6.55	6.15
Cumulative identity cards		0	0	0	0	3.95	9.2	15.45	21.9	28.45	34.6

Source: Data taken from fourth s.37 Cost Report (UKIPS, 2008k).

given its infrastructural qualities, which are discussed in more detail in the next section.

An identity infrastructure

From the large number of government agencies and commercial organizations that are expected to make use of identity cards, it is clear that the Scheme is not intended to be a stand-alone system, but rather that it is best conceptualized as part of a government-managed infrastructure providing identity services. Academic research on large-scale information infrastructures (Ciborra and associates, 2000; Darking and Whitley, 2007; Hanseth et al., 1996; Monteiro, 1998; Star and Ruhleder, 1996;) suggests that managing such infrastructures is often problematic. Lessons from academic research raise serious questions about the Home Office's notion on the deployment and eventual success of the Scheme.

Previously, all parties in the Parliamentary deliberation presumed that the Home Office was speaking on behalf of the set of government departments and envisioning a scheme that would apply across all services. The latter was certainly true, but as time went on, the Home Office admitted that the former was less clear. That is, when prodded as to when and how other government departments and public services will adopt, or "buy-in" to the Scheme, the Home Office began responding that "decisions on whether, when and how particular public services will make use of the identity cards scheme will be made by those services – individually or collectively as appropriate depending on how services are managed" (Burnham, 2005). The reason for this lack of synergy could be explained by academic research on infrastructures that show that infrastructures often constrain decisions in unexpected ways.

The logic behind providing a single, government-managed, identity infrastructure is easy to understand. Many government agencies currently need to verify the identity of the individuals with whom they have dealings. At the present time, each government service has its own ways of verifying the identity of individuals. Each method has different levels of quality and the government clearly sees benefits to providing a single, high quality identity service used across the public sector (Home Office, 2005d).

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

It also, however, highlights some of the practical management issues associated with the use of the proposed information infrastructure. To use an example, the Department of Work and Pensions, one of the largest and most public-facing ministries, has spent considerable time and money creating the new Departmental Central Index that stores details on individuals according to their National Insurance number (NINo), used for administering the national pension scheme. As a result, all the systems that use the Central Index will not be able to switch across to using the NIRNo without further expenditure. Moreover, during the periods of transition (from using the DWP NINo in the Central Index to using the Home Office's NIRNo in the Central Index and using the NINo for those who do not have an identity card and the NIRNo for those who do) there will need to be two "systems" in existence, with two sets of processes for handling identification and data matching. There are also likely to be complex issues associated with tidying up the data in terms of matching records that are indexed by NINo to those that are indexed by the NIRNo, which are very much about the redesign of government processes and not just government systems and indexes.

Further problems can be predicted, as unique identifiers are not in fact diminishing through convergence. Instead the number of identifiers used in government is growing in part because of the silos that exist in bureaucratic government organizations. For instance, in his written evidence to the Public Administration Select Committee, Professor Patrick Dunleavy (Dunleavy, 2005) noted that the UK tax ministry, HMRC, encouraged taxpayers to use that ministry's own taxpayer number rather than National Insurance numbers. This was because they were not prepared to pay the Department of Work and Pensions to use their NINo identity data.

At present over 80 departments and agencies have their own unique identifiers for each record because that numbering system is appropriate for their systems, processes, and policies. Introducing a new uniform numbering system will not only be costly but also burdensome and most likely unnecessary.

Characteristics of information infrastructures

Information infrastructures are generally understood to consist of standardized systems and data, as well as formal communication mechanisms. They are often classified according to their reach and scope in terms of the number of activities they support and the type and variety of activities supported (Darking and Whitley, 2007).

Infrastructures can be classified in terms of providing a utility, a dependence, or as enabling services. Utility infrastructures typically aim to reduce the cost of processing and communicating information, often taking advantage of economies of scale. They are designed not to interfere with applications and business processes (Ciborra and associates, 2000). Dependence infrastructures allow for new applications to be launched across the infrastructure and so enable new processes to take place. Enabling infrastructures are intended to provide as much flexibility for future expansion and use as possible.

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

It is apparent that an information infrastructure deals with questions of universal use and access and, as such, requires high levels of standardization from all potential users of the system (Bowker and Star, 1999). Interoperability between systems is required and this has implications for the flexibility, resilience, and security of the system (Star and Ruhleder, 1996).

Infrastructures must also be able to cope with the dual constraints of local variety and centralized planning. Issues of standardization and interoperability in the case of the Scheme mean that if a government department is intending to use the infrastructure to verify identity using biometrics (i.e. for situations that require a higher level of assurance than simply visual inspection or PIN-based confirmation), they will need to provide the full range of biometric readers (fingerprints, face recognition, and iris scanning) to ensure that biometrics could be captured for verification. Moreover, if these biometrics are to be compared against the Register the quality of the biometrics obtained must be of the same standard as those collected during the enrolment process.

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

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

This means that any infrastructure development project will never cover the whole of the infrastructure, but rather will need to be developed in conjunction with the constraints arising from existing aspects of the infrastructure. It is therefore very difficult to determine in advance what the boundaries of the infrastructure will be. Similarly, it is not straightforward to determine which parts of an infrastructure can be dropped once replacement elements have been introduced (Darking and Whitley, 2007). There are many examples of infrastructure code that contain elements that have been superseded but which remain in place because of the desire not to affect other code that is successfully running. For example, Hosein et al. (2003) describe how Microsoft products use a Cryptographic Application Programme Interface (CAPI) as a standard interface to cryptographic software that requires the cryptographic algorithms to be digitally signed, even though the export controls that led to their introduction have been superseded.

There are also examples of this problem in government projects. For example, a study by the National Audit Office, the agency that audits the accounts of all other departments and agencies, on a cancelled project for a “benefits card” notes:

> This project initially proceeded on the basis of proposals from bidders that it would involve mainly the integration of existing software packages. In the event, the greater than expected complexity of the service

> requirement obliged Pathway [the supplier of the system] to develop much more new software than they had planned. The Department's view is that Pathway knew what was required but had intended to fit the requirement to match a system they had already implemented in Eire. The extent of new software development had major implications for the degree of difficulty of the project, since this a high-risk activity with high failure rates, especially in large organizations. (National Audit Office, 2000, p. 15)

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

It is important to understand the purpose of charging. Charges are sometimes used merely to manage an infrastructure to ensure against abuse, or to pay for processing charges and possibly for revenue generation. It is not clear, however, whether the Scheme's charges would be based on full cost accounting of all elements of the infrastructure. For example, should user departments simply pay for the provision of the act of verifying a particular identity, or should they also contribute toward the ongoing maintenance of the system from which they receive these indirect benefits? Should such contributions also include the process of enrolment into the system, or is this cost to be solely associated with the individual who obtains the identity card, or new, more secure passport? If, as the government expects, the identity card infrastructure becomes increasingly widely used, further issues of costing arise. Should the cost of use be fixed over time, or would the first departments to use the service be expected to pay a higher average cost than departments using the infrastructure once it has become an installed base?

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

This means that once the infrastructure is initialized, unless it is very carefully designed and managed, it will be increasingly difficult to make changes to it. For example, will the Scheme be able to cope with innovations such as new biometric technologies as they become available? As a result, most key decisions about information infrastructures have to be taken at times when knowledge about the factors that are affecting the decision is least known. Similarly, there is often a limited period of time when such decisions can be taken (Ciborra and associates, 2000).

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

Angry orphans can disrupt the successful implementation of an infrastructure. For example, suppose a high-profile department evaluates the benefits of using the identity card infrastructure for one of its policy goals against the costs of implementing the infrastructure outside its existing technology upgrade process (having, for example, recently invested heavily in a major system upgrade) and decides not to link into the Scheme immediately. Their decision not to take-up the system would likely affect the take-up decisions of other departments as well, which might have a clearer case for their own use of the Scheme but are worried by the high-profile department's decision.

Benefits of the Scheme

With the issue of the relative costs and benefits of the Scheme becoming a key issue for Parliamentary debate, the Home Office was keen to present the various benefits of the Scheme to Parliamentarians. Thus, in June 2005, as the Bill returned to the House of Commons after the election, the Home Office issued a "Benefits overview" report (Home Office, 2005d). According to this document, the Home Office promised that the Scheme would deliver:

- Strategic benefits, for example in the delivery of public and private sector services;
- Quantifiable benefits such as improved detection of crime by matching unidentified scenes of crime markings; and
- Nonquantifiable benefits such as allowing for more public and private sector business to be conducted securely and conveniently on-line and the public safety benefits of conducting Criminal Records Bureau checks more quickly (Home Office, 2005d, p. 1).

In addition, there were "important" individual benefits, detailed in a separate Annex. Thus, as far as the government was concerned, the primary benefits of the Scheme could be broadly defined as state- rather than citizen-based benefits.

According to the government, many of the strategic benefits "derive from the use of the National Identity Registration Number (NIRNo) which will be a unique number that will be unequivocally linked to an individual. The use of this number will revolutionise efficiency in public and private sector organisations alike" (cf Cabinet Office, 2005).

In terms of quantifiable strategic benefits, the document listed the Scheme's ability to reduce identity-related fraud, to combat money laundering, to enable employers as they check the immigration status of employees, and to introduce a "step change" in identity management and electronic transactions. Some of the problems with the claims about identity-related fraud have been reviewed in Chapter 1.

There were also a series of nonfinancial strategic benefits associated with the Scheme. For example, the Home Office's Benefits Overview report of June 2005 also highlights the benefits to policing associated with the introduction of the Scheme (Home Office, 2005d, p. 3). These include "improving the intelligence picture by providing fast, reliable access to information on intelligence targets," "increasing the likelihood of matching marks from scenes of crime ... as there are currently 900,000 outstanding crime scene marks on police databases," "speeding identification of incapacitated victims of crime," "reducing the resources required to prove that missing persons are alive and well," and "increasing the robustness of DNA mass screening activities" by ensuring "the police having confidence in the identity of the individual providing a DNA sample and ensuring they do not return and provide a further sample for a friend."

Not covered in the Benefits Overview document and not clearly disclosed to Parliament until after the Bill was passed, were the plans to use the Register as a de facto National Adult Population Register as part of the Citizen Information Project (CIP), allowing the government to "improve services by increasing the sharing of basic citizen information (contact details such as name, address and date of birth) across central and local government" (Johnston, 2008). As written evidence provided by noted UK data protection expert Chris Pounder to the House of Commons Home Affairs Committee noted (Pounder, 2008), despite numerous opportunities, the government chose to avoid pre-legislative scrutiny of these proposals, including avoiding these discussions as part of the general debate about the Bill. The relationship between the Register and the CIP had been noted in the Office of Government Commerce Gateway Reviews undertaken in June 2003 and January 2004.

Instead a written statement about the proposals was only issued three weeks after the Act had received Royal Assent. In it, the Chief Secretary to the Treasury noted a 2004 statement that "the Government had accepted a recommendation from the Citizen Information Project (CIP) about using the proposed National Identity Register (NIR) as an adult population register" [18 Apr 2006 : Column 1WS]. He reported that the CIP project had now completed its work, including the recommendation that "The Identity and Passport Service should be responsible for developing the National Identity Register (NIR) as an adult population database." The proposals were not felt to be an example of "scope creep" as the Act "includes securing the efficient and effective provision of public services as a purpose of the National Identity Register."

Paying for the Scheme

Given the uncertainties as to the scope and cost of the Scheme, particular attention was paid to how the Scheme was intended to pay for itself. In a statement to Parliament, the then-Home Secretary Charles Clarke announced:

> I have just published overall figures for verification and all the other services, but three sources of income will deal with the charges. The first is the fees themselves, which is why I said that fees would make up the giant's share, rather than a call on public funds. The second is a small contribution from public funds, which is the only amount that could be spent on other things – as is widely alleged – and the third is income that could be derived from contracts with organisations that use the database [13 February 2006 : Column 1119].

With the government announcing that the fee for identity cards would be £30 (making the full charge for a passport and identity card £93 at 2006 prices) and using the figures for the likely number of enrolments discussed above, it is possible to calculate the likely fee income for the Scheme. This leaves the "small contribution" from government and the "contracts with organisations that use the database." In order to infer an estimate of this remaining cost, it is necessary to infer take-up rates from the Home Office's (2005d) benefits overview document. This document was the only document publicly available to Parliamentarians and citizens and was surprisingly vague (for example, the graph detailing the benefits take-up, reproduced in Figure 4.1, did not have labels on the x-axis (presumably years of the Scheme) and a second graph of benefits growth compared to take-up, reproduced in Figure 4.2, was presented at a different scale making direct comparison a complex task.

On 8 November 2005 Home Office minister Tony McNulty clarified that the dates on Figure 4.1 were omitted because of uncertainty as to when the Bill would receive Royal Assent:

> The graph as it stands is flexible, as it represents annual movements in the benefits accrual. Therefore a reader of the graph could predict any start date for identity cards roll-out and then understand from the graph the progression of benefit accrual from that date. [WA 20869]

By manually rescaling the two graphs it is possible to combine them, see Figure 4.3.

The Home Office believes that the earliest benefits will arise from the use of the Scheme by the Criminal Records Bureau (CRB), the Driver and Vehicle Licensing Agency (DVLA), and the Department for Education and Skills (DfES). These benefits are time dependent as they require the sign-up of these departments and a sufficiently large registration base. For example, from the graph it is apparent that the DVLA would appear to start running checks against the Register when around 7 percent of the population is enrolled.

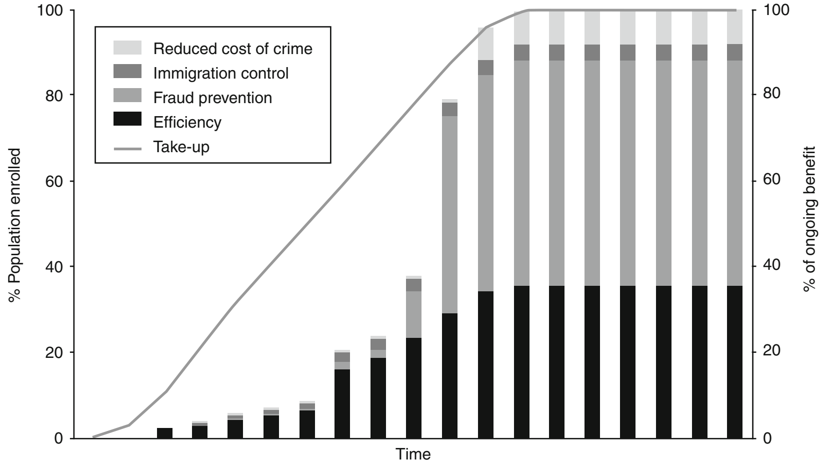

Figure 4.1 Benefits growth compared to take-up

Source: Home Office, 2005d.

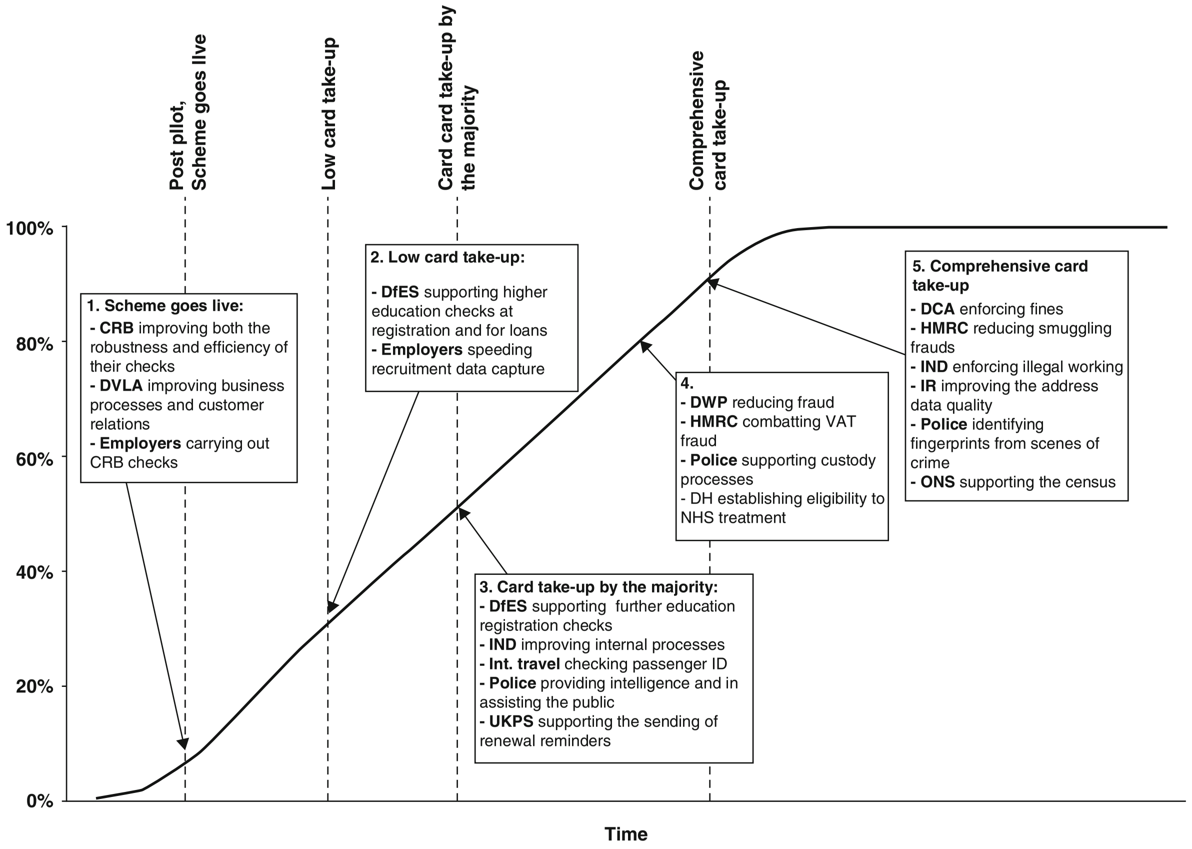

Figure 4.2 How key decisions regarding use of the Scheme impact upon when the benefits are realized

Source: Home Office, 2005d.

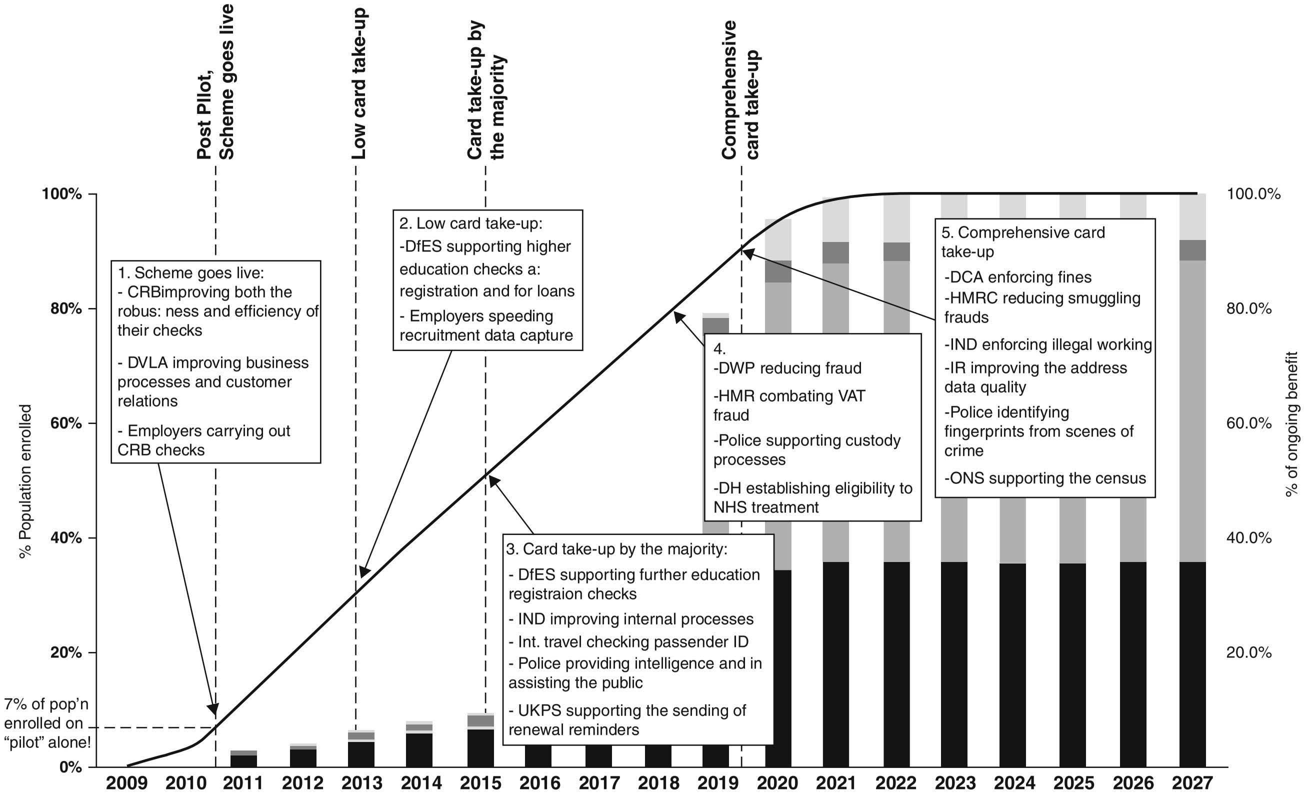

Figure 4.3 Combining the two graphs

Source: LSE Identity Project, 2006b.

When the Scheme is fully rolled out, it is possible to estimate the likely "verification" fee income from these Departments using a per-verification charge of £1.30 (this figure is based on the Home Office Trade-Off Study (Home Office, 2005a)). Thus, according to the CRB annual report from 2003/04 there are 2.25 million disclosures, suggesting a fee income of £2.93 million; the DVLA issues around 6.8 million drivers' licenses per year, with a resulting fee income of £8.84 million; and around 405,000 new students are accepted into higher education each year, resulting in a further £0.53 million in fee income. Before the Scheme is fully rolled out, of course, the annual verification fee income will be significantly lower.

Similar figures can be obtained by using the cost of the Passport Verification Service. Currently IPS offers this service for the Financial Services Industry (UKIPS, 2008j). It "allows financial services firms to check the validity of UK passports presented as evidence of identity by customers directly against IPS records. By verifying these details against IPS data, the service provides assurance of the validity of the document presented and significantly prevents the use of lost, stolen or counterfeit passports" (p. 2). It therefore helps organizations comply with antimoney-laundering regulations. IPS offers two fee levels for this service:

- a low-volume service with an initial set up fee of £750 (with 200 free queries) and a charge of £2.50 per query.
- a high-volume service which costs £5000 to set up and a charge per query of £1.77.

Either fee level suggests a significant deficit for the Scheme over ten years and so there needs to be further verifications from other government departments and the private sector. There is a question of whether the public sector is willing to pay for such services and a general question about the willingness of other government departments to buy into the Scheme. From the outset in 2002, identity cards have failed to win universal support amongst central government departments. The Home Office intended the Scheme to provide a "gold standard" identity infrastructure for use by all government departments and the Office of Government Commerce (OGC) Gateway reviews warned that "Practical, "joined-up" implementation across Departments will be essential" (Office of Government Commerce, 2003) and "The planning and implementation of the programme will need to continue to recognise the need of partner Departments to make a success of their own businesses alongside their participation in the ID Cards scheme" (Office of Government Commerce, 2004).

One might reasonably expect that if these other government departments were confident in the Home Office's ability to deliver the Scheme successfully they would have no problem being compelled to integrate their own systems with the Scheme. However, the Act places no obligation on other departments to make use of the Scheme.

Not mandating the use of the Scheme across government suggests major concerns with the project and goes against the stated government policy of providing "joined-up" government. For example, documents throughout the period from the Cabinet Office's "Privacy & Data Sharing" document (PIU, 2002) through to "Transformational Government" (Cabinet Office, 2005) have emphasized the Government's intention of pursuing joined-up government across the public sector.

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

The questions were addressed to a number of government departments and agencies and generally took the form of asking the Secretary of State for the Department:

> what estimate he has made of the (a) total and (b) net cost of (i) integrating the proposed identity card scheme into his Department's IT systems and (ii) the ongoing operation of the scheme within his Department. [Asked by Lynne Jones, MP for Birmingham on 21 November 2005]

while other questions took the form of asking departments:

> Whether they will publish (a) any analysis they have made of the potential use that the Department [in question] may make of the National Identity Register or identity cards introduced following enactment of the Identity Cards Bill; and (b) their estimate of the costs that will or may be incurred by the Department [in question] in connection with such use. [Asked by Baroness Anelay of St Johns, Baroness Noakes, and Baroness Seccombe]

Answers were received from

- Department for Constitutional Affairs;
- Department for Education and Skills;
- Department for Environment, Food and Rural Affairs;

- Department of Health;
- Department of Trade and Industry;
- Department of Transport;
- Department of Work and Pensions;
- Foreign and Commonwealth Office;
- Northern Ireland, Scotland and Wales Offices; and
- Treasury.

The responses to Parliamentary questions revealed that no department had taken a decision to integrate its systems and processes with the Scheme and none had conducted publishable research into the costs or benefits of doing so. Moreover, the responses received were all virtually identical suggesting a standard, centrally issued response:

> ... has, in consultation with the identity cards programme, developed its current best estimate of the costs and benefits of using the ID cards scheme to enhance its services and these have been incorporated into the business case.

Indeed there appear to be indications of resistance to take-up of the ID proposals. In answer to a question on take-up and integration costs from Lynne Jones MP, Treasury stated that it anticipated "no additional" integration costs with the Scheme "or to the on-going operation of the scheme within HM Treasury" [WA 31117]. In answering a similarly worded question from Baroness Anelay, the same department answered that "it had neither made a decision nor conducted research." These two answers prompt the quite reasonable conclusion that, at that time, Treasury had no plans to integrate with the Scheme.

In early 2008, a similar series of questions were asked. Again they had a standard form:

> To ask the Secretary of State for ... what plans his Department has to make use of data on the National Identity Register when it is established; and what the estimated annual cost to his Department of that use is. [Asked by Conservative MP Philip Hammond]

Responses were received from the following departments:

- Department of Business, Enterprise and Regulatory Reform;
- Department for Communities and Local Government;
- Department of Culture, Media and Sport;

- Department of Environment, Food and Rural Affairs;
- Department of Health;
- Department of Innovation, Universities and Skills;
- Department of Work and Pensions;
- Duchy of Lancaster;
- Foreign and Commonwealth Office;
- Ministry of Defence;
- Northern Ireland; and
- Treasury.

The responses received were, once again, virtually identical:

> The ... will be working with the Home Office prior to the introduction of the National Identity Scheme to establish how identity information held on the proposed National Identity Register might be used to provide easier access to ...'s services for our customers. It is too early in the process to establish the detailed costs and benefits.

Given that the Act had been in existence for almost two years at the time, these answers point to a continued lack of progress associated with government adoption of the Scheme that raises concerns about its cost effectiveness.

Assuming the Scheme is intended to be self-financing and subject to clarification of whether these other government departments will choose to use the Scheme for identity verification and be prepared to pay for the use of the identity infrastructure, any remaining deficit must be covered either by increasing the fee for receiving an identity card (a politically unpopular move) or by private sector use of the verification services.

The challenge for those who wish to understand the Scheme and for the government is to resolve the Home Office's expectations for income generated by verification services (estimated at around 4 verifications per person per year) with the fact that no one appears prepared to join the new infrastructure.

CHAPTER 5

Due process and short-circuiting debate

Does a thoroughly debated policy result in a better policy? Answering such a question requires going into the depths of political theory and philosophy. To add further confusion, does the essence of this question change when dealing with a technologically complex policy domain, where limited debate could limit scrutiny of a technology?

As qualifying a "good policy" is beyond the scope of this book, this chapter addresses this issue by approaching it from another perspective: instead of focusing on the policy itself, the focus is primarily on the quality of a particular aspect of the policy deliberation.

Together with the next three chapters, this chapter argues the case for a form of "due process" for the deliberation of technology-leveraged identity policies. It is generally understood that policies must go through some form of process of discussion, deliberation, and debate in order to pass the democratic test. It is also generally assumed that this democratic test is fair and appropriate and often a good thing in itself. By focusing on the challenges of technologically leveraged identity policies the chapter shows how the contentions around the policy and the implicated technologies require a different and perhaps more thorough form of policy process.

The review of the identity policies of a number of countries has already noted, with some concern, that identity policies were often established through minimal deliberation. Historically, some were developed during darker times where political debate was unlikely; others were implemented by government dictat. When a substantive debate did take place, limitations were often placed on the government's vision for an identity policy, whether to limit its budget, application, and/or effects on freedom and privacy. On some occasions, the policy was rejected outright.

Indeed, identity policy development can be intensely political. It should not be a surprise to anyone, therefore, that many governments try to avoid public debate on identity policy, or try to short-circuit the debate. First, governments have recently tried to point to international pressures and international obligations to adopt and transform existing identity policies, so as to avoid national debate and scrutiny. Second, governments have tried to limit debate and discussion around the technological essence of their proposals. Often these tactics are used simultaneously.

Policy laundering

Although the conventional understanding of policy tends to rely on a single-state deliberative process (such as the Parliamentary deliberations discussed in this book) the dynamics of policy-making are changing significantly. Increasingly, policies are being developed through international policy-making processes and transnational agreements. The number of these agreements keeps mounting, as do the places they are created. According to Alvarez (2002), the United States concluded over 10,000 treaties between 1970 and 1997 and Drezner notes that the number of intergovernmental organizations has doubled in the past 20 years (Drezner, 2001). All too often academic analysis downplays the role of these influences on national policies.

These international influences can be used strategically to minimize local deliberative processes. Hosein identifies three such strategies: Policy laundering is the practice whereby policy-makers "make use of other jurisdictions to circumvent national deliberative processes" (p. 187); "Modelling" occurs "when governments, overtly through calls of harmonization or subtly through quiet influence and translating of concepts, shape their laws based on laws developed in other jurisdictions" (p. 188). Finally, "forum shifting" occurs when "actors pursue rules in intergovernmental organisations (IGOs) that suit their purposes and interests and, when opposition and challenges arise, shift to other IGOs or agreement structures" (Hosein, 2004, p. 188).

Intergovernmental organizations and other institutions "channel and circumscribe the way state power is exercised" (Ikenberry, 1996, p. 62). International institutions may reduce transaction costs for developing norms, reduce ambiguity surrounding compliance, and provide high-quality information to policy-makers (Perritt Jr., 1998). Smaller states may participate in these forums, leading to the democratization of international policy and treaties (Alvarez, 2002). The dynamics at this international level involve power and selection, however.

Cooperating internationally and establishing international agreements are not neutral activities. Power politics may prevail, as countries may use international institutions to further their own ends when they find it convenient and disregard them when they do not (Slaughter, 2000). This "convenience" arises particularly when it serves a domestic political purpose (Goldstein, 1996).

For example, Goldstein (1996) notes how the Canada–United States free trade agreement actually served the interests of the Reagan administration in circumventing domestic institutions.

Not all institutions are ideal, and intergovernmental organizations function differently. Alvarez (2002) argues that "the choice of organizational venue speaks volumes concerning the intent of principal treaty backers" (p. 225). For example, the United States pursued antiterrorism rules in the 1970s through the International Civil Aviation Organization (ICAO) choosing the ICAO over the United Nations General Assembly in order to avoid the latter's inefficiencies.

In the same manner, when proposals for communications surveillance through the retention of communications data were put forward in the UK in 2000, they were not discussed at the UK level. Instead, the policy ended up being driven by a Council of European Union "framework decision" that would require all member states to have policies requiring retention (Whitley and Hosein, 2005).

Writing in 2003 before the UK proposals were debated in Parliament, Hosein noted the growing trend toward biometrically based travel documents and the introduction of identity databases. Speaking about the likely outcome for U.S. citizens, he asks "whether officials make use of 'international obligations' and harmonization articulations to justify the policy change" (p. 194).

This chapter shows how British officials made use of "international obligations" and policy laundering to support the specific proposals for identity cards in the UK.

International obligations on travel documents

As noted previously, the UK government has always intended that the roll-out of the Scheme will be linked to the issuing of passports. In addition, the identity card is intended to be valid as a travel document within Europe. As a result, it must satisfy the various requirements for machine-readable travel documents (MRTD) as specified by ICAO and others. The link between the minimum requirements for travel documents and the implementation of biometrically based identity cards has, however, frequently been presented as an obligation on the UK government as well as an inevitability.

Such "deterministic" arguments are frequently unsound both politically and academically (MacKenzie and Wajcman, 1999) as they fail to acknowledge the variety of factors that also shape the way an argument or policy develops (Aus, 2006; Hosein, 2004). That is, such deterministic arguments undermine the due process of effective scrutiny of policy proposals.

The claim of international obligations

Throughout the Parliamentary debate the government frequently referred to the "international obligations" on the UK to update its travel documents. For example, during a debate in the first cycle of the Bill, the then-Home Secretary informed Parliament that:

> under current plans, from next autumn, British tourists who need a new passport will have to have a biometric one to visit the United States, or a biometric visa instead. We will rightly have to bear the costs of introducing the new technology to enhance our passports in any case, but I believe that we should take the opportunity of that investment to secure wider benefits, such as those that I have just set out. [20 December 2004, Column 1942–1943]

A similar point was made by Mr Des Browne, then Minister for Citizenship and Immigration, during the Bill's first Committee stage:

> The scheme will give us – due to technological developments and the coincidence of the fact that we will be collecting biometrics in relation to a substantial proportion of the population for international travel documents and passports – the opportunity to make that step towards a system for proving people's identity to a proper, secure standard. [20 January 2005, Column 126]

He also noted that "the introduction of a facial image biometric in British passports starts in about a year" [20 January 2005, Column 158]. He continued

> The United States US Visit biometric scheme is already in operation and means that every British citizen who wants to visit the U.S. will need to enroll their fingerprints in anticipation of it. That measure does not affect British citizens immediately, but it will progressively do so. A substantial number of British citizens travel between the UK and the U.S. [20 January 2005, Column 158]

From this logic, the government argued that the cost of introducing identity cards would only be an additional £85 million (on an expected cost of £415 million associated with upgrading passports).

This logic was repeated during the second passage of the Bill. For example, the then-Home Secretary, Charles Clarke, told the House of Commons on 28 June 2005 that "As the House knows, the UK Government propose to introduce biometric passports to keep in line with developments in international standards through the International Civil Aviation Organization" [28 June 2005, Column 1159]. He continued:

> In the case of Europe, facial image and fingerprint biometrics, in line with those standards, will be required in passports issued by EU states under Council Regulation 2252/2004. Facial biometrics must be introduced by August 2006 and fingerprint biometrics three years after the technical specification has been agreed. All EU member states will have to introduce the same biometrics into the EU common format residence permits and visas for nationals of non-EU states.
>
> The United States has issued a further deadline for visa waiver programme countries to introduce facial image biometric passports from 26 October 2006. Biometric passports, or e-passports, incorporate an integrated circuit chip capable of storing the biographic information from the data page and a digitised photograph or other biometrics. Once all those United States requirements are implemented, nationals of those countries not issuing biometric passports will require a visa to visit the United States. The current cost of a United States non-immigrant biometric visa is £100, requiring a personal visit to London or Belfast and currently taking 31 working days to make an appointment for fingerprints to be recorded and a further three days to issue a visa. [28 June 2005, Column 1160]

He continued, noting that the "The effect of moving to a biometric passport is to raise the cost of the passport to of the order of £65 on each occasion. ... On top of that biometric passport cost, the biometric ID card would cost an additional £25 to £30" [28 June 2005, Column 1160].

In a similar manner, during a debate in the House of Lords, Lord Mackenzie of Framwellgate stated:

> In any event, we are being pushed by events. It will be an international obligation to have facial biometrics on passports by 2006. All passport applicants will be interviewed as an antifraud measure and it will be a European Union requirement for biometric residence permits and visas for foreign nationals by 2008. [31 October 2005, Column 62]

Thus, a frequent claim of the government, especially in response to the LSE alternative costings, was that 70 percent of the cost of identity cards would be required for implementing the second generation of biometric passports.

In parallel to the obligations on the UK, there is also a strong determinism in discussion about identity cards. Tony Blair referred to them as an "idea whose time had come" (Blair, 2005). He repeated the claim in November 2006 where he argued:

> The case for ID cards is a case not about liberty but about the modern world. Biometrics give us the chance to have secure identity and the bulk of the ID cards' cost will have to be spent on the new biometric passports in any event. (Blair, 2006)

Similarly, the 2005 Identity Cards Briefing from the Home Office under the heading "Why now" states that:

> Now is the right time to introduce an ID cards scheme because of advances in technology. ... These technological advances are now being adopted across the world to improve the security of travel documents and border controls. Following the 9/11 attacks, the U.S. toughened its immigration laws and introduced fingerprint biometric visas for those visiting the U.S. who required a visa. Countries such as the UK which are part of the U.S. visa waiver scheme must comply with new International Civil Aviation Organization (ICAO) standards and begin issuing biometric passports incorporating a facial image to remain in the scheme. ... the European Union has gone further and mandated both fingerprints 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. (Home Office, 2005c, p. 3)

Challenging the claim of international obligations

Chapter 7 of the LSE *main* report (LSE Identity Project, 2005c) specifically sought to address the claims of international obligations. The chapter reviewed the role of ICAO as well as U.S. and EU requirements for travel documents. This next section draws heavily on and updates this analysis.

For a number of years the international community has cooperated in increasing the security standards on passports. The UN-level agency responsible for these standards is the ICAO. In the late 1990s ICAO undertook research on the potential uses of biometrics and other forms of digitization of passport information but, in the years that followed, little progress was made (Stanton, 2008).

The U.S. Government enlivened the process with the USA-PATRIOT Act, passed by the U.S. 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 U.S. 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 cooperation 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). (Secretary of State, 2003)

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

When the issue of biometric passports passed to ICAO, the biometrics policy moved far beyond the Visa Waiver Program countries. As the international standard-setter for passports, 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 (Stanton, 2008).

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 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.

Key considerations for ICAO reviews included compatibility with existing enrolment, renewal, and verification requirements. Machine-readable passports have to be based on open (nonproprietary) standards and have graceful degradation capabilities in case of technological failure. For example, they have to be human-as well as machine-readable.

By 2003, facial recognition emerged as the primary candidate (ICAO, 2004). Intellectual property issues hindered the acceptance of iris scans, whereas facial recognition was believed to be more socially acceptable. International Civil Aviation Organization 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.

However, in 2003, the working group also noted 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. (ICAO, 2003, §3.3.3)

However, by attempting to accommodate flexibility for the varying demands of the member states of ICAO working groups, ICAO 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 U.S. does not record or verify iris scans. The inclusion of any additional biometrics is unnecessary for added international travel security. Thus the choice of biometrics to include in the system raises all the problems of large information infrastructures discussed in Chapter 4.

The ICAO's new position has given rise to two conditions. First, despite its goal of interoperability, the current international standard is flexible in the use of biometrics provided that all passports include the mandatory digital photograph. Second, 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. As a result, if British passports include, for example, iris scans then although these are not required for travel to the U.S., there is nothing that would prevent the U.S., or any other country, from collecting and storing this biometric information. In this way, design choices in a UK identity policy could result in unintended disclosure of personal data to third parties (cf ENISA, 2009).

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, ICAO is aware that there are contentious legal issues involved with the infrastructure for these passports, including potential conflict between the goals of centralizing citizens' biometrics and protecting privacy laws and collision with "cultural practices." According to ICAO documents, states should decide for themselves whether they extract biometrics from the passports of visitors or compare them to biometric databases.

Thus the ICAO 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. (ICAO, 2004)

As a result, ICAO guidance left states with a great level of discretion, which is contrary to the goal of harmonization. States could have biometric databases, or could choose to not do so; as long as states have digital photographs in their documents, they could require multiple further biometrics or none at all. This has led to a variety of (sometimes conflicting) implementations around the world and has permitted states to argue that the international "standard" is whatever they want it to be.

Analysis

EU specifications and actions

In Autumn 2004 the Council of the European Union decided to standardize all EU passports through the drafting of regulation and the European Parliament began consideration of a standardized biometric passport shortly afterwards (Aus, 2006). 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. In addition, if the Parliament had refused, the Council threatened to delay the introduction of the co-decision procedure for immigration and asylum issues to 1 April instead of the scheduled date of 1 January.

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

It is important to note that the United Kingdom is not bound by the EU specifications. The Council Regulation referred to by the UK Home Secretary explicitly states:

> This Regulation constitutes a development of provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC of 29 May 2000 (Council Regulation (EC), 2000) concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis. *The United Kingdom is therefore not taking part in its adoption and is not bound by it or subject to its application.* (Council Regulation (EC), 2004, §11, emphasis added)

Aus (2006) indicates that the UK challenged this decision.

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 (a tamper-proof image of the face – effectively a digitized, printed photograph rather than one that is pasted into the document) in its passport with the same minimal data held on the chip, this would not create a problem; in fact the results would be to the advantage of the UK, as it would reduce the costs and administrative burdens. Also, if the UK followed the U.S. requirements for a single biometric, the UK certainly would not have to worry about having a "second class" passport. Australia, Canada, and the U.S. have also rejected implementing additional biometrics in their own passports.

U.S. demands and requirements

It is useful to review the U.S. requirements and deadlines for machine-readable travel documents and the visa waiver program, particularly as these have slipped significantly in the time since the LSE *main* report was published. The USA-PATRIOT Act requires only that the President, within two years, certify a biometric technology standard for use in identifying aliens seeking admission into the U.S. The policy was modified by the Enhanced Border Security and Visa Entry Reform Act 2002, requiring that all visa-waiver program countries implement, by October 2004, biometric passport programs that satisfy 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 recognized that this could create a potential hazard as hundreds of thousands of visitors to the U.S. would have to apply for a visa, creating chaos at U.S. consulates and embassies.

The Secretaries of State and Homeland Security appealed to the 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 U.S. would "vote with their feet" and go elsewhere.

Congress responded unfavorably to this request and granted only a one-year extension. Countries had until October 2005 to implement new passport regimes that include a biometric.

Representative James Sensenbrenner is the Chairman of the Congressional committee responsible for the biometric passport deadline. He warned EU and UK diplomats against what he saw as unnecessary complications that were holding up the deployment process. According to one report, Representative Sensenbrenner expressed "dismay" that the European Union had 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. ... That the EU should choose an elaborate and expensive path to meet the requirement has led to consequences that are regrettable, but not insurmountable. (Zetter, 2005)

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. (Sensenbrenner Jr., 2005)

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

In response to continued failures from other governments to abide by the U.S. requirements, the U.S. 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 would not be required to implement chips in their passports until October 2006 (Department of State, 2005).

In order to comply with the ICAO standard, the U.S. is implementing a biometric passport of its own. However, the U.S., in compliance with the ICAO standard, is requiring only a digital photograph on a chip in the passport. Nevertheless, informal conversations with some Home Office officials suggest that even they, on occasion, accepted the narrative that the UK scheme had included fingerprints because the U.S. Government was requiring it.

Parliamentary challenges

In part inspired by the LSE analysis, a number of MPs questioned the obligatory nature of the requirements to update British passports. For example, during the debate on 28 June 2005, Lynne Jones asked whether the EU-wide passport with fingerprint biometrics was a proposal or a definite agreement, to which Charles Clarke replied that:

> the regulation to which I referred is binding on the Schengen countries, although not necessarily on us. However, it is expected that all

> EU member states will have to introduce the same biometrics into the EU common format residence permits and into visas for nationals of non-EU states.
>
> I should point out to my hon. Friend and to others who are concerned about this issue that in the view of all observers, there is absolutely no doubt that the development of biometric travel documents in the ways that I have described is the future. Given that environment, we would seriously disadvantage the citizens of this country if we did not go down the biometric route. [28 June 2005, Column 1161]

It is important to note that the UK government played a significant role at both ICAO deliberations and the Council of the European Union. So the UK government knew full well the nature of the requirements, because it had lobbied hard for them (Stanton, 2008).

However, by the time of the remaining stages of the Commons debate, the government was resorting to the language of obligation once again, with Home Office minister Andy Burnham informing the House of Commons that:

> The European Union has already agreed to move in the direction of requiring the widespread use of biometrics. The United States has also taken such a decision in principle, as has the International Civil Aviation Organization, to which my hon. Friend the Member for Birmingham, Selly Oak referred a few moments ago. It is up to the hon. Gentleman if he wants the British Government to stand back from that and thus ensure that British citizens have second-class passports that will not enable them to travel with freedom and convenience in the future, but Labour Members will not take that decision. [18 October 2005, Column 740]

Similarly, during the Lords second reading debate, the Home Office minister Baroness Scotland again referred to the fact that "70 per cent of that cost would be incurred anyway because of the worldwide move to biometric passports" [31 October 2005, Column 15]. Later in the same debate the Earl of Northesk asked the Baroness to:

> confirm that the International Civil Aviation Organization has been absolutely adamant that what is not required as an international standard is a biometric passport; what actually is required is a digitised version of the biometric? That is one of the fictions which the Government consistently parade as a justification for the Identity Cards Bill. It is

> very important that it should be knocked on the head. [31 October 2005, Column 110]

Despite this explicit attempt at clarification, in the debate on 14 December 2005, Lord Bassam, representing the government, stated "that around 70 per cent of the unit cost would be accounted for anyway by the cost of introducing biometric passports with both facial image and fingerprint biometrics" [14 December 2005, Column 1280].

The matter came to head during the debate on 13 February 2006 that considered Lords' amendments. Once again, the inevitable introduction of biometric passports and the associated costs was raised by the government. However, when the Home Secretary told the House that "A number of countries, including the United States of America" had passports with 13 sets of biometric data on a centrally held database he was "invited to be quite careful about this" by MP Edward Garnier [13 February 2006, Column 1171]. He responded by clarifying his claim:

> We are in an evolving situation as far as the international requirements are concerned. That applies to the EU, the International Civil Aviation Organization and the UN Security Council resolution. It is equally the case that many countries are evolving their own systems. ... It is also true that there are different states of decision in different countries on those points. All is evolving. However, both within the EU and in the dialogue between the EU and the United States that has explicitly addressed these matters, including in the G8 context, the overwhelming view is to move towards the most rigorous form of biometrics for fundamental documents such as passports and visas. [13 February 2006, Column 1171]

This statement was followed up by a Parliamentary question seeking clarification of the "evidential basis was for his statement that a number of countries, including the U.S., propose to have 13 sets of biometric data per person on a centrally held database." The written answer stated:

> I am clear from discussions with my opposite numbers internationally that a number of other countries, including the United States are likely to move to using 13 biometrics in due course, based on face fingerprints and iris biometrics. The use of multiple biometrics has been accepted in principle in the International Civil Aviation Organization (ICAO) Blueprint for machine readable travel documents which has been accepted by the 188 ICAO contracting states and includes the

> face as the primary mandatory biometric and iris or fingerprints as secondary and optional biometrics. [WA 57293]

Nevertheless, despite these various opportunities for the government to clarify the relationship between obligations that it was under and best practice that it had chosen to follow, the claim about the need to upgrade passports continued to be made, including in the first s.37 Cost Report (UKIPS, 2006a) issued in October 2006 and the Strategic Action Plan issued in December 2006 (UKIPS, 2006b) and has remained an element of the rhetoric of government documents about identity cards thereafter.

The National Audit Office's review of the introduction of e-Passports (National Audit Office, 2007), however, does provide a clear statement of the issue:

> To ensure that UK citizens can travel freely, ePassports must conform to standards set by the International Organization for Standardization on the design of the chip and data formats and by the International Civil Aviation Organization on the overall design and features of the ePassport, including the data and the security features protecting it. ... The latter organisation requires that the chip contains an image of the passport holder's face. ... There are additional EU requirements specifying that by 2009 ePassports should include fingerprint data which will require personal attendance for fingerprint enrolment. The UK is not obliged to comply with the EU regulations as it is not a signatory of the Schengen Agreement but *has decided to do so voluntarily* so that it can participate in the development of the EU regulations and maintain the security of the British passport on a par with other major EU nations. (National Audit Office, 2007, §1.7 emphasis added)

Though it took nearly four years, finally the policy-debate could be perceived as settled: fingerprints are merely an optional component of ICAO's standards and an optional component of the EU policy as well. Moreover, when the OGC Gateway Review documents were finally released in 2009, it was apparent that the early plans for identity cards were not based on these "international obligations."

For example, the June 2003 Review states that the collection of biometrics is "another option" that the government "would like to explore" (Office of Government Commerce, 2003, p. 3). It continues, noting that:

> Opinion seems divided on how effective or dependable biometrics will be. There is little past experience, in the UK or elsewhere, to go on.

> Pilots will be especially important. (Office of Government Commerce, 2003, p. 11)

In the January 2004 OGC Review, the Review Team notes that:

> Biometric passports are already being developed in the UK, elsewhere in Europe and the U.S. partly in response to this situation. The U.S. has announced that a biometric will shortly be required for foreign nationals entering the U.S. (Office of Government Commerce, 2004, p. 1)

The Review continues by noting that:

> there is general agreement that there should be a second biometric as well as the photograph (or digital photograph). On the assumption that DNA would be too expensive, however, should it be fingerprints or irises (or both)? How scalable are the two technologies? And what are the cost implications? It was put to us that EU Directives and international passport standards might leave little option but to use fingerprints (which could also, unlike irises, be compared with existing stocks held by the police and others). The matter needs, however, to be firmly decided. (Office of Government Commerce, 2004, p. 11)

Discussion

One way of telling the story about the UK scheme would be to say that the Home Office early on decided that it wanted to use the best available technologies and the most promising future technologies to record the unique identifying features of the entire population. A project of this scale had never previously been conducted and it was likely to be politically contentious and technologically challenging and consequently expensive. The merits of the technologies and the needs of the system design meant that the choice of biometrics was settled and the Bill was drafted. Parliament then approved the Bill and the Identity Cards Act became law.

Another version of the story, however, is that the government knew that the Bill would have a rough ride through Parliament because of its costs and technology implications. The Government therefore chose to use the international policy processes to their advantage. First, they would push for international policies requiring expansive biometric collection. Then, every time the policy was questioned in Parliament the government could point to the international standards and obligations requiring that the Act merely comply.

In so doing, the Government had devised a perfect strategy. For the "internationalists" in Parliament, though they may oppose an identity card they would certainly abide by international obligations (particularly from the UN) in the quest for global harmony. The pro-EU MPs would not turn down something that had been approved by the European Parliament. With the "security hawks" that may oppose the bill, including members of the Conservative Party, the Government could argue that without these advanced technologies the UK would have a "second-class" passport that would be vulnerable to fraud while other countries would not suffer so needlessly. Finally, to those who questioned identity cards on the grounds of public policy, where considerations of costs and feasibility would be raised, the Government could easily claim that much of the costs for the identity card were to be incurred anyways due to the international obligation to implement UN requirements.

By using international policy-making strategies, the Government tried to short-circuit debate around identity policy. It was not alone, of course. Germany implemented fingerprints in their identity cards on the back of ICAO requirements. Similarly, France proposed collecting eight-fingerprints for their identity scheme. Members of the Bush Administration cabinet, in their final days in office, began complaining that European practices of fingerprint collection were helping the EU to secure their identity documents and the U.S. should consider following suit.

In addition to questions of parliamentary accountability, a particular concern about such tactics for technologically leveraged identity policy is that governments could actually limit scrutiny of the technological basis of the proposed policy. At the European Parliament, just as in the UK Parliament, not a single feasibility study or technology study was introduced to inform Parliamentarians about the advantages, disadvantages, or potential for failure (indeed, as the OGC Review noted, "there is little past experience, in the UK or elsewhere, to go on" (Office of Government Commerce, 2003)). The common view, identified in discussions with Parliamentarians, was that because the technology was approved by UN bodies, the technologies must be ready for application.

The ICAO did not scrutinize the technology in detail either, however. At a conference presentation from a member of the ICAO technology working group, the member admitted that when ICAO approved some of the technologies in the standard, they were unsure of the abilities of the technology to match their goals. In fact, in the case of the standard on "contact-less" chips for the biometric passports, the ICAO member later admitted that he did not even know what a contact-less chip was, at the time. Further examples of this confusion about what a contact-less chip might be arose in the UK (Lettice, 2006).

Therefore, the greatest risk that emerges from policy laundering is not necessarily that Governments can short-circuit debate; but rather that the policies are never adequately reviewed at any level as each level presumes that the other level will or has done it.

CHAPTER 6

Due process and the politics of science and technology

Policy-making processes need, amongst other things, good information about the nature of the problem being addressed by the new policy, consideration of the variety of possible solutions or measures, and possibly recognition of the identity of the key constituencies for engagement and building political support. To this, experience has shown that for technologically-leveraged policies the process requires a further component: a detailed understanding of the technologies implicated by the policy.

As the review in the previous chapter about the short-circuiting of debate on identity policy by using international standards and obligations to their advantage showed, some governments appear keen to minimize discussion of technology. In the case of international obligations on the use of biometrics there were limited feasibility studies and discussions of the merits of one technology over another were more focused on the characteristics of the market conditions around the technologies rather than their relative effectiveness.

Even though some governments are keen to push new technologies, this is not necessarily a problem. The review of emerging identity policies around the world has shown that some governments are keen to start discussions on identity policies using new techniques and for new environments such as for on-line transactions and even mobile authentication, truly leveraging the capabilities of new technologies to transform the public sector (Fishenden, 2009).

Therefore this concern does not arise from some sense of skepticism about technology. Rather it seeks discussion and debate about the essence of the technologies implicated by identity policies.

This needs to go beyond "being specific about the technology" (Monteiro and Hanseth, 1995). When compelled into disclosing details, governments often have many statistics to offer and are unlikely to spread falsehoods with the disclosure of these details. Rather the approach advocated is that the essences of technologies must be debated, because they are seldom settled upon. Grint and Woolgar (1997) criticize the idea that there is a truth about a technology, something within its capacity that determines how it acts. This chapter takes this criticism to focus on the discourse and the debate over the essences of the technologies and from these debates analyze the competition of claims about the technology.

Alternative knowledge claims occur frequently in policy debates; this chapter shows that they may also be about the technology. Therefore a technology policy process will include actors and institutions that have differing views on the technologies. Sometimes these may be opposition parties, other times they may be special interest groups. Sometimes the interests are not entirely clear or necessarily discernable, as Haas' identifies with his epistemic communities of scientists and experts (Haas, 1989). These claims add richness and color to the policy-making process and can lead to a settlement on the understanding of the essence of the technologies. But there is possibly more than a mere settlement that could be achieved through this process.

In the case of the UK, although the extent of the politicization (and personalization) of the debate surrounding the LSE report was surprising, the reaction of the government to alternative knowledge claims, especially with regard to the science and technology underlying the Scheme, was less surprising as it had been foreshadowed by Bruno Latour in his argument about the Politics of Nature (2004).

In this work, Latour decries the tendency for politics to short-circuit "any and all questioning as to the nature of the complex bonds between the science and societies, through the invocation of Science as the only salvation from the prison of the social world" (p. 13). That is, he argues that politics prefers to see only scientific facts and would rather not see the detailed work associated with scientific controversies.

In response, Latour proposes a due process model for building a "common world" that acknowledges that in many cases (e.g. in terms of nature, global warming, mad cow disease, GM crops) scientific consensus does not (yet) exist, yet there is a need for (political) action to take place and decisions to be made. Latour's model proposes replacing the invocation of Science as the provider of truth with a mechanism for consideration of "perplexities" that could be part of the new common world.

Before discussing how the debate over the essence of the technology occurred in the UK, the chapter develops an analytical frame to better understand the technology policy process itself from the perspective of alternative knowledge claims. That is, in order to demonstrate the effect of this approach this chapter describes how the first round of Parliamentary discussion sought to short-circuit the scientific and technological perplexities associated with the government's plans. This is followed by the presentation of some of the new candidates for the common world associated with the implementation of the Scheme. Finally, the chapter shows how the government reacted to the possibility of considering these alternative knowledge claims.

From facts and values to due process

Science and technology have traditionally been seen as distinct from society, with their own internal logic and status (Barry, 2001, p. 7). For example, Habermas (1970) argues that "scientific experts advise the decision-makers and politicians consult scientists in accordance with practical needs" (Habermas, 1970, pp. 66–67). In this view, scientific experts are seen to provide politicians with the "facts" that they need in order to implement policy. However, one of the key insights of the academic field known as Science and Technology Studies (STS) has been to question this separation of science and society and to undertake detailed empirical study of the work that scientists and technologists actually do, rather than accepting their status uncritically (Barnes et al., 1996; Bijker et al., 1987; Collins, 1981; Latour, 1999).

This has resulted in an extensive body of STS research that has shown all the instruments, laboratories, workshops, and factories that work to "fabricate" the "facts" that science produces, the alliances that lead to consensus and shared understandings and the variety of interests and interpretations that are essential to those understandings (e.g. Bauchspies et al., 2006; Yearley, 2005).

Nevertheless many political decisions to build a "common world" need to be able to "use science and technology before there is consensus in the technical community" (Collins and Evans, 2007, p. 8) as science cannot deliver truth at the speed politics requires (p. 1). Latour suggests that this results in a tendency to short-circuit the scientific process and invoke scientific knowledge as truth despite the growing evidence that, for scientific controversies, reaching unanimous positions is a difficult, time-consuming process.

Part of the problem, Latour suggests, is the language used. When politicians cite scientific "facts" they are really talking about two very different things associated with science. On the one hand, scientific facts are related to matters of concern which may be well or badly "articulated." The work of scientists is therefore to develop experiments and experimental apparatus that identify and better articulate these matters of concern so that one can decide if they are "serious, stable, delimited, present, or whether they may not soon, through another experiment, another trial, scatter into as many artifacts, reducing the number of those whose existence matters" (p. 103). These many matters of concern leave those who are discussing them "perplexed" (p. 104). Matters of fact, on the other hand, are indisputable, institutionalized knowledge claims that represent the "unanimous text of a resolution on the state of the art" (p. 64), claims that need not be reconsidered and belong once and for all "to the realm of reality" (p. 98).

The short-circuiting of due process arises when both aspects of scientific work in the term "facts" are combined and then separated from "values." A similar mishmash of responsibilities, Latour suggests, can be found with consideration of values that covers processes for consultation about possible members of the common world and the process of organizing them into a hierarchy.

Latour (2004) therefore proposes a new separation of powers that prohibits the short cut from scientific perplexity to scientific institution and proposes proper consideration of the perplexities that are candidates for the new common world. This can be seen diagrammatically in Table 6.1 The traditional fact/value distinction and Table 6.2 Latour's new division of powers.

Thus, using Latour's language, the political deliberation of the science and technology associated with the National Identity Scheme was short-circuiting the consideration of the perplexities associated with both the use of biometrics and the single, centralized database associated with the National Identity Register (NIR). The LSE report therefore sought to contribute to the scrutiny of the Scheme by explicitly raising these candidate perplexities.

Short-circuiting deliberations

It is possible to identify numerous examples of the short-circuiting of deliberations of scientific and technological elements of the Scheme, and in the early stages of debate this process was rarely questioned.

Table 6.1 The traditional fact/value distinction

Facts	Values
Perplexity	Consultation
Institution	Hierarchy

Table 6.2 Latour's new division of powers

Perplexity	Consultation	**How many are we?**
Institution	Hierarchy	**Can we live together?**

In particular, the House of Commons Home Affairs Committee (HAC) (2004) scrutinized the draft legislation. The cross-party Committee's work is independent, with Government ministers responding to the questions and concerns of Committee. The HAC noted that while they did not have the expertise to make judgments on the technological issues, they were struck by "witnesses' insistence on the importance of the Government getting the structure right from the beginning and sticking to its decisions" (Home Affairs Committee, 2004, Recommendation 31). Similarly, in terms of biometrics the HAC noted "that no comparable system of this size has been introduced anywhere in the world" (Home Affairs Committee, 2004, Recommendation 39).

Despite the early identification of these concerns, in the first round of Parliamentary debate, which is led entirely by the Government, there was very little consideration given to alternative knowledge claims and perplexities about the science and technology underlying the Scheme. For example, the only discussion of biometrics revolved around consideration of the Government's own small-scale pilot trials (Mansfield and Rejman-Greene, 2003), concerns about unstable (facial) biometrics for people under 16 (who are not due to be enrolled into the Scheme) and some discussion of how biometrics could, in theory, be spoofed.

Similarly, debate about the NIR was very limited, with little more than occasional comments about the risks of the database being hacked into or corrupted, even by viruses. The government's responses to such concerns relied on assurances that the government had taken "the best possible advice in this area" from relevant industry and academic experts.

Introducing perplexities

Perplexities for the National Identity Register

The Government's line of argument was that most other countries have identity cards (particularly those in Europe) and that the Government was developing the Scheme in order to be consistent with the practices elsewhere. The LSE report questioned this logic by pointing out that not all identity systems are the same; see also the review in Chapter 2 of this book. Although most European countries have some form of identity card, the LSE's research showed that not all are compulsory (LSE Identity Project, 2006a) and few, if any, are based on a central database that provides an audit trail of every time the identity card is formally used to verify an individual's identity.

As was noted earlier, 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. Under Federal Data Protection Law, the Federal Government is forbidden from creating a back-end database of biometrics for the identity card. As a result, German privacy law prevents the creation of the kind of central database envisaged for the UK. Instead, any information that is collected for the identity card system is stored locally at the registration offices. A private contractor uses this information to issue the card but as soon as the document is completed all personal data are deleted and destroyed.

In a similar manner, alternative models exist about the use of the single national identification number for government services. France explicitly does not use a single identifier to link government records across departments. Hungary and Germany explicitly ban the use of a single identification number for citizens, citing data protection concerns, while Hungary and the Czech Republic do not allow shared databases across government departments (Otjacques et al., 2007). The Austrian e-government initiative has introduced a novel technology-based solution, where all Austrian citizens are registered on a national Central Register of Residents but have a variety of identification numbers that link to the central records via sector-specific tags and strong encryption algorithms (Otjacques et al., 2007).

While Ministers were trying to show that a centralized design was the only option, they were ignoring the extensive debates elsewhere about whether identification systems should be centralized or federated. Over the years, a number of companies tried to present themselves as the one-stop-shop for centralizing identity information. For instance, Microsoft tried to implement a “Passport” scheme where it would hold all your identity information (e.g. log-in details for all your on-line accounts) and would manage them accordingly. Under this (failed) scheme Microsoft would know every transaction you made but it also ran the risk of becoming the central point of failure for all your on-line accounts and a high-profile target for hackers. Other companies proposed (as Microsoft now does) federated and distributed schemes where there are multiple, independent identity assurance providers who have far less information on their users and are at lower risk of failure. Along with the LSE reports, a number of industry experts and bodies promoted this federated scheme over the government’s centralized model.

Perplexities with biometrics

The government's faith in biometrics was remarkable. Repeated statements from Ministers and even the Prime Minister indicated that they believed that biometrics made the entire scheme not only possible, but necessary (cf Office of Government Commerce, 2003). The LSE report challenged the belief in the perfectibility of biometrics noting evidence that suggested that there were significant potential problems with each of the proposed biometrics, especially when the Scheme is rolled out for the entire UK population (i.e. upwards of 50 million people).

The LSE report did not do any biometric testing of its own, but instead presented an alternative review of the available scientific evidence. The LSE analyses highlighted the key role of the "experimental setup" in determining the efficacy of biometrics. Most of the existing studies, for example "frequent traveller" studies, had carefully arranged setups (e.g. controlled lighting) and limited profiles (typically white, male professionals aged 20–55). Issues raised by such studies as well as concerns about their applicability to the wider, more heterogeneous population highlighted the need for the studies to be carefully reviewed to isolate the effects of the experimental setup from the underlying science being evaluated (cf Collins, 1992; Collins and Pinch, 1998a).

The LSE researchers also reviewed the evidence given to Parliament and to the government warning of the error rates with fingerprints, the limited large-scale tests of iris systems, and the unreliability of facial recognition techniques (e.g. British Telecommunications PLC, 2004). It also considered government-commissioned studies that warned of the perplexities of enrolment and subsequent error rates (Mansfield et al., 2001) and the challenges (and likely costs) of dealing with large populations in a way that is untried (Mansfield and Rejman-Greene, 2003). The report also looked to the studies conducted in other countries, particularly in the U.S. (e.g. NIST, 2005; Government Accountability Office, 2005).

The LSE reports were able to identify perplexities that the government was glossing over, given the size of the biometric database. These included the need to contain very accurate biometrics to prevent false nonmatches and a verification process that would have to involve high-integrity devices to avoid excessive false matches. Moreover, in relation to spoofing and other attacks, the LSE reports noted techniques for forging or counterfeiting fingerprints (Matsumoto et al., 2002) and relayed findings of researchers in Germany who established that there were forgery vulnerabilities in iris recognition (Anonymous, n.d.).

Responses to perplexities

With the publication of LSE reports, the Parliamentary deliberations about most aspects of the Scheme (including the scientific and technological elements) now included consideration of many of the issues that the reports highlighted, often with an explicit reference to the LSE as the source. This section describes how the government responded to the perplexities that the LSE reports introduced into the Parliamentary scrutiny of the Scheme and suggests that rather than seeking to embrace the kind of due process that Latour suggests, the government attempted, once again, to short-circuit the deliberations by invoking their experts and their interpretations of the issues.

Contests of experts: Technology design and the LSE alternative blueprint

Given the concerns with the government proposals, the LSE reports outlined an alternative scheme based on federated databases for identity data. It also avoided relying on biometrics to help achieve a perfect, unique identification and enrolment process, by drawing upon existing social networks and endorsements by individuals in positions of trust in society to implement the enrolment and identification process.

In August 2005 the Home Office issued its response to the LSE alternative blueprint (Home Office, 2005b). In this document, the Home Office noted that “the Government has consulted with over 300 organizations and acknowledged leading universities in the field of biometrics” (p. 1).

Discussing the design choice of a central database, the Home Office response draws on “common sense”: “For example, a bank or supermarket does not leave small amounts of cash in its tills overnight; it transfers this cash to a safe – a highly secure central environment. This is more cost-effective than making every individual till as secure as the safe.” They also point to industry “best practice”: “a centralized database model is recognised by leading IT, security and resilience specialists to provide the most secure and cost-effective way to administer the personal details of individuals. Requirements for the National Identity Register will comply with such industry standard best practice. The LSE model would not” (p. 5) adding that “The Government have been working with acknowledged security experts to ensure the Scheme will meet highest industry standards” (p. 7).

Biometrics and the selective use of sources

Discussion of the LSE analysis of the available biometric evidence was even more nuanced. One argument made by the government in dismissing the LSE's presentation of the perplexities associated with biometrics was the "surprising" "basic error" of missing "one of the major reports on biometrics and the way in which that was dealt with in the United States" [Baroness Scotland, 19 December 2005, Column 1565].

As Home Office minister Baroness Scotland informed the House of Lords:

> One of the largest scientific studies today of fingerprints, with a sample size of 6 million, was conducted by the United States National Institute of Standards and Technology using data collected in operational circumstances, rather than laboratory conditions. It showed a performance consistent with the needs of a scheme on the scale of the ID cards scheme. Although it was one of the world's leading studies into the use of biometrics, the London School of Economics overlooked it in its report, which is curious because we know how assiduous that body usually is when looking at research that may be pertinent. I am surprised that the LSE does not appear to have alighted on that study. One reason why we treat the LSE study with caution is because it is just not as rigorous as one would normally come to expect. [15 November 2005, Column 1057]

The LSE research status report issued in January 2006 (LSE Identity Project, 2006c) reviewed this point. This noted that the LSE Identity Project was:

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

Thus, both the LSE report and the Home Office were drawing upon the same evidence, supporting Fuchs's (1992) claim that "knowledge claims are always 'underdetermined' by the available evidence, so that alternative claims are always equally justifiable in the light of that very same evidence" (p. 21; see also Collins, 1992; Collins and Pinch, 1998b).

Discussion

While the previous chapter has shown how governments have used geopolitics to short-circuit debate and deliberation (Hosein, 2004; Whitley and Hosein, 2005), this chapter has shown how debate was short-circuited on technology issues. In any political debate, the management of knowledge is likely to be used in political ways and Latour's model provides a means of addressing the tendency to short-circuit deliberation, not just in the area of nature, but also technology and potentially many other areas as well.

By utilizing Latour's concerns about due process, the LSE Identity Project transformed the debate about the identity cards policy in the UK. It did this by introducing a range of candidate entities about biometrics and the design of the NIR, perplexities that the government was attempting to gloss over. At one level, this did result in a better due process consideration of these elements as they were, at least, considered in the debates about the Scheme.

The government, however, continued to short-circuit the consideration of these elements by invoking its own interpretation of the science and technology involved and challenging the status of the report that introduced the candidate entities. This approach, however, was not always totally effective (Pieri, 2009). For example, shortly before a key debate in the House of Commons, a former British NATO and defense security expert Brian Gladman wrote to the Prime Minister to respond to the government's attacks on the quality of the LSE's research. Gladman informed the Prime Minister that he was the (unacknowledged) author of the sections of the LSE report dealing with safety and security of the NIR and that his material had been reviewed by two independent and internationally recognized information security experts. This was subsequently covered by the media (Hencke and Dodd, 2006), causing considerable embarrassment to the government.

At another level, the due process might be seen to be less effective, at least in terms of the Parliamentary debate. The Bill was passed and on 31 March 2006 the Identity Cards Act received Royal Assent. Apart from a commitment for periodic reporting on costs and a few other minor amendments, the final form of the Act is very similar to the original Bill. As such, it would appear that despite the presence of the various perplexities that the LSE report introduced into the debate, the controversy was settled. However, as the years move on from the launch of the LSE report, the plans for the Scheme remain in a state of flux, with a delayed roll-out of the Scheme for UK citizens and further consultation about the collection of biometrics (UKIPS, 2008b). Iris biometrics, despite being explicitly listed in the Act as an example of biometric information (a "matter of fact"?), have been dropped from the Scheme. Similarly, the government announced that the NIR would now be implemented on three distinct databases, rather than a single, centralized Register (UKIPS, 2006b), a decision that has received higher prominence following the notorious tax agency data breach where the personal details of 25 million UK citizens were lost from a single, centralized database.

At a more general level, this case contributes to the ongoing debate about what it means to be political. For example, a recent paper by Whittle and Spicer (2008) suggests that actor-network theory and, by implication, STS more generally, degrades our understanding of political action by arguing that only human intervention can lead to the transformation of social arrangements. Such a position comes close to reinforcing the traditional separation of scientific knowledge from social action. If this logic had been followed in the identity cards case, it would risk encouraging "a passive attitude to an enormously important part of our lives" (MacKenzie and Wajcman, 1999, p. xiv).

Latour's book describes six professions or skill sets that can contribute to the implementation of the politics of nature: scientist, politician, economist, moralist, bureaucrat, and diplomat. The experiences with the LSE report suggest at least one other skill set to add to this mix, namely the *informed advocate*. This skill set is closely related to those of the moralist, whom Latour describes as actively looking for candidate perplexities that should be given due consideration, as a matter of principle.

The informed advocate differs from the moralist, however, in that while the moralist's concerns are purely processual, informed advocates use their interactional expertise (Collins and Evans, 2007) to identify those candidate entities that are most likely to contribute usefully to the deliberative process. Although they are short listing and highlighting likely candidate perplexities, informed advocates are not shortcutting the political process as other candidate perplexities can also be included, for example by the moralists. They are simply using their expertise to identify the most challenging entities for the current iteration of the process.

Thus the LSE report drew on the relations with appropriate contributory experts to identify those perplexities that were most likely to be significant for the implementation of the Scheme. This involved interacting with experts in areas as diverse as policing policy, law as well as information technology and biometrics. The skills required for the broad ranging interactional expertise for modern policy processes differ from the specialist expertise provided by scientists.

"Advocate" can be seen as a dirty word, particularly in academia that is supposed to be unbiased and disinterested. The difference is methodological rather than necessarily ideological. Rather than just finding evidence that opposed the government's view of the world, as researchers the LSE Identity Project presented sources of evidence that contradicted, confused, and also clarified issues. The academic challenge is to provide coherence to all this dissonance in ways that are digestible to the key audiences. It also requires the presentation of conflicting evidence in ways that are not perceived as merely providing obstructions.

The case also identifies aspects of the due process model that are not covered in Latour's analysis. For example, throughout the period under study many aspects of the Scheme were not specified in detail and yet the government's position was one of certainty about the Scheme (e.g. the likely cost of the Scheme remained unchanged). Thus, the short-circuiting of due process appears to have been undertaken not just on the basis of scientific facts but also on the basis of expectations about the Scheme. This is explored in more detail in Chapter 8.

It is possible that in a highly politicized process where no side can show weakness, governments must short-circuit due process in order to show confidence, certainty, and assurance. Yet, neglecting perplexities is a hazardous way to develop policy. If this condition is endemic to the political process then the implications for future technology policies are worrying.

CHAPTER 7

Intentional ambiguity about technology

> We will introduce ID cards, including biometric data like fingerprints, backed up by a national register and rolling out initially on a voluntary basis as people renew their passports. (The Labour Party, 2005, pp. 52–53)
>
> 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. (Home Office, 2005e)

Much is made about how our societies have changed in the era of rolling 24-hour news coverage and how governments are far more accountable today than in previous times because of the sheer amount of information that is now made available. Whitepapers, green papers, consultation documents, public speeches, Parliamentary debates, and media interviews are now all available for the public, researchers, and analysts to study. This information can be codified, weighted, interpreted, or counted in order to draw conclusions about the quality and quantity of public disclosure, discussion, and even deliberation.

Despite attempts to short-circuit the debate about identity policy described previously, surprising amounts of information have been made public. Thus, much information has been made available about international standards for passport security; access to the working papers, and minutes of meetings of international institutions such as International Civil Aviation Organisation have been made available through freedom of information requests in the U.S.

It is also recognized that governments are no longer the sole holders of the wisdom on these policies as the traditional boundaries between different areas of research, policy, and practice break down (Gibbons et al., 1994). Research on the various techniques implicated by modern identity policy is often circulated within academia, standards bodies, and for public discussion through conferences and media coverage.

In the case of the UK, the government was willing to speak often about its proposed identity policy. The proposals went through Parliament twice, so there was much discussion of the Scheme. A record of these debates (Hansard) including detailed consideration of the Bill at the Committee stage is freely available on the Parliament website (Bayley, 2004). Ministers spoke at dozens of conferences, interacted with hundreds of journalists, offering insight into their thinking and their intentions. Whitepapers and consultation documents were released from the earliest stages of the policy-making process. The Bill itself was released with a "regulatory impact assessment" that outlined the larger implications of the bill in language that was clearer than is possible in legislative language (Home Office, 2005e).

In modern policy debates, therefore, there is rarely a shortage of information. Where shortages arise, controversy often follows and through a variety of mechanisms, researchers, or informed advocates work at finding this information and ensuring its release. But the mere availability of information does not in and of itself help in understanding a policy process, the policy itself, or the intentions of the policy-makers.

In monitoring the policy process it is important to analyze the publicly available information about the policy, but it is also important to pay attention to how this information is presented, particularly when the statements are made about technological issues associated with the policy. This chapter focuses on the two statements which are presented above – statements about technology-related issues that were intentionally ambiguous and therefore hampered the effective scrutiny of the government's identity policy proposals.

On information, meaning, and information systems research

Although theories of information and meaning have their origins as a technological measure of signal quality (Shannon and Weaver, 1949), information and meaning have become increasingly important for information systems researchers (Willcocks and Whitley, 2009). In the positivist research tradition, information and meaning have been studied in many areas including computer-mediated communication, decision support systems, and computer adoption. Within the interpretive tradition, particular emphasis has been given to the social nature of information in a variety of contexts, and information is generally recognized to be something that has inextricably contextual characteristics (Brown and Duguid, 2002; Klein and Myers, 1999; Poster, 1990). In particular, information is often understood in relation to our use of language (and signs more generally) and as a result is best understood in terms of the particular social and historical circumstances of those who use it (Introna, 1997; Searle, 1969; Stamper, 1973; Winograd and Flores, 1986).

Although some theories of language imply a direct mapping between words and the world (Lyytinen, 1985), many others suggest that language is socially and culturally shaped (Lakoff and Johnson, 1980). Amongst the most influential theoretical approaches are semiotics, Wittgenstein's later work on language, Habermas' theory of ideal speech situations, Berger and Luckmann's social construction of reality, Searle's "construction of social reality," and Gadamer's hermeneutic approach (Jones, 2000).

One theory of meaning that has been widely used in information systems and organizational research is semiotics. Stamper (1973) argues for an understanding of meaning based on the signs that are used and exchanged in organizational contexts, emphasizing the difference between formal and informal systems (Liebenau and Backhouse, 1991).

Ludwig Wittgenstein's later philosophy of language (Wittgenstein, 1956) introduced the notion that meanings and understandings are very much a social outcome and cannot be produced by just one person (i.e. a private language is meaningless). Peter Berger and Thomas Luckmann (1966) present a related theory of institutions, legitimations, and socializations that also emphasize the role of social practice where "language marks the coordinates of my life in society and fills that life with meaningful objects" (p. 36).

John Searle (1995) takes the argument further, arguing that social reality (things like money, marriage, etc.) is the result of collective agreement to assign a new (deontic) status to something that goes beyond its original (physical) properties. Thus we (collectively) assign the status "money" to pieces of paper (that have the appropriate printed marks on them, are the right kind of paper, etc.). This new status is over and above the paperness of the paper and so this new status must take the form of a linguistic marker since the physical object is unchanged. Searle argues that speech acts are used to create and destroy these new statuses (Searle, 1969).

The work of Jürgen Habermas (e.g. Habermas, 1984, 1987) on the conditions for effective communication in ideal speech situations also uses the notion of speech acts. This approach also sees language as socially based, but highlights the typical inequalities that exist when language is normally used and proposes an alternative, less constrained opportunity for communication.

For many interpretivist researchers, however, perhaps the most influential approach (if not always the most frequently cited) is hermeneutics as proposed by Gadamer and advocated in information systems research by Boland (1983), Chalmers (2004), Walsham (1993), and Westrup (1994) amongst others. Although hermeneutics started out as the study of sacred texts it is now taken to be associated with the interpretation of any textual materials.

Researchers such as Boland (e.g. 1991), Introna (e.g. 1997), and Lee (1994) take this further and draw on Ricoeur's philosophical hermeneutics (Ricoeur, 1981) and his notion of Distanciation as a means to interpret textual materials found in organizational life. Distanciation emphasizes the separation (distance) between the authors (and what they meant) and the readers (and what they understand). This Distanciation always arises with texts, but can cause particular issues when information spans the boundaries between different contexts and user groups (e.g. Collins et al., 1985; Marche, 1991; Wenger, 1999). In particular, problems arise when different groups form different interpretations of the same information, causing or revealing major organizational issues (Lee, 1994).

In the context of technology, this means that different groups, for example developers and users, can shape their use of language differently as very distinct social and historical circumstances can emerge because of differing levels of engagement with the technological artifact. As a consequence, when such different groups come together their language use might not be straightforward and many problems may surface.

The analysis in this chapter distinguishes between two kinds of problems of meaning that can arise in such situations: misunderstanding and intentional ambiguity. Misunderstandings arise when one group fails to appreciate the particular meanings that another group has given to particular terms and concepts. Once misunderstandings have been noticed (Whitley, 1996), there is a variety of well-understood mechanisms for addressing them. These typically involve making the background assumptions behind the differing interpretations explicit and developing a shared understanding and agreement of the terms being used (Collins and Kusch, 1998; Habermas, 1984, 1987; Winograd and Flores, 1986).

In some cases, however, such clarifications are not possible because the language used is intentionally ambiguous. As before, terms used can be accorded more than one meaning, but in this case it is not apparent that one particular meaning was intended by the group first using the term, that is, it was intentionally ambiguous.

Misunderstandings and intentional ambiguity

With meaning closely intertwined with the use of language and social convention determining how language is to be understood (Kent, 1978), it is perhaps surprising that we make ourselves understood so easily. Many daily interactions are with individuals and groups who have a very different socialization from us and who would have different meanings and understandings for the information we share. It is only when shared norms and expectations evolve out of repeated interactions and explanations that we can begin to learn a shared understanding and avoid many problems of misunderstanding (Collins and Kusch, 1998; Duguid, 2005; Wenger, 1999).

For example, the information that there is some water in the refrigerator can be understood differently by someone looking for something to drink, someone looking for pure water for a car radiator, or someone searching for a source of moisture (Winograd and Flores, 1986). Confusion over what is meant by "water" in this situation will only be resolved when agreement over what is meant by the term is reached (Whitley, 1996).

Examples of misunderstandings are particularly likely to be found in discourse surrounding the implementation of new technological systems. At company level, this can arise because of the inevitable technological complexity of the new system, coupled with the lack of expertise that most executives have for technological matters. At the level of implementation, similar problems arise, especially when different groups are brought together to implement the system. In each case, it takes time for shared meanings and understandings to be arrived at, if they ever do.

Unless one is wedded to the idea that everything must be clear and well defined and that steps should be taken to ensure that this happens (Te'eni, 2001), these socially determined different meanings are not necessarily problematic, with some authors highlighting the benefits of openness that ambiguity can provide (Eisenberg and Witten, 1987). In information systems, Swanson and Ramiller's (2004) discussion of mindful and mindless innovation relates to how some companies seek to deal with "ambiguous, portentous and disruptive issues of organizational transformation and strategic repositioning" (p. 554). Wang and Ramiller (2004) develop this approach to study the ways in which the trade press provide different kinds of information over time as the organizing vision of Enterprise Resource Planning systems develops and becomes increasingly well understood.

Within organization studies more generally, there is a stream of research that has focused on the strategic use of ambiguity to achieve particular, often political, aims (Alvesson, 1993; Davenport and Leitch, 2005; Eisenberg, 1984).

Eisenberg (1984) takes ambiguity and explicitly makes it an aspect of some organizational strategies. For him, openness in communications is not necessarily a desirable attribute (Eisenberg and Witten, 1987) and ambiguity allows for more flexible organizational communications by creating a space in which multiple interpretations by stakeholders can exist and multiple responses are possible.

Similarly, Alvesson (1993) suggests that ambiguity involves uncertainty, contradictions that cannot be resolved, absence of agreement on boundaries and is a crucial element of organization. In particular, ambiguity cannot be clarified by gathering more facts, but instead opens up a space for new organizational activities.

For some organizational contexts, a key characteristic of ambiguous statements that allows progress to be made is their deniability (Davenport and Leitch, 2005 p.1606). Thus, one mechanism that can be used if an ambiguous statement causes organizational stalemates is to deny that certain meanings were ever intended. Davenport and Leitch (2005) present an analysis of a New Zealand research funding agency that sought to change the basis of its policies for funding research. The new policy used the ambiguous phrase "investment operations" and talked of "portfolio management" and "investment principles" along with an associated "disinvestment strategy." For those academic stakeholders who were concerned about their funding being withdrawn, this new language was worrying. The funding council was therefore required to draw upon the deniability of this particular claim and argue that this was not what they had intended to be understood by their proposals.

Giroux (2006) questions the relationship between language and ambiguity in her review of the adoption of the term "Quality Management." She labels the ambiguity she studies as "pragmatic" rather than strategic to emphasize the often unintentional ways in which such strategic ambiguity arises and develops. In contrast, this chapter focuses on strategic ambiguity that is intentional.

This chapter develops the concept of intentional ambiguity to examine the two short statements presented at the start of the chapter. The two statements came to be key elements of the Parliamentary debate about the proposals and, despite their apparent clarity, turned out to be very ambiguous and were interpreted in very different ways by different stakeholders in the policy process (e.g. House of Commons and House of Lords, 2006, Volume 2 §3.6).

The concept of intentional ambiguity becomes particularly significant for policy analysis because, unlike misunderstandings, intentional ambiguity cannot be easily resolved by clarifying what was meant. Instead, when problems with intentionally ambiguous statements unravel, the only resolution involves "translating" key aspects of policy in unexpected ways, thus further limiting the ability to effectively scrutinize the technological aspects of the policy itself.

An analytical theory for studying ambiguity and its consequences

According to Gregor (2006) analytic theories focus on "what is" rather than seeking to explain causality or attempting predictive generalizations. As such, the analytical theory for studying intentional ambiguity in this chapter presents a means of classifying cases of ambiguity as distinct from misunderstandings and presents some of the strategies used to translate the policy when the statements unravel.

The first step is to identify the case as one of intentional ambiguity rather than simple misunderstanding. Misunderstandings arise in situations where the same piece of information may have different interpretations for different people, often as a result of different experiences of socialization (Collins and Kusch, 1998; Whitley, 1997). Misunderstandings, therefore, can normally be resolved by making these differing viewpoints and experiences explicit and reaching agreement as to which meaning is most appropriate for the situation, or which test of meaning should be applied in that case (Boltanski and Thevenot, 2006 [1991]). Thus, a misunderstanding about what was meant by water can be resolved by, for example, agreeing that for that group the term "water" will only refer to pure water.

Intentional ambiguity, in contrast, is not the consequence of different forms of socialization. Instead, it arises in situations where the author of the ambiguous text is aware of the problems that might arise but chooses to use the ambiguity to open up space for alternative actions and in so doing obviate the problems that would arise by seeking to clarify the information at that time. That is, the ambiguity is intentional. In the case of the New Zealand funding body described by Davenport and Leitch (2005), for example, the funders could have chosen to explain clearly that their policy was to redistribute funding to more closely reflect the changing priorities of the funding body. To do so, however, could have resulted in direct conflict with those researchers whose funding would be reduced.

This case, however, also shows that the choice of the ambiguous investment metaphor did not succeed in avoiding conflict as the chosen language became widely understood to be problematic and needed to be addressed before the purposeful action of the agency could be continued.

In situations such as these, where intentional ambiguity "unravels," organizational activities around the ambiguous information come to a halt. Since straightforward clarification of different socializations and understandings cannot be found, the situation must be altered in some way for the impasse to be overcome. In order to do this, this chapter draws on the notion of translation as it has been articulated by Callon and Latour in the context of actor-network theory.

Callon (1986) introduces translation as one of the four moments in his sociology of association. Translation, Latour (1987) points out, has two common meanings, both of which are implied in actor-network theory: a linguistic one relating versions in one language to those in another and a geometric one involving movement from one place to another. Translations are undertaken by mediators that "transform, translate, distort, [or] modify the meaning or the elements they are supposed to carry" (Latour, 2005 p. 59). Therefore translations transform the situation to resolve the impasse that arises.

In the policy process, such translations are likely to result in unintended and unexpected consequences that transform the policy. These changes can limit the scrutiny of the policy proposals and as such should be avoided wherever possible.

Voluntary enrolment into the Scheme

Although the Government has been clear that its intention is to eventually make the Scheme compulsory, the initial proposals were for a Scheme where enrolment was voluntary, linked to the renewal of passports. Compulsion would follow at a later stage, once a significant proportion of the UK population had enrolled into the voluntary scheme. Given that the arguments for compulsion in an area like identity cards are complex and politically uncertain (Perri 6, 2005), opposition parties picked on the fact that the Government was not proposing a Scheme that was compulsory from the start but instead had this link to passports. Thus, Liberal Democrat MP Sir Robert Smith suggested that not making identity cards compulsory from the start:

> suggests that it would not be a popular scheme if it were left to the voluntary initiative of individuals to decide to register on the database? By doing this, are not the Government recognising that the scheme will be unpopular? [18 October 2005, Column 750]

The issue of how to enroll people into the Scheme underlies the first statement given at the start of this chapter. This statement was made in the Labour Party election manifesto in 2005 and, at first sight, indicates that the Scheme would roll-out on a voluntary basis. However, as shown below, a key question about the technological implementation of the Scheme hangs on what is meant by the link to the issuance and renewal of passports. The differing interpretations of this linkage between identity cards and passports formed the basis for a major constitutional crisis between the House of Commons and the House of Lords (Whitaker, 2006).

In the UK Parliamentary system, membership of the House of Commons is decided by a general election held within five years of the last election. Members of the House of Lords are unelected and include honorary peers (in the Lords because of family or other historical reasons) and appointed peers (often former MPs and other dignitaries).

With the ruling party in the House of Commons elected by the general public, on the basis of the manifesto commitments as presented at the General Election, an important question of political precedence arises when members of the (unelected) House of Lords wish to challenge legislation that is proposed by the elected House of Commons.

In some cases, the amendments proposed by the House of Lords are recognized as valuable contributions to the proposed legislation and may be accepted by the House of Commons, even if they run counter to manifesto commitments. In other cases, however, the House of Commons may claim priority over the House of Lords, as the public voted for them on the basis of their published manifesto. (In some cases, of course, especially later in the life of a Parliament, government may propose legislation that was never mentioned in any election manifesto, which falls outside this discussion.)

When this issue of precedence has arisen in the past, a convention, the Salisbury Convention, has been proposed that effectively dictates that when a manifesto commitment is challenged by the House of Lords, the House of Lords must bow to the will of “the other place” (as one house refers to the other house, in this case how the Lords refer to the House of Commons) and accept the manifesto pledge.

Thus discussions about the meaning of the manifesto statement were not simply academic exercises where “any word, phrase or sentence or utterance can, with sufficient ingenuity, be accorded more than one meaning” (Coulter, 1985, p. 12). Rather, the issue became a major constitutional crisis between the unelected House of Lords and the elected House of Commons. The debate, therefore, recursively developed to consider whether the Salisbury Convention applied in this case and whether, more generally, Lords had a constitutional right to argue against a potentially undesirable scheme.

The debate about voluntary enrolment

The issue of voluntary versus compulsory enrolment into the Scheme was first raised during the House of Commons Committee Stage, but primarily in relation to the issue of whether it would be possible to charge people who apply for a voluntary card but not charge those who are forced to apply for a compulsory card [e.g. 12 July 2005, Column 245]. The main debate about voluntary enrolment took place after the end of the Committee stage.

Misunderstanding or ambiguity?

Initially Government representatives made strong claims that the situation was neither one of misunderstanding nor ambiguity. For instance, Home Office minister Baroness Scotland stated:

> The Government have been absolutely clear that their policy was for identity cards; that their policy was for compulsory cards; and that this is the way in which we seek to deliver them. It was our clear intention throughout the period 2002 to 2005, before the general election, that this procedure would be adopted; that is, the same procedure that comes before the House today. [23 January 2006, Column 974]

She continued:

> We have been clear about what has been offered to members of the public. The Government have been utterly straightforward and frank in that regard. [23 January 2006, Column 975]

In the House of Commons, the then-Home Secretary Charles Clarke made a very similar point:

> Election manifestos cannot possibly deal with every detail of an existing policy, but it is clear to me that, in saying very explicitly that the roll-out would initially be on a voluntary basis, the manifesto refers to what has always been the Government's position. ... That position is that the scheme will initially be based on a stand-alone identity card,

> issued on its own on a voluntary basis, or together with a document such as a passport, which is also issued on a voluntary basis. That seems to be clear and unequivocal. [13 March 2006 : Column 1249]

Nevertheless, members of the House of Lords opposed to the Bill took a different view, suggesting that the manifesto commitment meant exactly the opposite of that claimed by the Government. For example, Liberal Democrat and leading opponent of the Bill, Lord Phillips of Sudbury suggested that:

> If ever a matter was not merely not clear but rather clearer in the opposite direction has been made manifestly plain this afternoon. [23 January 2006, Column 975]

This sentiment was echoed by opposition MPs, including Conservative MP Edward Garnier who noted:

> The words are plain and their meaning is obvious. I doubt that anybody, even the Home Secretary, is confused by what the Government intended that the public should understand before the general election in 2005. [13 March 2006, Column 1251]

Intentional ambiguity?

Some of the debate about whether the manifesto wording was intentionally ambiguous centerd on the process by which election manifestos are written. Bara (2005) notes that manifestos contain a range of statements from specific pledges to campaign rhetoric. Using her approach, the statement in question would be classified as a "specific"/"detailed," rather than "general"/"vague," pledge. Manifestos are "labouriously produced by party members, bureaucrats and advisors and are approved by party leaderships" (Bara, 2005 p. 586). This point was addressed to Baroness Scotland who had been trying to suggest that the opposition parties were exploiting "infelicitous" drafting. She was challenged on this by Conservative Peer Baroness Anelay who asked Baroness Scotland if she had had direct experience of drafting manifestos:

> If she has, she will know that every word, in every sentence, in every manifesto is pored over, discussed, decided and cleared at the highest level. The pledge that ID cards would be rolled out voluntarily will have been agreed personally by the Prime Minister, as it would by

> every Prime Minister and by the Home Secretary. So the Government must have decided deliberately on the wording in the manifesto. They had the chance to state openly in the manifesto that, if elected, they would force us all to be registered and to pay for an ID card, but they chose not to do so. [15 Mar 2006, Column 1231–1232]

MPs and Lords made numerous suggestions for ways in which the ambiguity could have been avoided, implying that the choice of words used in the manifesto was very deliberate. For example, Lord Phillips of Sudbury suggested that:

> If as they now claim the intention all along was for the scheme to be compulsory, they only had to change one crucial word or add one clarifying phrase. [23 January 2006, Column 958]

In the Commons Conservative Home Affairs spokesperson David Davis claimed that:

> To justify what this Bill does, the Labour manifesto should have said: "We will introduce ID cards, including biometric data like fingerprints, backed up by a national register and rolling out initially on a compulsory basis for a progressively larger portion of the population as people renew their passports." [13 February 2006, Column 1179]

They were joined by Baroness Anelay who declared that:

> Ministers had a chance to state clearly and openly in the manifesto that if elected they would force us all to be registered and to pay for an ID card with our passport before being given the freedom to go abroad for work, for a holiday, or for whatever reason – but they did not take that opportunity. That was their choice. [6 March 2006, Column 555]

Translations

The intentionally ambiguous wording about the voluntary roll-out of the Scheme resulted in the Bill "ping-ponging" between the House of Commons and the House of Lords and so various strategies were proposed to resolve the issue. These initially drew on the notion that the issue was simply a case of a misunderstanding. The strategies used referred directly to the words used in the manifesto and drew on various arguments about the nature of language. These were later developed into broader arguments about compulsion, especially in relation to passports, in part echoing some of the arguments outlined by Perri 6 (2005).

The issue was eventually resolved by a far more radical translation of the situation, following an amendment introduced by former Cabinet Secretary Lord Armstrong. Each of these strategies is now reviewed.

Liberal Democrat Home Affairs spokesperson MP Nick Clegg (and current party leader) noted that "this debate is ... about our specific disagreement on the meaning of that one word," i.e. "the Government now seek to persuade us that 'voluntary' actually means 'compulsory' " [13 March 2006, Column 1254].

The argument about a "lay person's" use of language was made by a number of speakers throughout the passage of the Bill. For example, Baroness Anelay, speaking on 20 March 2006 suggested that:

> Any normal person reading the manifesto commitment on this matter would interpret that commitment as, "When I renew my passport, I can choose whether I go on the register and have an ID card. And if I don't want to, I can choose not to." That is what "voluntary" would initially mean to anyone who read it. [20 March 2006, Column 26]

Lord Phillips of Sudbury also expressed disbelief that the debate was continuing in the form that it had:

> It staggers me that we are still discussing that point. Try that argument out on anyone in the high street or in a pub and you will get an "are you mad?" look. [15 March 2006, Column 1227]

In the House of Commons Conservative MP John Selwyn Gummer argued:

> To tell us that we cannot have a passport unless we are prepared to pay extra for something that we do not want is not to suggest that we have a voluntary choice. ... I say to the Home Secretary very directly: no one outside this House believes you. No one thinks that what you say, as a translation of the Labour party manifesto, is what anyone else ever thought and those on the Benches behind you do not believe it either, because they are honourable men who understand what the English language says. [13 March 2006, Column 1256]

Arguments about language more generally were made by various speakers including Baroness Anelay:

> The Government's definition of "voluntary" is very different from anything that I have ever come across. It is a case of, "have an ID card or don't leave the country." That is not right. [23 January 2006, Column 970]

Conservative MP Edward Garnier suggested that:

> The problem facing the Government is that they have, as usual, misused the English language. When they say "voluntary," they mean "compulsory" and that is why they have got stuck. When they say "may," they mean "must" and when they say "possibly," they mean "definitely." [13 February 2006, Column 1152]

In a debate a month later he noted:

> It is clear beyond doubt that the Government know that their case is flawed ... They knew what "voluntary" means, but now they pretend it means something else ... It is about a Government who are guilty of intellectual dishonesty on a grand scale and who do not have the decency or the common sense to understand that, admittedly unusually, the public have read their manifesto and taken them at their word. [13 March 2006, Column 1251]

Another attempt at translating the problem to resolve the impasse drew on formal definitions of language. For example, Nick Clegg used the Oxford English Dictionary which:

> gives the following definition of "voluntary": "done, given, or acting of one's own free will." [13 March 2006, Column 1254]

In the House of Lords, Lord Phillips of Sudbury drew on his childhood experiences:

> I am afraid that my primary school teacher, Miss Lovelace, would have given Mr Clarke 0 out of 10 for that. She would have pointed out ... that the word "voluntary" in that sentence related to ID cards, not passports. [15 March 2006, Column 1226]

Labour MP Anne Snelgrove drew on her own experiences as an English teacher:

> I shall give him an English lesson if that is what he wants. In our manifesto, we understood that ID cards would be "rolling out on a voluntary basis as people renewed their passports."
>
> We know what that means. [16 March 2006, Column 1649]

Edward Garnier had a different training in English as he argued:

> it does not take much knowledge of the English language and its syntax to realise that the expression "on a voluntary basis" governs the phrase "will introduce ID cards." [21 March 2006, Column 186]

In parallel with the linguistic arguments about the meaning of the word "voluntary" another strategy was attempted using the very documents that were being linked with enrolment into the Scheme, namely passports. In this case there were arguments about the right to have a passport and about the need to travel in certain circumstances. Thus, Viscount Bledisloe argued: "The indirect compulsion denies me the right to travel if I apply only for a passport that I do want, but not for an identity card that I do not want" [23 January 2006, Column 974].

Some, including Viscount Bledisloe questioned the right of an individual to hold a passport:

> Is it compatible with the freedom of the individual and the Human Rights Act that one shall be debarred from exercising the freedom to move about the world unless one "chooses" to go on some other government register and to pay them an extra fee for that privilege? [23 January 2006, Column 964]

In the Commons, Mr Clarke reaffirmed that:

> Passports are voluntary documents – [Laughter]. Well, of course they are. No one is forced to renew a passport if they choose not to do so. That will remain the case once we begin issuing identity cards alongside passports. [13 March 2006, Column 1249]

Related to this point was the need to hold a passport in order to travel, David Davis suggested that holding a passport was not always voluntary:

> That is not the case if someone's work takes them abroad, nor if their parents live abroad, nor if their spouse or partner is from another country. Nor is it the case if their children travel abroad, fall sick or get into trouble. It is a novel interpretation of "voluntary" if the price of a foreign holiday is a requirement for inclusion in the national identity register. [13 February 2006, Column 1179]

However, despite the ingenuity of these various strategies for resolving the ambiguity, none succeeded because the ambiguity was intentional and not the result of differing socialization or interpretation of terms. Whilst strategies of clarification can succeed for misunderstandings, they do not work in cases of intentional ambiguity. Instead, it is necessary for the policy to be translated and radically transformed. This is precisely what happened. Following the ping-ponging of the proposals between the Lords and the Commons, former Cabinet Secretary Lord Armstrong proposed an Amendment that "would restore an element of voluntariness – of personal freedom – which is absent from the Government's proposals" [28 March 2006, Column 651], whereby an individual applying for a passport may "opt out" of being issued with an identity card until 1 January 2010, although their details would still be recorded on the Register (Wadham et al., 2006, ch. 4).

Although Lord Armstrong's Amendment was initially rejected by the Labour Government, it did receive opposition support and was finally accepted by both Houses on 29 March 2006, allowing the Bill to receive Royal Assent the following day. Whilst the Amendment did address the issue of "voluntary" enrolment until 2010, it continued to mix issues about the issue of an identity card with the recording of details on the Register. Moreover, resulting delays and reorganization of plans for the Scheme have meant that, in effect, the clause is unlikely to have any significant effect on the current roll-out, voluntary or not.

Costing the Scheme

The debate about costs took a very different path to that about the voluntary enrolment with the Scheme. As was shown above, the discussion about voluntary enrolment and attempts to resolve the ambiguity took place at many different times during the Parliamentary process. By contrast, the debate about the ambiguity over the issue of costs had a very clear timeline, driven by a single event that caused the ambiguity to be resolved.

Government IT projects, as examples of large IT projects, often have a poor success record. This seems to be particularly the case with UK government projects (Craig and Brooks, 2006; Dunleavy et al., 2006; Organ, 2003). The accumulated independent evidence on large complex IT projects is that they have been, and always will be, high risk in terms of implementation and unanticipated costs. The key risk dimensions include high complexity, large size, innovativeness of technology, integration issues, number of units and stakeholders affected, overambitious timescales, and overreliance on technologists and IT suppliers for development and implementation (e.g. Collingridge, 1992; Royal Academy of Engineering and British Computer Society, 2003; Sauer and Willcocks, 2001; Willcocks and Griffiths, 1997; Willcocks et al., 2003).

In this context, it is unsurprising that Parliamentarians were concerned about the government's ability to deliver the large, complex scheme that lay behind the legislative proposals. In order to address these concerns, the government's Regulatory Impact Assessment (Home Office, 2005e) included the second statement listed at the start of the chapter, claiming that the total average annual running costs for issuing passports and identity cards to UK nationals was estimated at £584m per year. (When the earlier version of the Bill had been introduced in 2004, the associated Regulatory Impact Assessment had said that current projections "forecast annual operating costs of UKPS of £415m in 2008/09" (Home Office, 2004), that is, the estimates had risen by £169m per annum).

The debate about costs

In June 2005 the LSE Identity Project published its alternative costings of the Scheme, which suggested that the likely cost of the Scheme could range between £10 and £19 billion over ten years. The government repeatedly stood by its claim of a fully costed estimate of £584m per year for ten years. Indeed, in one Parliamentary debate, the Home Secretary suggested that the claim was accurate and indeed, that the figure was "likely to go down, rather than up" [13 February 2006, Column 1118].

Over time, however, the topic of costs and the discrepancy between the Home Office estimate and the range of figures produced by the LSE became so controversial that the Home Office decided that it needed to bring in an external organization to review its costings and to give them a stamp of approval. Throughout the process the Home Office refused to share the details of its costs with Parliament claiming that the figures were "commercially confidential," that is, if they were to disclose the details of the costings they may prejudice the future contract bidding process and fail to achieve best value for money for the government.

The Government hired an accounting firm, KPMG, to review 60 percent of their costs model and released, on 7 November 2005, a small excerpt of KPMG's final report (KPMG, 2005).

The KPMG excerpt began with a clear endorsement of the government's model as being robust. While the rest of the report made a number of substantive criticisms of the Home Office's costings model, ministers were able to repeat time and again that "KPMG has found the cost claims to be robust."

Misunderstanding or ambiguity?

For a large part of the debate, the government statement on costs was not seen as confusing or ambiguous: it was accepted at face value. Indeed, for a while, the most contentious issue around costs appeared to be clarifying what was meant by the term "billion": a thousand million or a million million.

When the likely costs of the Scheme were challenged, the focus of debate was on the likelihood that the government's figures were a good estimate, given that alternative costings from the LSE were far higher.

The basis of the government statement, however, was not challenged. For example, Labour MP Mr David Winnick said:

> Even if we dismiss the figures of the London School of Economics, which may have exaggerated the costs, it is pretty certain that the costs now ventured by the Government are unlikely to be the final costs. Who really believes otherwise? [28 June 2005, Column 1184]

Another Labour MP, Mr Austin Mitchell said:

> The costs will be enormous. The Government estimates keep going up and will go up again. The current estimates are going up even before anything has happened and they are bound to increase further. The LSE estimate of the costs, which varies between £10.6 billion and £19.2 billion, with a median of £14.5 billion, seems to me to be far more accurate. [28 June 2005, Column 1215]

Intentional ambiguity?

Until November 2005, although Parliamentarians did not believe the government's predicted costs, no one in Parliament suggested that they were intentionally ambiguous. However, at a public meeting organized by the LSE Identity Project at the House of Lords on 9 November 2005, the carefully worded statement about costings began to unravel. The LSE group organized the event and invited speakers from academia, representatives from industry and the Minister responsible for the Bill, Andy Burnham.

One of the academics, Simon Davies, had taken part in a number of public debates on the topic with the Minister on previous occasions, including one the previous day. On this occasion, however, the Minister diverted from his carefully chosen words and revealed a narrower definition of costs for the Home Office estimate than had previously been given. That is, he clarified that the £584m per year was only the cost to be incurred by the Home Office itself, for the administration of the system and not the cost to the Home Office as a whole (e.g. immigration services), let alone the government as a whole (e.g. costs of implementing biometric readers and changing systems at welfare and benefits offices).

Immediately following the meeting and surprised by the Minister's candor, the LSE Identity Project wrote to him seeking confirmation of what he had said (Angell, 2005). He replied, posting his response on the Identity Cards website (Burnham, 2005). In this letter he stated that:

> Decisions on whether, when and how particular public services will make use of the ID cards scheme will be made by those services – individually or collectively as appropriate depending on how services are managed. (Burnham, 2005)

He continued:

> There is therefore no "one size fits all" ready-reckoner to estimate the costs across all public services as each case is different. (Burnham, 2005)

For some government departments, he suggested, integration costs can be designed into new systems, but for others:

> integration costs will be absorbed in the usual cycle of system upgrades and technology refresh. Rather than having to incur the costs of a

> specific project to "ID-enable" their system they will wait and plan it into their upgrade and maintenance cycles.
>
> Where costs of using the ID cards scheme have been identified, they are included in the business case of calculating the net present value of the scheme. It would not be appropriate to include these costs as part of the issuing costs of the scheme. (Burnham, 2005)

This answer revealed two important aspects of the way the government had intentionally presented its own cost estimates in an ambiguous manner. First, it made clear that set-up costs were not included in the figure of £584 million per annum. Second, their costings also did not include any costs that were likely to be incurred by other government departments that might (choose to) make use of the Scheme. The cost to the taxpayer, rather than the Home Office, was therefore likely to be much higher than had previously been presented. An essential difference between the two costings was becoming quite clear: whilst the LSE report had included the costs of the larger scheme, for example, the costs of implementing biometric readers at benefits offices and in police cars, etc., the Home Office was only calculating the costs to itself and even then only the costs of operating the scheme.

Translations

This new understanding of the government's statement on costs was immediately picked up in the next Parliamentary debate, in the House of Lords on 15 November 2005, where Lord Waddington asked:

> I should like to put some very straightforward questions to the Government. When they put forward a figure of £5.8 billion, are they talking purely about the launching costs for the Home Office? Are they excluding all the other costs involved for the scheme to have any use at all? Those other costs will clearly involve adapting the computer systems in other government departments so that they may have access to the Home Office computer and to the information on the Register. What will be the cost of adapting all those computer systems so that others may use the information kept on the National Identity Register? Am I right in saying that those costs are not included in the figure of £5.8 billion put forward by the Government? If I am, what is the total figure?

> Nobody has begun to answer, on behalf of the Government, these crucial questions and I hope that if the Minister cannot answer us today she will give a firm undertaking to give a detailed statement of these costs as soon as possible and before we proceed very much further with the Bill. I agree entirely with the noble Lord, Lord Barnett, that it is very difficult to debate any of these matters when the costs may be so astronomical as not to equate with any benefits that will accrue from the scheme. [15 November 2005, Column 973]

In responding to this question, Baroness Scotland replied:

> I gave those costs at Second Reading but I am very happy to reiterate the comments that I made then for my noble friend Lord Barnett and I shall indicate how the costs are made up. We have estimated that the annual running cost is £584 million per year. A number of commentators have aggregated those sums and given a 10-year estimate and they say that over 10 years the cost would be £5.8 billion. But that is a 10-year figure, not an annual figure. We have produced the annual figure. I hope that I indicated it clearly at Second Reading. [15 November 2005, Column 983]

When pressed on the set-up and wider costs, she replied:

> First, I have already sought to deal with the issue of developmental costs and commercial confidentiality and why we have difficulties in relation to those matters. Secondly, the cost for the identity card is £584 million. Thirdly, the costs for other government departments will be for those departments. We would not expect Home Office costs for manning immigration controls, for instance, to be paid for from the passport fee, nor should the cost, if any, of checking identity cards be paid for from the identity card fee. So the figures that we are giving are those that we have estimated as the annual cost of issuing identity cards and passports. [15 November 2005, Column 984]

In the remainder of the debate that day, the government struggled to convince the peers that it was appropriate for them to approve the legislation on the basis of the costs to the Home Office of setting up the scheme, rather than the costs to government as a whole.

The next day, the issue of the missing capital costs reappeared, with Lord Phillips of Sudbury announcing that:

> It completely defeats me how it could have allowed through to this place a Bill with no indication of the capital costs which are attendant

> on it, let alone the capital costs of integrating between government departments. [16 November 2005, Column 1132]

And the issue arose again, emphasizing the intentional way that the Government had presented its costings, led by Conservative Party front-bench peer Baroness Noakes:

> We regard it as unacceptable that the Government have introduced legislation that will have far-reaching effects on the citizens of this country without being prepared to discuss the full costings with Parliament. I cannot think of a precedent for this ...
>
> There was some confusion in the earlier days of Committee about whether the Government's own estimated annual costs of £584 million covered both revenue and capital costs. The Minister repeatedly said that the £584 million is the annual running cost, which implies that it includes nothing for capital costs and, possibly, other up-front costs.
>
> Suffice it to say that the capital costs are a major matter of dispute. That reinforces the need for Parliament to look at precisely what is in those figures and how allowances are made for capital spend, both during and after the initial phase of implementing the Bill. [19 December 2005, Column 1545]

In January 2006, Baroness Noakes reported:

> Our Committee stage was unusual, in that we failed to get any useful information, despite spending several hours on the matter. In fact, our only achievement was to establish with more precision what the Government would not tell us about costs. [16 January 2006, Column 428]

Faced with this intentional ambiguity, the opposition Lords voted through an amendment that sought more information about the costs before the Scheme would proceed. As Lord Phillips of Sudbury noted:

> I would not be as adamant about this – and, I am sure, many of your Lordships would not feel as keenly – were it not that what information we have been given has been extracted with as much difficulty as if we were pulling out the Prime Minister's teeth. [16 January 2006, Column 431]

This was reinforced by a statement by Baroness Noakes in the same debate:

> The Minister's figure of £584 million is only a small slice of the overall picture – it is the big picture that we are trying to see. [16 January 2006, Column 429]

When the Lords amendment on costs returned to the House of Commons, the government faced a tricky problem. To accept the Lords amendment would delay the Scheme considerably, but to simply reject it would be to imply to MPs (the holders of the public purse) that the desire for more information on costs was unreasonable. Instead, the Government supported an Amendment from Labour MP Frank Dobson which "would impose a requirement on the Government to report every six months to the House on the latest estimated cost of the ID scheme, if it goes ahead" [13 February 2006, Column 1220].

Dobson made it clear that although the Government supported his Amendment, he did not himself have confidence in the Scheme. He did not believe that it would provide value for money, bring an end to terrorism, or have much impact on identity fraud.

In the Commons debate, concern about the Government's ability to deliver on budget and the precision of the estimate were once again raised. With the Government's majority in the House of Commons, the Dobson Amendment was passed and the Lords, not seeking another fight with the Commons, voted to accept this alternative Amendment in place of their own.

Every six months thereafter the government has been providing increasingly detailed cost reports about the Scheme. In addition to providing some transparency to Parliamentarians as to the progress of the Scheme, each cost report has been widely covered in the media, keeping the Scheme and the concerns with it, in the public imagination throughout this period (Whitley, 2009).

Discussion

The intentional use of ambiguous language raises important questions for the policy process. However, one might argue that the realpolitik of deliberative democracy sometimes requires such economy with the truth. The challenge, of course, arises if the problems that the intentional ambiguity is not effective in deferring issues. If it fails in deferring the issue there is no simple way out. In the cases examined in this chapter, resolving the ambiguity involved changing the basis of enrolment onto the Scheme to one of “application” rather than compulsion and presenting updated cost estimates every six months that keep the Scheme in the public’s imagination.

CHAPTER 8

Technological expertise and decision-making

Previous chapters have examined both the role of language about technology in the policy-making process and the ways in which technology is conceptualized by policy-makers. In this chapter, these two elements come together in a review of the ways in which technological expertise relating to the UK's identity policy was presented.

The relationship between technological expertise and organizational decision-making has always been complex and moving this issue to policy-making only increases the complexity. Although information technology is playing an increasingly important role in the implementation of most aspects of public policy ranging from taxation and border control to the payment of welfare benefits and other forms of social security (Avgerou and McGrath, 2007; Dunleavy et al., 2006), elected public servants are likely to have as little technological knowledge as most nontechnical senior executives and as such will have to rely on specialists to guide them about the technological aspects of the proposals (Bassellier et al., 2003).

This can result in a tension between technology leading organizational innovation and technology following organizational innovation in the public sector. There are direct parallels with similar debates in the private sector where information systems were seen, at different times, as providing opportunities for competitive advantage (Porter and Millar, 1985), supporting organizational innovation and restructuring (Davenport, 1993; Hammer and Champy, 1993), to becoming a necessary but not sufficient condition for operating in the global economy (Carr, 2003).

There are, therefore, important questions about the relationship between technological knowledge and expertise (typically provided by information systems specialists) and the processes of organizational and institutional decision-making (often undertaken by senior "managers" with limited knowledge of technological issues) that use this knowledge in the case of technologically-leveraged policy initiatives. There is extensive research into many aspects of this relationship in the private sector, covering for example the IT experience of business managers (Bassellier et al., 2003), how technological expertise and prior success (Martins and Kambil, 1999) might lead to overconfidence (Simon and Houghton, 2003) or project escalation (Keil, 1995) as well as the limited attention spans of directors for IT matters (Huff et al., 2006).

Far less is known about the role that technological expertise plays in decision-making in the public sector, despite the fact that the process is likely to be much more open and can potentially draw on more detailed expert advice than many similar private sector decisions. The need to draw on the best possible advice is particularly important given the size of many public sector systems that are of a vastly larger scale than most private sector systems (Willcocks and Kern, 1998), with public sector successes and failures often having a far higher profile than the equivalent private sector systems (e.g. BBC News, 2007b; Beynon-Davies, 1995).

The relationship between technological expertise and decision-making can be inferred from the language used to describe the environment and decision-making processes. This chapter analyzes the espoused relationship and relates it to existing perspectives of decision-making. It then draws on insights from science and technology studies about the nature of scientific and technological expertise to explain why the chosen approach reveals a misplaced certainty relating to technological issues which has resulted in many of the perceived problems with the Scheme. An alternative strategy based on espoused confidence rather than certainty would present a more effective way of supporting the decision-making for the Scheme.

Technological expertise and organizational decision-making

The relationship between technology and organizational processes in the public and private sector has varied considerably over time (Bassellier et al., 2003). By definition, in the private sector decisions about the earliest business applications of computers were made on the basis of limited existing technological expertise (Caminer et al., 1998; Ferry, 2003; Glass, 2005). As a result, decisions about what processes could be automated or supplemented by computing resources were typically made on the basis of existing expertise in “systems research” and “organization and methods” (Ferry, 2003).

The emergence of a distinct cadre of technological specialists, often experimenting with technological systems (Ciborra, 1991), led – in the

1980s – to what have been called "strategic information systems" (Earl, 1993; Galliers, 1991; Johnston and Carrico, 1988; King, 1978; Somogyi and Galliers, 1987). Drawing on a number of classic case studies, the argument was made that technologically-leveraged innovation was the key to successful, sustained competitive advantage (Cash and Konsynski, 1985; Ives and Learmonth, 1984; McFarlan, 1984; Porter and Millar, 1985; Porter, 1985). Decisions about changes to organizational processes were therefore believed to be heavily influenced by the successful incorporation of this technological expertise by senior managers who would adapt their organizations to reflect the opportunities offered by technology.

By the late 1980s, however, this technology driven approach was being replaced with a more process oriented perspective (Davenport, 1993; Hammer and Champy, 1993). Here the argument was based on focusing on the key business processes of the organization and using technology to support the reengineering of business activities around these key processes (Hammer, 1990). At this time, therefore, technological experts had reverted to a more subsidiary role in organizational life, supporting the reorganization of business processes.

The advent of the internet as a means of supporting interorganizational systems (Benjamin et al., 1990; Johnston and Vitale, 1988) reasserted the role of technological experts in providing opportunities for technology driven innovative business practices (Castells, 1996) which have, in many cases, now become standard practices that all in a particular industry need to mimic (Carr, 2003).

Technological decisions in the public sector have followed this pattern, although perhaps with less violent fluctuations, partly as a result of the conservatism inherent in most civil service organizations and partly because of the scale issues associated with any large-scale public sector innovation (Dunleavy et al., 2006). This is not to say, however, that there have not been attempts at innovation in the public sector, particularly in terms of the new public management agenda (Barzelay, 1992; Bevir et al., 2003; Cabinet Office, 1999; Hood, 1996) and e-government (Fountain, 2001; Ho, 2002; Moon and Norris, 2005; Mosse and Whitley, 2009; West, 2004).

As it presented its views on the technological components of the Identity Cards Scheme, the language used by the Home Office reflected its socially determined understanding of the capabilities and limitations of the technology. That is, using the language of Collins and Kusch (1998), the choices taken were polimorphic rather than mimeomorphic.

Mimeomorphic actions are those that do not need an understanding of society to be performed correctly; that is they can be applied in any situation and still be performed correctly. Polimorphic actions, in contrast, are both many-shaped and take their shape from society (1998, p. 33). The choice of what to say or how to say it depends crucially on an understanding of the society (or community) within which one is speaking.

For example, choosing whether to tell a risqué joke in the presence of others requires an understanding of whether those friends would find the joke acceptable or not; no context-free rules can be given for determining this choice, instead the appropriateness or not of the action is learned through immersion in that social context.

Applying this insight to the context of descriptions of the technology underlying the Scheme and the Government's ability to deliver a successful identity policy, the choice of language used reflects the prevailing norms about the technology in the Home Office at that time. This allows a clearer understanding of the various conflicting priorities that face policy-makers and the distinct role that technological considerations play in this process – conflicts that may not arise to the same extent in the private sector.

For example, Martins and Kambil (1999) suggest that prior experiences affect current decisions, with successful prior experiences potentially being given more weight than is necessarily appropriate, raising the possibility of project escalation (Keil, 1995). Thus, a government with a patchy record with IT systems might use language that suggests a more cautious approach to technological expertise.

Similarly, Simon and Houghton (2003) suggest that problems with risky products might arise through the effects of overconfidence in the decision-making process. Such overconfidence may arise because the decision-making process lacks "prior similar actions to help calibrate judgment" (p. 140). Alternatively, the espoused language might reflect an awareness of this issue by highlighting a costing methodology that explicitly includes consideration of an "optimism bias" (KPMG, 2005).

Statements about the technological elements of the Identity Cards Scheme

The idea that different social norms lead to different choices in the language used to describe the basis for technological decision-making is used to inform the analysis in this chapter. Here various statements by the government are presented and analyzed.

The statements that are presented below are taken from key stages or "critical incidents" (Pettigrew, 1990) in the development of the proposals from the time the Bill was introduced to Parliament (May 2005) to the announcement of the issuance of the first identity cards for some foreign nationals (November 2008). Pettigrew (1990) argues for the "importance of temporal interconnectedness, locating change in past, present, and future time" as statements and events taken in isolation might convey a very different sense of what is happening from those evolving over time. By studying these statements over time it becomes apparent that the statements relate to institutional norms and views rather than the perspectives of individuals.

The Parliamentary debate (June 2005–March 2006)

When the then-Home Secretary Charles Clarke introduced the Identity Cards Bill to Parliament for its second reading he told Parliament that he would "address the concerns about the project's size, technology and scale" [28 June 2005, Column 1152]. With the flow of debate in Parliament, he did not actually return to address these points on that day although it is clear that he would have been briefed in advance of the debate and had prepared statements to make on these points.

When the Bill returned to the House of Commons after its Committee stage, disquiet about the Scheme had increased and Mr Clarke assured politicians that:

> Intellect [the trade association for the UK technology industry] and the wider UK technology industry have the ability to meet the technological challenges created by the Government's ID card proposals. The technology being considered, which will form the basis of the scheme, has already been used in similar programmes across the world and is well established. [18 October 2005, Column 800]

A similar point was made by Lord Mackenzie of Framwellgate shortly afterwards during a debate in the House of Lords:

> I am confident in saying that the technology for a large-scale national identity scheme is available and proven. There are at least 40 projects in 31 countries involving identity storage, the majority incorporating the use of biometric details. If the UK decides to pursue such a scheme, technology will not be a limiting factor. [31 October 2005, Column 62]

Another argument that was used to support the government's position was that the proposals for the Scheme had been reviewed by the Office of Government Commerce (OGC) Gateway Review Process. The OGC review process had been introduced to

> deliver a 'peer review' in which independent practitioners from outside the program/project use their experience and expertise to examine the progress and likelihood of successful delivery of the program or project. They are used to provide a valuable additional perspective on the issues facing the internal team, and an external challenge to the robustness of plans and processes. (Office of Government Commerce, 2009)

The results of the reviews are traffic light signals, with Green and Amber projects being allowed to proceed and Red reviews requiring immediate action to be taken.

During the same debate in the House of Lords the Home Office minister Baroness Scotland informed the Lords that the project:

> has been through a further Office of Government Commerce review, Gateway 1, on business justification and the review confirmed that the project is ready to proceed to the next phase. [31 October 2005, Column 15]

She also made a similar claim to Mr Clarke about the viability of the Scheme:

> Many concerns have been expressed about the technical viability of the prescribed scheme. We recognise that there are challenges. Projects such as this will always face such challenges and opinions in the field of technology will differ. However, the body of representations within industry, existing project experience and research by established experts in the field of biometrics and database technology indicate that we are right to proceed with our plans at this stage. As with all major government projects, the technology behind the identity card scheme will ultimately come from the industry, and key sections of the industry are telling us that the technology can work.
>
> An identity technology advisory group representing leading technology companies in this field says that if the UK decides to pursue such a scheme it will work. The industry can also point to a number of existing technology projects run successfully, including many for the United Kingdom Government using large databases. [31 October 2005, Column 111]

After its passage through the Lords the House of Commons debated an amendment about the costs of the Scheme and the Home Secretary again made reference to the technological expertise provided by industry:

> We had a substantial discussion with the whole industry about our proposals to ensure that we work as best we can with the most up-to-date technologies. The right hon. Member for Haltemprice and Howden (David Davis) was right to say that the technology is fast moving. Many companies are involved – many British companies are in the lead, by the way – and we want to work closely with them. That is an intelligent course for us to follow. [13 February 2006, Column 1173]

Thus, throughout the Parliamentary debate, the government's position was clear: they had learned the lessons of previous IT failures and knew exactly what they were doing now.

The Science and Technology Select Committee Inquiry (March 2006–August 2006)

The question of the government's use of scientific and technological advice formed a key part of a House of Commons Science and Technology Select Committee inquiry. The inquiry looked at three areas of government policy: the classification of illegal drugs, the use of MRI equipment, and the technologies supporting the Government's proposals for identity cards.

The inquiry into identity cards took place after the Bill had become Law and received written and oral submissions from the Home Office as well as representatives from industry and academia (Science and Technology Select Committee, 2006).

Again, the language from the Home Office gives clear indications as to its relationship with the technological expertise it was drawing upon. For example, Katherine Courtney, then Director of the Identity Cards Programme assured the Committee that she had a "very high level of confidence" that they would be able to come to an agreement "around the specification for that system with suppliers" and that it would be "delivered when we have agreed they will deliver it" (Science and Technology Select Committee, 2006, Answer to Q328), although later oral evidence from academia and industry (Science and Technology Select Committee, 2006, Evidence given on 3 May 2006) disagreed about the amount of interaction between government and industry.

When the Junior Home Office minister Joan Ryan appeared before the Committee on 14 June 2006, she told the Committee that:

> I am not anticipating something major that would completely delay or derail the programme. (Science and Technology Select Committee, 2006, Answer to Q1175)

Leaked e-mails and the Strategic Action Plan (June 2006–December 2006)

On 9 July 2006, however, a leading Sunday Newspaper ran a front page headline story entitled “ID cards doomed” based on leaked e-mails sent between senior officials from the Office of Government Commerce and the Identity and Passport Service. As described in Chapter 3, these e-mails had been exchanged on 8 and 9 June 2006 (i.e. a week before Ryan had told the Select Committee that she did not anticipate major problems).

Following these leaks, however, the recently appointed Home Secretary John Reid delayed all aspects of the procurement process and ordered a full scale review of the proposed Scheme. As a result of this review, a new Strategic Action Plan (UKIPS, 2006b) was released in December 2006.

Despite the wholesale review that had resulted in the Strategic Action Plan, the language it used was similar to the earlier statements:

> The Scheme is a long-term programme, creating a comprehensive identity management infrastructure for the UK. We have already begun work on laying its foundations.
>
> As with any such long-term plan, the Scheme will evolve over time. The plan we are publishing today sets out our current intentions and focuses on what we plan to deliver between now and 2010. As with any undertaking of this scale, there is still much detailed planning work to be done, and we shall learn many lessons as we start to deliver. We shall adjust the details of this Action Plan as required by experience, and we shall keep the public informed by publishing updated plans periodically. (UKIPS, 2006b, p. 5)

The plan continued, stating:

> The Scheme will be implemented carefully and securely and we will take an incremental approach to getting it right. We have focused much

> effort on reducing risk and have developed contingency plans to cover potential delays. The overall timetable for delivering the components set out in this Action Plan will be determined by our total resources: central funding, efficiency savings and income from charging. It will also need to take account of technical and commercial feasibility.
>
> So, while continuing to provide excellent customer service, we will strike a balance to ensure that best value for money is obtained, without compromising the Scheme's integrity. (UKIPS, 2006b, Executive Summary p. 6)

Procurement

As noted in Chapter 3 procurement for the Identity Cards Scheme finally began in August 2007. The procurement "Prospectus" speaks of "a set of challenging issues" (UKIPS, 2007b, p. 4) that are still to be resolved and a Scheme that could "change over time as a result of the current review of delivery options" (p. 7).

According to the Prospectus, the reason for this new position because the Scheme "is a large scale, long term business transformation programme involving multiple stakeholders" that "will exist in an environment of ongoing change as well as emerging technologies" (p. 9).

Delivery Plan 2008

The Delivery Plan issued in March 2008, although primarily issued as a consultation document about the next stages of the Government's revised implementation plans, included these statements about the technological capabilities of the selected suppliers:

> The Scheme is made up of a large number of components, each involving a variety of people, processes, technology, physical infrastructure and estates. These components are being delivered by several organisations in the public and private sectors
>
> We aim to achieve a positive, partnering environment with strong commercial safeguards and will conduct the procurement process with these principles firmly in mind, seeking strategic suppliers who will work cooperatively over the long term, with us and with each other, to achieve our goals in the most cost-effective and lowest risk manner. The process will be fair and balanced but commercially challenging.

> Mechanisms will be in place to encourage both cooperation and competition. (UKIPS, 2008a §54, §56)

Discussion

The statements made by government about the basis for decision-making around technology are polimorphic as they reflect the culture and norms of the organization that they originate from. This is particularly the case for formally issued documents that are likely to have been reviewed on a number of occasions before they are issued. The language used therefore reflects the underlying attitudes to technological expertise. An organization that was aware of the risk of project escalation would use very different language from that used by one that had not considered this risk.

The statements made by the government about the technological expertise underlying the Scheme, particularly for the first two incidents presented above, demonstrates a particular relationship to the expertise that is driving the technological aspects of the Scheme – a relationship based on very strong confidence in the accumulated expertise.

Thus, there is confident talk of "well established" technology that will not be a "limiting factor" and project plans that have the support of industry and that have successfully passed internal reviews. When questioned by the Science and Technology Select Committee officials spoke of their very high levels of confidence in the project, with problems being unlikely.

Up until this stage at least the front stage (Goffman, 1990 [1959]) presentation of the relationship between government and its technological expertise was always one of self-assurance: belief in the technology, belief in its plans, and belief in its ability to deliver the Scheme on time and on cost. Backstage, however, as the leaked e-mails suggest, this self-assurance was more muted and calls into question the simple relationship that government had excellent technological expertise that it used as a basis for its policy decision-making.

Insights from the social studies of science and technology (e.g. Bauchspies et al., 2006; Sismondo, 2004; Yearley, 2005) raise important concerns about the nature of technological expertise and the extent to which it produces the claims of technological certainty described above. Through detailed empirical studies, science and technology studies have shown that technological expertise is often context-bound and tacit (e.g. Collins, 1992; Latour, 1999). In particular, these studies have shown that expert knowledge is much more conditional and less certain than what the popular image of scientific knowledge suggests (Latour, 2004). See also the discussion in Chapter 6.

MacKenzie (1993 [1990]) illustrates this in the case of technological expertise about nuclear weapon guidance systems and, in particular, the technological expertise about their likely accuracy in real-world situations. In doing so, he highlights a novel form of uncertainty: "that of those closest to the heart of the production of knowledge of accuracy" (p. 371) with this group finding doubts because of their "intimacy with this process of production" (p. 371). As a result, he proposes a "certainty" trough where those directly involved in knowledge production have greater uncertainty than those "committed to technological institution/program but [as] users rather than producers of knowledge." Those alienated or uncommitted to the technology are likely to have high uncertainty simply as a result of their lack of knowledge (p. 372).

During the early stages of the Scheme (i.e. the first two critical incidents presented above), it would appear that MacKenzie's uncertainty principle does not hold. Here, there is strong confidence in the technological aspects of the Scheme based on the available technological expertise. It is unclear what the basis for this strong confidence is as, at least initially, the program was driven by civil servants who did not have a strong technological background. This is probably a matter of degree, however, as many will have been drawn from the IT industry; for example, James Hall, appointed CEO of the Identity and Passport Service in September 2006 had extensive experience in managing large public sector IT projects for Accenture.

During the later stages of the Scheme, the pattern appears closer to that suggested by MacKenzie – that is, those with technological expertise are less confident in their ability to deliver the Scheme successfully (third incident) and highlighting the complexities that a Scheme of this size will invariably face (fourth and fifth incident).

For those in academia and industry, the idea that large-scale systems will, in all likelihood, change and develop before they are finally implemented is hardly a novel insight, thus reinforcing MacKenzie's point that those close to the technology will have less confidence in it than those further away. Indeed, in an editorial to a journal special issue focusing on the UK's National Programme for IT, Sauer and Willcocks (2007) examine some of the problems associated with delivering large-scale IT systems. They argue that in such "multi-year, multi-billion pound" schemes "problems are to be expected and that it is a misunderstanding of the nature of the enterprise to suppose that initial expectations will be met" (p. 196).

Why, then, when the Scheme was being debated in Parliament, was the language from the government almost exclusively framed in terms of certainty about the technology, its implementation, and its likely costs?

One plausible explanation is a mismatched relationship between public sector decision-making about technology and technological expertise. That is, the Home Office felt that the only way it could pass the legislation was by presenting its confidence in the Scheme in terms of certainty about its technological implementation, with any acknowledgment of the kinds of complexities raised by Sauer and Willcocks likely to be seized on by opponents as a sign of weakness. This confusion of confidence with technological certainty is problematic, both for the implementation of the Scheme and for its effective scrutiny by Parliament. For example, in relation to the projected costs of the Scheme, the Science and Technology Select Committee noted that they were:

> sceptical about the validity of costs produced at this early stage. We acknowledge that the release of firm overall costing has been driven by political imperatives but the Home Office could have credibly given a broad range instead of precise figures. (Science and Technology Select Committee, 2006, recommendation 32)

This echoes Sauer and Willcocks' (2007) suggestion that when project sponsors and supporters are aware of the complexity that the systems are likely to entail they are more likely to trust the judgments of the experts implementing the scheme. Thus, they advocate a policy of honesty as to the likely problems that any large-scale IT systems in the public (or private, for that matter) sector is likely to entail, arguing that such an approach is both ethical and engenders better working relationships leading to more opportunities for openness and discussion than situations based on misrepresenting the benefits and risks of such schemes.

In the case of the Identity Cards Scheme, however, an alternative strategy was followed that drew heavily on technological certainty as a means of highlighting the close relationship between public sector decision-making and technological expertise. However, too much emphasis on technological certainty is unlikely to be a successful approach, particularly if the policy proposals are controversial as this means that any deviation from the certain plans will be seized upon by opponents as "proof" that their concerns were justified. However, a strategy that presented a detailed consideration of all the ways in which a policy initiative might fail given the inherent complexities of large-scale infrastructures is also not an effective strategy as this would simply result in the project never taking off.

What is required, both for identity policies and technology policies, is a more effective presentation of the arguments in favor of the proposals based not on technological certainty but rather on confidence that the organization is able to deliver the policy in the way it intends, acknowledging that there are important technological challenges to be faced but that it has the resources and expertise to address these challenges effectively.

Moreover, as the language used is a reflection of the underlying organizational culture, it is not simply a requirement to use the right kind of language in public statements (which, as Chapter 7 has shown, can unravel at inopportune times). Rather it requires a fundamental reassessment of the internal organizational culture that sees technological confidence rather than certainty as a strategy that will be appreciated by the organization's decision-makers. Thus, organizational decision-makers must also develop the sophistication to be able to respond effectively to technological presentations made in this way.

CHAPTER 9

The Scheme five years on

In November 2008 the UK government began requiring certain classes of non-European Economic Area (EEA) foreign nationals to apply for biometric residence permits issued in the form of a card under the UK Borders Act 2007, heralding the "successful start" to the Scheme. It also published a variety of documents detailing its plans for identity cards for UK nationals. These included

- a response to the consultation about the 2008 Delivery Plan (UKIPS, 2008g);
- a prospectus for the provision of "Front Office Services" (including biometric enrolment) (UKIPS, 2008b); and
- a detailed guide outlining "how the Scheme will work and how it will benefit you" (UKIPS, 2008e).

Shortly thereafter, a 97 page document outlining the proposed secondary legislation for implementing the first stages of the Delivery Plan (UKIPS, 2008c) was also issued.

What these documents show, however, is that the Scheme has shifted significantly from the vision that was presented to, and debated by, Parliament. Although large technology-based infrastructures are likely to drift during implementation (Ciborra and associates, 2000), it is important to understand precisely the extent of the changes that the Scheme has undergone. This chapter argues that these changes are a direct consequence of the failure by the UK government to appreciate the technological challenges of identity policy. It also highlights the difficulties of Parliamentary scrutiny of such proposals, the implications of which are discussed in more detail in the next chapter.

The new roll-out strategy

The Delivery Plan introduced by the Home Office in 2008 was the *second* major shift in the implementation of the Scheme since the Act was passed (the first was the Strategic Action Plan (UKIPS, 2006b; see Chapter 3). The Delivery Plan presents a much slower roll-out of the Scheme than had previously been envisaged in either the initial proposals or the Strategic Action Plan.

As was discussed in Chapter 4, when the Bill was being debated in Parliament, the intention was that once the Register had been implemented and the enrolment centers created, identity cards would be issued to UK nationals as they "voluntarily" renewed their passports. Although the first two years would involve an incremental roll-out of around 3 million people (1.3 million in the first and 1.7 million in the second, implying that not all passport renewers would be enrolled into the Scheme), by the third year all individuals renewing their passports would have their biographical and biometric details entered onto the Register and be issued with an identity card (around 4 million people per year).

The Strategic Action Plan (UKIPS, 2006b) proposed that:

- by the end of 2007 biometrics would be recorded for "most" visa applicants;
- by the end of 2008 the National Identity Scheme Commissioner would be in post;
- by the end of 2009 the first identity cards would be issued to British Citizens "using the improved application and enrolment systems"; and
- by 2010 "significant" volumes of cards would be issued (UKIPS, 2006b).

In the Delivery Plan (UKIPS, 2008a), the roll-out is significantly slower. Rather than enrolling individuals into the Scheme as they renew their passports, the intention is to start the Scheme by focusing on identity cards for critical workers. This would involve bringing the highest level of identity assurance to an important area of strong personnel security in airports and elsewhere. The process will involve issuing identity cards to those working airside as part of an "18-month evaluation period," an experiment that would take place at "selected airports" (UKIPS, 2008g) from late 2009.

This part of the roll-out will involve the creation of a Temporary or Tactical Register, containing the details of a geographically limited small number of individuals. Details of the individuals stored on this version of the Register will be transferred to the main Register when it becomes operational. According to a document leaked by NO2ID (2008) the choice of this group provides "a strong narrative" (i.e. playing on the national security angle is likely to make this option more acceptable politically and socially). Although there are some practical benefits to starting small and growing incrementally, even this modest strategy has faced considerable problems. For example, as a result of opposition by pilots' unions backed by the Trades Union Congress, the first wave of airports is, in fact, limited to only two relatively small airports: London City and Manchester and even here, a successful roll-out is not guaranteed. Concerns about the costs of the identity cards mean that the government has agreed to issue these workers with free identity cards. Moreover, the draft secondary legislation issued in November 2008 includes a number of elements specifically to address this roll-out, dealing with complexities such as those workers who live abroad, those who are proposing to enter the UK and those who are applying for a permanent airside pass in connection with a job, or an application for a job, that requires such a pass (UKIPS, 2008c, 2.5 (b)).

In addition, the whole process is presented as part of a much larger business process reengineering project that combines "greater assurance of employee identity" and "improved efficiency of pre-employment checking" as part of a more joined-up approach to airside passes. This will mean that if an employee moves from one employer to another within an airport, or from one airport to another, the results of previous checks should be transferable. This work is being supported by a "Process Improvement Fund" that presumably includes the cost of issuing the identity cards to the Wave One workers and the associated Temporary Register. As such, it has very little to do with the kinds of identity cards that were the basis of the Parliamentary scrutiny of the Act.

The next phase of the roll-out of identity cards is to "young people" (i.e. those aged 16–25) who will be offered cards from 2010. This group has been targeted because they are "at the forefront of our current plans given the potential benefits to them of a simple, convenient way to prove their age and identity" (UKIPS, 2008g) and is also "the quickest option" (NO2ID, 2008). Young people often have a limited biographical "history" and may find it difficult to prove their identity in situations such as when opening bank accounts and proving that they are eligible for access to age-restricted products and locations. Cards may be made available to volunteers in so-called "beacon areas" at some point slightly earlier than this, but detailed plans are yet to be announced (Home Office, 2009).

However, given the infrastructural nature of the Scheme, it is unclear how quickly public and private sector organizations will start to use identity cards as part of their formal verification processes. For example, the banking sector already has processes in place for allowing young people to open bank accounts. Moreover, at the time, the British Bankers' Association said that it had not been involved in any discussion on the use of ID cards by young people (Palmer and Burns, 2008a).

Finally, "from 2011/12" the government "shall start to enrol British citizens at high volumes" (UKIPS, 2008a, p. 8) and it is intended that personalized, joined-up public services would begin to be available from 2015.

The cards that are being issued

There are at least five different kinds of cards that the government is issuing or plans to issue. These are:

- the cards for foreign (non-EEA) nationals that have begun to be issued;
- the cards for "Wave One" employees working at two UK airports that are due to be issued from late 2009;
- the cards to be issued to UK nationals that are usable for travel (due to begin to be issued sometime between 2010 and 2012);
- the cards for UK nationals that are not usable for travel (presumably due to be issued in the same time period); and
- the cards for EEA nationals that are not usable as travel documents. These last cards will probably be issued from 2012 onwards.

The "Foreign National Identity Cards" issued as part of the UK Borders Act 2007 replace a "vignette" in the individual's passport and will include a biometric "contact" chip. As such, they are little more than a different physical manifestation of the previously issued vignettes.

The government has begun claiming, however, that the new process of issuing these visas has resulted in at least one failed asylum seeker being caught through the biometric-checking process within days of the new process being introduced (Young, 2008) and is proof of the utility of its biometrically driven identity policy. It is not clear, however, whether such matches are being picked up solely as a result of the biometric checking process or if they would have been picked up in the general process anyway.

One consequence of the small number of individuals that will be issued with these cards is that there are no card readers in circulation that can be used to check the cards, the contents of the chip or compare the information on the card with information held on the Register [WA 258100]. The current guidance about the use of the card includes the use of a card verification phone line and emphasizes the card's physical characteristics. "As it is made entirely from polycarbonate, it will have a distinctive sound when flicked, and the holder's image will always be in grey-scale" (UKIPS, 2008d).

How the Scheme is now expected to work

The response to the consultation on the Delivery Plan, when read in conjunction with the draft Secondary Legislation and the prospectus for "Front Office Services" whereby biometric enrolment will be provided by commercial organizations rather than government, presents a radically different view of how the Scheme is intended to operate from that presented to Parliamentarians during the consideration of the Bill and discussed in detail in Chapter 4.

Enrolment

The first significant difference arises in relation to enrolment in the Scheme. The government has always emphasized the need for this process to have high integrity, as it is the foundation of the remaining processes (Berghel, 2006; Collings, 2008;). That is, it is in the nature of the Scheme that once someone has entered their details onto the Register, all the other processes (verification, data sharing, etc.) proceed from this. Therefore, if someone is able to enter their details onto the Register fraudulently, then they will have a bona fide government-issued identity that cannot be easily challenged and, in practice, is unlikely ever to be challenged in regular use. The integrity of the enrolment process is therefore paramount.

Recall that under the original plans, the enrolment process would involve both biographical and biometric checks. The Delivery Plan changes this process significantly. In particular, in an effort to reduce the costs of the Scheme for the Identity and Passport Service (IPS) (i.e. the costs that are reported every six months in s.37 cost reports), biometric enrolment will not take place at the 69 enrolment centers that IPS had planned to build (and of which seven are being used to enroll the biometrics of foreign nationals). Instead, biometric enrolment will take place at partner organizations that are providing "Front Office Services" for IPS.

The vision behind the front office services is "a future where the Government would not provide biometric enrolment services" and, instead, this is provided "by the market, giving citizens a choice of competing services, which should maximise convenience and drive down price" (UKIPS, 2008b). Organizations that choose to work with the government in providing these services will benefit from

- a new revenue stream;
- increased footfall;

- access to new customer segments;
- association with a respected and trusted brand; and
- goodwill generated by providing a valuable public service (UKIPS, 2008b).

They will have to satisfy government standards relating to integrity, security, and information assurance that will be enforced and overseen throughout the service provider network. Thus, organizations will need to be "accredited" so as to guarantee the integrity of the Scheme in areas such as staffing, infrastructure, technical security, and customer service capability (UKIPS, 2008b). For example, the collection of biometric data needs to be supervised one-to-one by a trained operator who will have undergone security checks and be employed by an accredited organization.

Thus, the duties on accredited service providers include setting up and maintaining the services they offer, including

- supplying the estate either themselves or through a partnership organization;
- procuring, deploying, and maintaining appropriate biometric recording equipment;
- recruiting and/or training suitably vetted staff;
- developing business processes in conjunction and adhering to specified service levels;
- integrating their systems with any interfaces to IPS systems; and
- marketing these services in conjunction with the IPS (UKIPS, 2008b).

To date, little progress has been made in identifying suitable business partners, particularly given the global economic downturn that began in 2007. The kinds of organizations that are envisaged for this role include supermarkets and post offices. However, public opinion surveys undertaken on behalf of IPS have reported that only 28 percent of respondents would consider having their fingerprints enrolled at a post office (UKIPS, 2008h). In the next survey the question was reversed and 75 percent of respondents stated that they would not want to give their fingerprints at a supermarket, and 47 percent would not do so at a post office (UKIPS, 2008i).

Whereas the initial discussion of the Bill talked about face, fingerprint, and iris biometrics, the Delivery Plan confirms that iris biometrics have been dropped from the implementation of the Scheme (a decision foreshadowed by the Strategic Action Plan that noted that "the introduction of biometrics remains an option" (UKIPS, 2006b, §65)) and that only face and ten fingerprint biometrics will be collected and stored, with two fingerprint images stored on the card (UKIPS, 2008e). The reason for collecting more fingerprints than are required is to provide a more robust approach to confirming identity, for example, by allowing other fingerprints to be checked against “other biometric databases” [WA 226409].

The Front Office Services prospectus helpfully notes that the fees charged for biometric enrolment “will be separate from the ones that the IPS will charge customers for processing their application and supplying their passport or Identity Card” (UKIPS, 2008b). That is, this move to the market does not necessarily reduce the cost of an identity card from the perspective of citizens; it simply removes a significant cost element from the Scheme costs as are reported to Parliament every six months. With a total market value that has been estimated at between £120 million and £280 million per annum, and approximately 4 million identity cards being issued per annum, this suggests that citizens will have to pay around £30 to record their biometrics in addition to the fee for enrolling in the Scheme.

The biographical enrolment process can be done on-line and “the information requested will be similar to the current passport application form” (UKIPS, 2008e). This form-based biographical check will involve extensive checking of the data on the form against data held in public and private sector databases. It will be possible to receive assistance in the application process by using one of the Front Office Suppliers.

In a few cases, applicants will be asked to come for an interview as currently happens for adults applying for their first passport [WA 268936]. The intention here is to verify the details on the application form, particularly for those with limited evidence of identity, such as those with no previous passport history. The interview process would also confirm that the photograph (and presumably the biometrics) submitted are those of the person in the interview. This interview process is intended to be straightforward and take no more than 10 minutes. If necessary, it can be done remotely (UKIPS, 2008e).

Verification

The process of verification associated with the use of the Scheme has also been significantly altered in the Delivery Plan/proposed secondary legislation. Depending on the level of identity assurance required, different forms of check can be performed. An individual’s identity can be checked

- visually (does the person look like the photograph on the card and does the card look legitimate?);
- through entry of a PIN number;

- by checking fingerprints against what is held on the chip on the card; and
- against the Register (UKIPS, 2008e).

As was noted above, guidance information is available for visual inspection of the cards for foreign nationals but, at present, there are no plans within Government to roll out card readers for either PIN checks or fingerprint checks [WA 258100].

Any checks against the Register will involve a simple Yes/No answer being sent to the requesting organization (UKIPS, 2008e) although other government agencies and bodies such as the police may have greater access. In terms of the audit trail that is created, "no details of the reason for the check will be recorded, only the fact that a check was made and by whom" (UKIPS, 2008e).

What is on the card?

The design of the card continues to be driven by the requirements of International Civil Aviation Organization (ICAO) travel documents so that the card could be used for travel within Europe (although, according to IPS's own polling, in August 2008, only 34 percent of those sampled were interested in purchasing a card for travel purposes (UKIPS, 2008i). For the first cards, only the English language will be used, although there are plans to introduce other languages, such as Welsh in due course.

The symbolism on the card is also important. The first cards for foreign nationals are "covered in EU symbols to satisfy Brussels" (Hickley, 2008). For the British cards, there will be further concerns, particularly in Northern Ireland (Holder, 2008) where the Police Service of Northern Ireland badge incorporates eight different symbols.

Significantly, there are no plans for the National Identity Register Number (NIRNo) to be on the face of the card or the chip. When taken in conjunction with the assurance that a check against the Register will only result in a Yes/No response, this will make it difficult for the NIRNo to act as a unique identifier across government and private sector organizations, thus avoiding the complications that have arisen in the United States where the Social Security number has become a de facto identification number (Berghel, 2000; Garfinkel, 1995; cf Otjacques et al., 2007) but also undermining the proposals for Transformational Government and cross-sector data-sharing.

Implications

Each of the changes proposed to the Scheme has significant implications that differ from those that could have been envisaged during the initial scrutiny of the legislative proposals. Although the Act was intended to be enabling legislation, it embodied significant policy design issues in the clauses of the Act, raising important questions of the nature of enabling legislation and its eventual, detailed implementation in the form of secondary legislation.

Biometrics

The changes to the biometrics used in the Scheme and their collection and use are particularly important. Throughout the Parliamentary debate, the government played up the role of iris biometrics and played down the role of fingerprint biometrics, not least, because as Kathryn Courtney, a Home Office official told the Science and Technology Select Committee:

> You may have individuals, for instance, who have lost their hands and are unable to register fingerprint biometrics but would be able to register a face and irises. (Science and Technology Select Committee, 2006, Answer to Q294)

Fingerprint biometrics, however, are cheaper to collect and verify than iris biometrics that will require specialist, expensive devices, trained users and careful lighting arrangements. Fingerprints can also be used for other Home Office policy purposes, such as attempting to match against crime scene prints (Whitley and Hosein, 2008).

According to the leading iris expert, Dr John Daugman, officials may struggle with the number of false positives that arise during the enrolment process as attempts are made to match fingerprints against the database of existing fingerprints to prevent individuals from enrolling more than once (BBC News, 2008a; Biometrics Assurance Group, 2008). According to Daugman, problems would arise once around six million people had been enrolled on the Scheme (Spiller, 2007). Iris biometrics, in contrast, he claimed would not face this limitation.

There are also significant security and public trust issues associated with the collection of biometrics by third party organizations. Again, the Home Office's own sponsored research has indicated that three quarters of UK citizens would *not* consider supermarkets as a location where they would be prepared to have their fingerprints, photo, and signature recorded (UKIPS, 2008i).

Other security implications include potential problems with finding a suitably secure and private location in these high street locations where individuals can be assured that their personally identifiable data are being securely recorded. There are also significant costs associated with having sufficient numbers of accredited staff available to supervise the enrolment process on a one-to-one basis. For the service to be customer-friendly and reliable, most outlets would require a number of such staff to cover for illness and annual leave of accredited staff.

In addition, given the key role that biometric enrolment plays in the Scheme, there are very likely to be attempts to infiltrate the supervision of the enrolment process so that individuals can enroll without necessarily using their real biometrics. These problems are compounded by the fact that the biographical enrolment process is being downplayed with the data provided by the individual being similar to that provided on the current passport application form.

Building an installed base

By linking the roll-out of identity cards to the issuing/renewal of passports, the Home Office had always intended to have a managed, incremental delivery of the Scheme that would, slowly, form an installed base of individuals who had been issued with an identity card or whose details were stored on the Register. The rate at which this occurred would determine when a significant proportion of the population was enrolled so that the government could introduce new legislation making enrolment compulsory. Under the original plans, this would probably take place after at least six years of the Scheme. However, under the new Delivery Plan, this installed base is likely to take much longer to be reached as, for the first three years, very few individuals would be enrolled (and a good proportion of these, who are working at Wave One airports, would need to have their records transferred from the Temporary Register to the main one).

This much slower take-up of the Scheme will have significant knock-on effects on the take-up of identity assurance measures in the public and private sector. For example, in January 2009, the Liberal Democrat MP Christopher Huhne asked a Parliamentary Question about government departments using card readers for verification of identity cards, to which the Home Secretary responded:

> Government agencies will all be able to make use of identity cards to verify identity through a visual check, as they do now for passports.

> It will be a matter for individual agencies to determine at what point in the future there is a case for the introduction of any further systems which might include identity card readers. The Identity and Passport Service will continue to work with other Government Departments to establish how each organisation may make the best use of the National Identity Scheme. [WA 243517]

Thus, more three years after the Act received the Royal Assent there are still no plans for government to integrate fully with the Scheme. If government cannot be persuaded to use the Scheme for identity assurance purposes, it will also be very difficult to persuade the private sector to sign up to use the Scheme (Heath, 2009).

This lack of appeal for the private sector could also affect the take-up of Front Office Services. The increased footfall and enhanced revenue that IPS promotes as some of the benefits of moving into this market may take a number of years to arise. In the meantime, the increased costs of accreditation and compliance may make the prospect unattractive for many, especially during a recession. It is unclear what will happen to the enrolment process if the market for biometric enrolment fails to take off.

Paying for the Scheme

Another consequence of the slower take-up of the Scheme will be in the much lower fee income from verifications. Unless all the costs of running the Scheme are obtained from the application fee, the income from on-line verification fees becomes significant. Once again, having few people able to have their identity verified against the Register is likely to affect this income stream significantly. As is often the case with information infrastructures, the limited take-up will have knock-on effects on, for example, the development of low-cost card readers and their roll-out.

A further limitation on the likely take-up of verification services is the limited information that will, according to the draft secondary legislation, be provided from the Register: Yes/No information only with no possibility, at this time, of value enhancing services (such as address data-push functionality). When coupled with the inability to use the NIRNo as a unique key for customer records to allow integration of services across business functions, these (late) design choices will further limit the attractiveness of the Scheme for industry and, consequently, the take-up of revenue-providing services.

A population register?

Another of the claimed financial benefits of the Scheme was, as discussed in Chapter 4, the possibility of using the Register as a national population register. To date, however, the specific work required to make the Register a national adult population register is not listed as part of the Delivery Plan or Cost Reports and it is also unclear exactly how much progress is being made in terms of implementing the population register functionality.

For example, written evidence by the Office of National Statistics to the Treasury Committee (Treasury Committee, 2007a) notes that the recommendations from the Citizen Information Project (CIP):

> are being taken forward by other government departments, i.e. where the opportunities exist, subject to legislation, to develop systems that have the potential to deliver many of the CIP benefits in the longer term. It is recognised that a statistical imperative alone will not be sufficient to establish and maintain a comprehensive and up to date population register. In the UK there are several administrative sources of information about the population that are registered for a particular service (e.g. NHS patient registers, NI numbers). None of them are sufficiently comprehensive or up to date to constitute a population register. In particular, there are significant practical difficulties in identifying those people on these registers who no longer live in the UK. (Treasury Committee, 2007a, p. 220)

In oral evidence to the Committee, Karen Dunnell noted:

> We had a major part to play in a project called the Citizen Information Project. This was done in preparation for the introduction of the national identity card scheme, and the conclusion of that work, which was a very large piece of work, was that the national identity card scheme should go ahead on a voluntary basis and create a register and use existing registers, in particular the one that is used for National Insurance purposes. That is the situation that we are in relation to that. It would be quite difficult, I think, for the Office for National Statistics (ONS) to make a case to Parliament on its own that something like this was necessary. Maybe that will change in the future but until we have something which is actually there and we have a requirement that people change their address and notify somebody when they leave the country, we are not very confident that a register will be suitable for the kinds of purposes that we need to measure the population every

> year and have a benchmark every ten years. (Treasury Committee, 2007b, Answer to Q 203)

This lack of clarity about the proposed plans to use the Register as a population register is particularly puzzling as, on 1 April 2008, IPS took over responsibility for the General Register Office which oversees the registration of all births, marriages, and deaths (General Register Office, 2008) and James Hall, Chief Executive of IPS was appointed as Registrar General for England and Wales. This becomes more puzzling given that the Register would provide "substantial CIP related benefits (address sharing benefits)" to the Home Office, benefits that in the outline business case amounted to around one-fifth of the total (Citizen Information Project Board, 2005) – a claim echoed by Atkins, who acted as consultants to the CIP (Atkins, 2009).

With the CIP mentioned in the earliest OGC Gateway Reviews of the Scheme (Office of Government Commerce, 2003, 2004) it would appear that the intention had always been for the Register to *also* act as a national population register. This decision has important implications for the costs and benefits of the Scheme as well as the design decisions that underlie its technological architecture. Thus, a national population register is intended to provide a range of data-sharing services for a variety of government departments and agencies that goes far beyond the simple Yes/No verification services currently envisaged. As such, the CIP's goals go way beyond the limits of "identity management" as espoused by IPS and certainly far beyond Crosby's notion of "identity assurance." However, Parliament was not informed of the links between the CIP and the Register until after the Act was passed and little further information about continued plans for these two services has been forthcoming.

Toward an effective identity assurance policy for the UK

It is apparent that the current Scheme that is being procured by the UK government is unlikely to achieve the intended goal of providing a successful means for individuals to reliably prove who they are in a variety of environments. Finding ourselves in this unsatisfactory situation requires urgent action to move to a new identity assurance infrastructure that both addresses citizen concerns and the requirements of business and the public sector.

This book is not an appropriate location for the detailed discussion of how the current implementation of the Scheme could be adjusted to provide such a new identity assurance infrastructure. It is, however, possible to outline key considerations from both industry (private and public) and citizens that should inform such developments.

The current proposals are inextricably intertwined with the issuance of passports. The government agency responsible for identity cards is part of the Home Office and its responsibilities have been merged with those of the previous Passport Service to create IPS. As was discussed in Chapter 4, the initial plan for the roll-out of identity cards was to be closely linked to the issuing/renewal of passports, thus preventing problems of workload balancing as upwards of 50 million people are issued with identity cards that have a ten-year validity period.

The link with passports continues with the claim that the government was under an international obligation to update its passports and passport-issuing processes to include biometric information. In addition, to counter claims that the current scheme could be scrapped in the future, the government repeatedly asserts that much of the investment in the scheme is linked to the passport issue with only a small proportion being associated with identity cards. As the political risk of the Scheme being scrapped increased, attempts were made to lessen the link between identity cards and passports so that the operational integrity of the passport system could be preserved. After the appointment of James Hall in 2006, however, this approach was dropped and the two systems were in effect merged. From a position where registration for an identity card could have been run in parallel and not threatened the passport-issuing process, from 2011/2012 onwards, the Scheme will require every person applying for a passport to *first* apply to be entered onto the Register, thus (artificially and unnecessarily) reinforcing the government's assertion that the two systems are closely related.

The requirement on biometric passports was attributed to both the ICAO and the U.S. visa waiver requirements. As Chapter 5 has shown, these claims were overstated and should not have formed the basis of compulsory changes. Indeed, other European countries, with different experiences of the use and abuse of government-held data, have interpreted these "requirements" very differently.

Problems of principle

When the link to passports is examined in this more critical light, a number of further issues emerge that further question the close linkages between identity cards and passports. Perhaps the most important of these relates to the principal purpose of a passport, namely to facilitate cross-border travel. The passport never was intended as the basis of identity assurance. Moreover, there are a number of situations in which the state might revoke the right of travel of individual citizens while not intending to revoke some of the other rights of that citizen.

In the UK, passports can be withdrawn from those with a banning order issued in relation to the Football Spectators Act (1989) and the Football Disorder Act (2000). The intention behind these Acts was to prevent known football hooligans from being able to travel abroad and cause trouble overseas by requiring the surrender of their passports. There is also discussion that absent parents who fall behind in child maintenance payments should follow suit (BBC News, 2009a). According to the draft secondary legislation for the Act, other categories of citizens who might have their passports rescinded include anyone with a travel restriction within the meaning of section 33 of the Criminal Justice and Police Act 2001(a), or any other requirement imposed by a court to surrender that individual's passport to the police or other authority.

It is apparent that even those individuals who have their travel rights rescinded are due to be included on the Register and should therefore be able to use their identity card to help assert their identity when, for example, registering with a GP, collecting a parcel, or opening a bank account. However, to prevent these individuals from being able to travel within the EU (which the identity card is intended to allow), these non-travel cards must be distinctive enough to allow a simple visual inspection to determine that they are not permitted to travel abroad. As with the football-banning orders, there are potential problems associated with issuing a replacement card and withdrawing the previous one. However, the distinction between identity cards for travel and those not for travel will also, of course, be observable by individuals not associated with travel, such as the GP's receptionist, the post office employee, or the bank official. When presented with a card that states that it is not valid for travel purposes, this person will be able to infer that the holder falls into one of the aforementioned categories and thus potentially subject the holder to discrimination.

Further complications are likely to arise with the increasing requirements to include travel details up to 72 hours before departure and where on-line check-in is permitted. In these cases, the on-line registration and check-in systems of all participating airlines will presumably have to include a real-time "valid for travel" checking function for UK identity documents which will increase the load on the Register. It is likely that this would be one of the verification services offered by IPS for which they would charge a fee.

There are other technological complications associated with having the identity card usable as a travel document within Europe. The design of machine readable travel documents is specified by ICAO and is based on open (nonproprietary) standards. This is because Machine Readable Travel Documents (MRTDs) have to be usable in a variety of situations from high-tech modern airports to border crossings where on-line connectivity is limited or nonexistent. Moreover, to prevent the creation of artificial monopolies and supplier lock-in, the technologies used (bar codes and chips) have to be based on open standards.

One consequence of this is the requirement to display the main data about the holder of the card in human-readable form on the face of the card. Thus passport pages typically include details of the holder's name, place, and country of birth, expiry date of the document and details of the issuing authority. Crucially, MRTDs also print the holder's date of birth on the face of the card. This means that if the identity card is to be used as a basis for determining whether an individual is of the appropriate age to enter or use certain age-restricted products and services, the MRTD *automatically* discloses their date of birth which is more detail than is required to achieve this particular function (Science and Technology Select Committee, 2006, §44).

The decision by the government to have the identity card function as a travel document within Europe therefore creates a series of problems associated with the very different purposes of a document for identity assurance and a document for travel purposes. The decision also locks in certain privacy-unfriendly measures – choices that an identity policy that fully appreciated the nuances of the technological issues would avoid.

Problems of practice

In addition to the problems of principle associated with the link between identity cards and passports, there are also a number of problems of practice associated with the current processes for issuing passports which will impact the effectiveness of the Scheme.

By basing the introduction of identity cards on the enrolment process for passports, the government has to ensure that the passport-issuing process is of a suitably high integrity, as the passport will then become the feeder document for all future identity-related activities. However, because of the original purpose of the passport, this concern about high integrity enrolment has not necessarily been a top priority (Collings, 2008). Although the UK passport agency has always taken an active role in minimizing the risk of passport application fraud, this has not been its ultimate goal and, as such, it has never claimed to be perfect at preventing fraud. This becomes an increasingly important issue when the enrolment process becomes the basis for the issuance of identity documents which it is intended will be accepted as the gold standard of identity or the basis of a national population register.

The role of biometrics to uniquely tie a person to a single identity is undermined if real biometrics are tied to the wrong individual (e.g. a situation where an illegal immigrant is associated with the biographical identity of a UK citizen).

Home Office surveys have also indicated that only a small proportion of UK citizens particularly value the use of the identity card as a means of traveling within Europe. In the August 2008 study, 34 percent of respondents said that they would be interested in purchasing the card for travel purposes (UKIPS, 2008i). Interestingly, this question has not been repeated since.

The earliest reviews of the Scheme (Office of Government Commerce, 2004) noted the importance of improving the quality of the enrolment process and many of the early plans for the Scheme (see Chapter 4) focused on improving the enrolment process. For example, the enrolment would be based on a face-to-face interview with enrolees, the collection of biometrics in controlled, government-run facilities, and extensive checking of the biographical footprint. However, over time these plans have been watered down significantly. Face-to-face interviews are taking place for some first time passport applicants (i.e. those "entering" the system for the first time). However, in practice interviews are currently only being held for around 1/3 of these applicants [WA 202852]. It is now expected that the decision as to whether an individual would be invited to attend an interview prior to registration on the Register

> will depend on the particular circumstances of the application but, as now with first time adult applicants for passports, it is likely that the Identity and Passport Service would need to interview an applicant where there is limited evidence of identity such as no previous passport history. An interview is one way of helping to establish identity. [WA 268936]

It would appear, therefore, that biographical enrolment for most people will be based on the information provided on the application form, information that may be checked by the employees of organizations providing Front Office Services. This information will, by definition, be far more limited and more generic than could be asked in a tailored face-to-face interview, emphasizing the importance of checking the data against existing public and private sector databases.

The enrolment of biometrics is also now being delegated to suitably accredited commercial service providers. Inevitably, the security risks in such situations are likely to be higher than in organizations that do not have competing commercial pressures on their staff (which is not to say that there would be no security risks with government enrolment locations).

A further practical problem with linking the issuance of identity cards with the renewal of passports is that it could take ten years before the entire UK population has been issued with an identity card. As a result it will take at least six years before a significant proportion of the population have an identity card. In a global environment where on-line transactions are increasingly common, an effective, secure method for on-line identity authentication should not be delayed so extensively.

Similarly, other measures to tackle identity fraud (e.g. credit freezes) that could be implemented almost immediately and at zero cost to the consumer have been ignored with the government repeatedly arguing that any measures to address this fraud would contain "the basic features of what the government is proposing" (Hillier, 2008).

The enrolment process has therefore shifted from something that could potentially have been a high integrity process (with the costs associated with providing such a high end service) to a relatively lower integrity process that is similar to that offered by other passport-issuing processes (see, for example, the U.S. passport application process described in Government Accountability Office, 2008b). This is not necessarily a problem as UK passports have been issued in much this way for many years and the passport-issuing agency has always been proactive in limiting passport fraud. However, the return to what is effectively the existing passport-issuing process is hardly "a modern means to confirm and protect identity."

A way forward

The two previous sections have demonstrated the problems with the plans to give the proposed identity cards the same functionality as passports and the problems with linking the enrolment and issuing of identity cards to the enrolment processes for passports. These insights, however, do open up novel opportunities for implementing a successful, innovative identity assurance scheme for the UK that can form the basis for identity assurance policies globally. These opportunities are discussed in more detail in the next chapter.

CHAPTER 10

The prospects for effective identity policies

When devising an identity policy, policy-makers often have a clear vision of what the resulting scheme will accomplish: just about everything. REAL ID was to prevent another 9/11; identity cards in the UK would combat identity fraud and benefits fraud, as well as terrorism and serious crime; biometric passports would prevent bad people from traveling around the world. All these years later it is often easy to look back with fondness at that era of simple solutions such as identity cards to complex problems like global terrorism.

In considering why identity policies are unlikely to provide simple solutions it becomes apparent that identity policies are themselves complex entities. The first step to an effective identity policy is therefore to acknowledge these complexities. When the UK policy proposals are taken into consideration with experiences of other identity policies, a number of key challenges emerge:

- No identification scheme 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 an entire population is misguided and counterproductive.
- 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 a zero-sum game where the value of one element is traded off against the value of other elements. Instead policy choices need to be made about each of these different elements.
- Public trust is the key to any successful national identity policy. Public trust can only be secured if citizen-facing issues of cost effectiveness,

dependability, security, legal rights, and utility are addressed and seen to be addressed at the same time as other, government-centered, policy objectives.

- Business buy-in is required for an effective identity policy. This means that the policy must address the concerns of industry, including service provision and liability issues as well as audit and compliance.
- A genuinely cooperative approach to establishing an identity policy must involve consultation based on principles as well as objectives. While a goal-based approach may provide short-term political cover and satisfy key stakeholders involved in those specific goals, the approach imperils other essential aspects, particularly public trust.

The UK's National Identity Scheme is a high-profile exemplar of the problems that can arise when these challenges are not properly addressed. Although planning for the Scheme began with the consultation around "entitlement cards" in 2002, the Government's current best case scenario is that significant numbers of UK citizens will only *begin* to be enrolled in the Scheme from 2012 – a decade after planning began.

In particular, the Home Office is failing to address the issue of public trust as the Scheme is increasingly unpopular with citizens and seen to be privacy-unfriendly, relying too heavily on centralized government management of data. The Scheme is also offering little of the functionality that industry requires.

The first part of this chapter reflects on why the traditional process of democratic scrutiny of the government's proposals was so inadequate and resulted in a Scheme that satisfies no one.

Academics are expected to understand the causes of things but they should also be able to make recommendations about the future direction of things and so this chapter develops the requirements for an effective identity assurance scheme drawing on lessons from the UK that can be adapted to other countries as well.

The chapter ends by reflecting on the role of academia more generally in contributing to, and engaging with, the policy process for identity policies and technologically-leveraged policies more generally.

Proposals for the democratic scrutiny of identity policies

It is tempting to suggest a mono-causal explanation for the almost unwavering progress of the fundamentally same identity policy for the UK from 2002 onwards. Such an explanation might be made in terms of the personalities involved or early technological lock-in to particular design decisions, yet these explanations fail to acknowledge the turnover of many of the key individuals (five Home Secretaries and counting, rotation of key civil servants in the Home Office and the Identity and Passport Service (IPS)), the two fundamental reviews that the Scheme has undergone, countless solicitations for and offers of independent advice and a procurement process that explicitly left implementation details to contracted suppliers.

Instead, the situation is best understood in terms of the limited ability of the democratic process to evaluate, scrutinize, and intervene in the development of an identity policy. Latour (2004) warns of the artificial separation of those who deal with the facts about science and technology and those who deal with the values of political democracy. In the case of identity policy we are not advocating a reintroduction of this divide by placing the decision-making power in the hands of technologists rather than politicians. We acknowledge and appreciate the role of democratic scrutiny by (elected) policy-makers. Indeed, in this case and earlier work (Whitley and Hosein, 2001, 2005) we have noted the important counterbalance that the (anachronistic and primarily unelected) House of Lords has played in the evaluation of technologically leveraged policies. The Lords have made a special effort to become informed about the particular characteristics and challenges that technologically leveraged policies introduce. Relying on conscientious individuals, however, is not inherently sustainable and needs to be supported by changes to the policy scrutiny process.

On the social shaping of technology

Technological developments, like social determinants, do not occur autonomously. Politicians can influence behaviors through the introduction of specific laws, by attempting to change norms or by influencing the market by making particular options more or less attractive (Lessig, 1999). A key starting point is an appreciation that decisions about identity policies can be directly influenced by the political process. The use of biometrics in a country's identity documents is not inevitable. Instead it is the consequence of decisions to legislate that they be included in an identity scheme, by the presentation of the technology as a means of "keeping everyone unique" or by stimulating the market for biometric enrolment functionality. Similarly, a second country may choose not to incorporate biometrics in their identity scheme, may emphasize the role that individuals can play in keeping their identity secure, and the government may not enter the market for biometric technologies. Another country may choose to provide an opportunity for individuals to use biometrics in their identity documents if they wish to do so, making specific design decisions that the biometrics would only be stored locally rather than centrally and may choose to intervene in the biometrics market by sponsoring academic research into applications of biometrics.

Associated with this notion of choice is the implication that not all choices have the same consequences. Although it has always been the case that alternative designs are theoretically possible, there are now systems in existence that demonstrate that different approaches to the design of identity schemes can be successful. A political process that assumes that the only way to build a government computer system is through a centralized data store ignores the potential benefits of federated and distributed systems, end-to-end functionality and citizen-focused schemes.

The private sector is struggling to acknowledge the benefits of being more customer-focused and is working to redesign its systems and processes so that they are no longer driven by the constraints of unimaginative technological designs. Just as in an earlier time it became unacceptable to argue simply that something happened because it was God's will, so it is becoming unacceptable to have a customer process driven by what the computer has determined: "the computer says no" (Postman, 1992).

In the specific case of identity policies, the review presented in Chapter 2 demonstrates that there is no one obviously best design for an identity policy. Instead each country's policy is a reflection of particular choices made by that country. These choices may be influenced by the size and ethnic makeup of the country, might be shaped by existing legacy applications and processes and might be swayed by historical circumstances. These concerns may also feed directly into the process of scrutinizing the policy proposals.

Given these influences, different countries have implemented very different identity schemes, many of which require the bespoke development of applications and systems that meet their specific requirements.

Recommendation

Technology is now a lever of policy-making and its effective use requires a careful appreciation of the constraints on, and flexibility of, technological components. The policy process should remain open to the design of systems that are driven by citizen-focused policy concerns and not misplaced beliefs about how technologies might operate in practice.

Technology is rarely infinitely flexible, however. Key design decisions taken early in the development process can often lock in particular architectures and limit future opportunities to adapt the system. This makes the early design decisions, which determine the direction rather than the detail of the implementation, particularly significant. These early decisions should therefore be based on careful consideration of the range of possibilities the technology affords.

On secrecy

Identity policies face many of the traditional challenges of any policy development. In particular the details of the Scheme presented in Chapters 3 and 4 are limited by the fact that key information about the government's proposals was being kept hidden and not disclosed (Edwardes et al., 2007). This secrecy was found in the case of the Office of Government Commerce (OGC) Gateway Reviews where the government argued against disclosure because of the potentially harmful effects on what was seen to be a particularly effective mechanism for internal oversight of government projects based on the candid exchange of opinions. Eventually, two of the reviews were made public and provided important insights into the government's thinking about its identity policy.

Commercial confidentiality was also used as an argument to prevent the disclosure of detailed costing of the Scheme, with the government arguing that if its detailed budget for the Scheme was made available this would disadvantage it in the competitive tendering process by distorting the normal information asymmetries that exist. However, when the Science and Technology Select Committee sought a confidential breakdown of the costs the Home Office "only provided a broad overview and did not include any figures" (Science and Technology Select Committee, 2006, §103). The six monthly s.37 cost reports have disclosed some of the project costs of the Scheme but a number of cost announcements (for example relating to contracts issued) are being disclosed to the press before they are reported to Parliament, suggesting that the Home Office is less concerned with its responsibilities to Parliament than with public perceptions of the Scheme and ensuring a positive news agenda. The KPMG review of the cost methodology (2005) has only been disclosed in summary form.

Recommendation

Arguments about "balance" and "proportionality" are frequently used when discussing the conflicting concerns of privacy and public good relating to identity cards, yet this same logic is not used when considering the question of obtaining value for money for policy proposals and the effective scrutiny of all aspects of policy proposals. In the case of technologically-leveraged identity policies, it is imperative that scrutiny is not trumped by claims of secrecy and that in due course full consideration is given to all aspects of the policy proposals, including costs.

If commercial considerations limit the disclosure of some of this information these limits must only apply for the duration of these considerations. For example, once contracts have been issued their details, including any "break clauses," should be made available for public scrutiny. Just as policy decisions made in one Parliament are not binding on future Parliaments unless they are implemented in law, plans for future Parliamentary business should not be constrained by secret contracts issued in earlier Parliaments.

On policy laundering

A key argument used to support the government's proposals was that the UK government was facing international obligations to upgrade its passports and that as a result, much of the cost of the Scheme would already need to be spent to meet this requirement. Such an argument appears compelling and provided much of the support for the Scheme from MPs, even if the first OGC Gateway Review does not report any such requirement as driving the policy. As Chapter 5 has shown, however, the reality of the situation is much more complex than this.

The Government failed to disclose that the Government had been a key driver behind many of the proposals for introducing biometrics into travel and identification documents. It failed to clarify that the UK was not actually under an obligation to implement these requirements and that its particular interpretation of the obligations was not the only one that existed.

The question of international obligations was reviewed in the LSE Identity Project but understanding the situation took months of research and analysis to access and understand the International Civil Aviation Organization documents, to try to make sense of their conventions and declarations and for colleagues to file requests using the Freedom of Information Act. In the absence of explicit disclosure of this complexity by the government, it is unreasonable to expect MPs with a full portfolio of other concerns to undertake similar research.

Such policy laundering is becoming increasingly commonplace and raises important questions about the authority of national parliaments in important matters of national governance (Raab, 2009). These other decision-making fora are not subject to the same level of scrutiny and influence as national parliaments. Of particular concern for technologically leveraged identity policies is the realization that policy laundering can result in a chain of "not scrutinised here" decisions, with each forum (wrongly) assuming that the technological components of the policies were (or will be) scrutinized in detail elsewhere. This results in policy decisions being enforced without any consideration of the implications of technological components.

Recommendation

Although parliaments may seek to introduce limitations on the amount of policy laundering that takes place, the practice is unlikely to disappear entirely. Therefore, when policies are introduced on the basis of decisions taken elsewhere, parliamentary scrutiny of the technological elements of the proposals must be undertaken unless there is detailed evidence presented to confirm that this analysis has been undertaken elsewhere in the policy chain. As noted above, this scrutiny should acknowledge that the technological components of the policy recommendations are open to more than one interpretation and so this scrutiny should not presume a simple, deterministic view of how the proposals must be implemented.

On the nature of technology

It was expected of the MPs to take the government's claims on the effectiveness of the technologies and the security risks of the proposals at face value. In so doing they were reinforcing the old divide discussed in Chapter 6 where scientists and technologists state the "facts" and politicians take value-based decisions. Doing so misunderstands the nature of the kind of science and technology that can drive policy developments. Just as with policy proposals relating to social policy there are always alternative viewpoints and perspectives that raise concerns and perplexities that the policy process must consider and, if appropriate, discount thereafter. An approach that does not bother seeking out "other" voices and expertise means that the policy process will be limited to the conventional wisdom that is presented in press releases and official statements from the government. As the proposals presented below show, there are always other ideas available that may be overlooked by "conventional wisdom."

It is inappropriate for the policy process to short-circuit consideration of technological perplexities by focusing on representations of technology coming from a limited set of sources. Effective deliberation therefore requires the expertise of informed advocates who are able to bring forward differing candidate perplexities that might influence the shape of the policy. In many cases, it is unlikely that Parliamentarians will have this necessary expertise themselves and so will require others, from academia, civil society, and industry, to fulfill this role for them.

To be effective, informed advocates need to be recognized for the insights and prioritization of the concerns that they can bring the policy process. The introduction of perplexities necessarily adds complexity and potential confusion but consideration of the perplexities will make the resulting policy better rather than worse. Informed advocates might be seen, therefore, as "critical friends." Implicit here is the argument that different groups of decision-makers might draw on different sets of such informed advocates as, recursively, it is unlikely that any group of informed advocates would have the complete perspective on the likely perplexities any more than another group of technologists.

Recommendation

Consideration of identity policies must draw on the issues and concerns raised by informed advocates and measures should be introduced to encourage and facilitate the development of an installed base of such advocates. Given the boundary-spanning nature of the skill sets of informed advocates, it is likely that they would need to be separate from the traditional research support provided to parliaments.

On ambiguity

There are many occasions where political statements may be intentionally ambiguous. They are often used to open up spaces for avoiding key discussions while alternative options are considered or resolved. In conventional policy areas the problems this strategy raises can be foreseen and understood by most policy-makers who have learned to read between the lines of these statements.

The limited technological knowledge of many policy-makers, however, means that they are less able to "read between the lines" when the intentionally ambiguous statements are made about technological issues. As Chapter 7 showed, such statements can unravel especially when they are subjected to scrutiny by informed advocates. The resulting shifts in policy that arise in order to address the stalemate that such unraveling can produce can affect the implementation of the policy in unexpected and potentially undesirable ways.

Intentionally ambiguous statements also undermine public trust in the proposals being considered as they raise the prospect that the government is deliberately hiding key elements of the policy.

Recommendation

Given that many politicians have limited knowledge of the capabilities of technological systems, it is imperative that intentionally ambiguous language is avoided for technological elements of the policy process. Instead, when key policy issues have not yet been determined, policy proposers should indicate these issues clearly, outlining the range of options under consideration and the most likely direction that the policy proposals are going to take. Such an approach is likely to engender trust in the proposals.

On certainty

Many of the issues raised above came together in the consideration of the language used to describe the UK Scheme as outlined in Chapter 8. Despite widespread realization in industry and academia that *any* large-scale system implementation is likely to face significant problems, slippage, and changing specifications, and despite the range of candidate perplexities raised by informed advocates such as the LSE Identity Project, the government presented its proposals using the language of technological certainty.

It is likely that the reason for this was that they did not believe that the democratic consideration of the proposals could allow for a situation where any fear, uncertainty, or doubt could be raised by the sponsors of the policy. Such a situation might be a realistic analysis of the current abilities of democratic institutions when evaluating technologically leveraged identity policies. It also clearly signals a lack of trust in both directions between the policy sponsors and parliamentarians.

Recommendation

Effective deliberation of identity policies requires greater levels of trust between the policy-makers and those reviewing the proposals. In the context of technological issues, a more effective and realistic strategy will be one that presents confidence in the ability to implement the proposals rather than certainty that it will cost exactly this amount or be delivered on exactly that day.

Policy-makers therefore need to be prepared to outline the basis for their confidence (for example, by drawing on existing expertise within government, or on the basis of detailed plans) and those scrutinizing the policy need to evaluate these beliefs in an objective manner rather than simply taking the lack of inappropriate detail as a sign of poorly thought through policies.

On public trust

The challenges to an identity policy do not cease once they have received parliamentary approval. The creation of public trust in an identity policy is also essential and can only be achieved by 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 policy is reliable and stable, and operates in conditions that provide genuine value and benefit to the individual and business.

These conditions are not easy to create. They must evolve through a clear, genuine, and thoughtful policy process that places the citizen at the center but acknowledges the requirements of business, government, and other relying parties in identity-based interactions.

Recommendation

Appropriate national identity policies must be based on a foundation of public trust and user demand rather than solely on compulsion and enforcement. As a policy that is leveraged through the effective use of technology, identity policies also require the use of reliable and secure technologies that are transparent and trusted. Many of the recommendations about the democratic scrutiny of identity policies above, such as transparent design choices, effective delivery based on decisions informed by visible discourse and deliberation, contribute directly to public trust in the proposals.

UK-specific considerations

The experiences of the UK identity policy process highlight a number of further issues that might not be replicated in other countries. Nevertheless, in the same way that policies are laundered between countries, a parallel process of informed advocacy "laundering" might highlight similar concerns in other countries.

Throughout the Parliamentary debate about the Act, Home Office ministers emphasized the fact that the Bill was "enabling legislation" that would "allow" a National Identity System based on identity cards to be introduced. As a result, they stated that there was "much still to be done in terms of detail, regulations and all the other elements" [Tony McNulty, 28 June 2005, Column 1253].

As such, many of the details of the Scheme were not included in the Act, with these details being left to secondary legislation and statutory instruments. The OGC Gateway Review in June 2003 emphasized that "the key accompanying secondary legislation, will need to proceed alongside the work on project definition" (Office of Government Commerce, 2003). In practice, however, the secondary legislation was not issued in draft form until November 2008 (UKIPS, 2008c) with key decisions (such as the decision to keep the National Identity Register Number (NIRNo) off the face and chip of the card) appearing to be made at the last moment (cf Science and Technology Select Committee, 2006, Conclusion 1).

The use of secondary legislation is not without its critics, as was acknowledged by the Home Office minister Tony McNulty during the Bill's Committee Stages in the House of Commons: "I shall pass over what is in part a serious debate about constitutionality, secondary legislation and the 'Christmas tree' nature of enabling legislation" [7 July 2005, Column 88].

The role of secondary legislation was also raised during the Parliamentary debates. For example, Democratic Unionist Party MP Mr Robinson noted: "Secondary legislation would be most unsatisfactory for dealing with changes in such an important measure. It does not give the House the ability to amend; we would simply be asked to accept, on a take-it-or-leave-it basis, any package that the Home Secretary might introduce" [28 June 2005, Column 1204].

A further problem with secondary legislation is that, in practice, the debates are often poorly attended and so effective scrutiny of the details of the Scheme will be limited, raising the prospect of what Conservative MP Edward Garnier described as "legislation by statutory instrument" [18 October 2005, Column 804].

Another argument for "enabling legislation" is that it allows for what might be called "technology neutral" policy. Rather than specifying in legislation what technological measures might need to be put in place, this form of legislation allows for these details to be added at a later stage, such as during the procurement process. For example, the final version of the Act simply states that an individual may be required to allow "his fingerprints, and other biometric information about himself, to be taken and recorded" rather than specifying the specific technologies that will be used by the Scheme. By not specifying that these biometrics must include face or iris recognition biometrics IPS was able to lower the risks and cost of the Scheme by dropping the use of iris biometrics in the revised Strategic Action Plan. Further "cost savings" were introduced in the Delivery Plan where the biometric enrolment process was moved to the open market, with the costs of biometric enrolment passed to the citizen as a separate cost element.

The Act further confuses the distinction between technology neutral legislation and legislation with specific design implications in the role of the Register. Thus, while the Act does not specify the form of biometrics to be stored by Government, it does specify that the Secretary of State "establish and maintain a register of individuals" (s.1(2)) that includes "information about occasions on which information recorded about him in the Register has been provided to any person" (s.1(5)(i)) (i.e. the audit trail). It also specifies other audit details that are recorded on the Register including

- the date of every application by him for a modification of the contents of his entry;
- the date of every application by him confirming the contents of his entry (with or without changes);
- particulars of every occasion on which information contained in the individual's entry has been provided to a person;
- particulars of every person to whom such information has been provided on such an occasion; and
- other particulars, in relation to each such occasion, of the provision of the information (Schedule 1 (6)).

As can be seen, this is a very detailed design specification for the Scheme and its operation. Although nominally neutral about the technology it actually implies a very particular way in which the Scheme would be used in practice. For example, it strongly suggests verification against the Register for confirming someone's identity (rather than, for example, verification against the card). It is also clearly based on a particular, centralizing approach to identity management rather than a more citizen-centric, federated identity assurance scheme.

Although Parliament approved the Act as the basis for enabling the Scheme, this pretence at technological-neutrality means that any alternative identity proposals introduced by future governments will find it more straightforward to repeal the Act and, probably, the UK Borders Act 2007 rather than seek to unravel the general "enabling powers" in the Act from those design decisions that are considered undesirable. Further Parliamentary costs arise from this mixture of technology-neutral and technology-specific legislation as to repeal these Acts would first require transition measures (for example, addressing the status of currently issued biometric immigration documents and the regulations that surround them) to be passed before the Acts can be repealed.

Section 37 of the Identity Cards Act 2006 provides the requirement to report to Parliament on the likely costs of the Scheme for the next ten years. It was explicitly introduced in response to concerns about the oversight of the Scheme by Parliament, given concerns about the lack of disclosure of costs. As such, one would expect that changes to the costs of the Scheme, even when just reporting cost changes for the Home Office, would be made to Parliament in the first instance. However, on a number of occasions, the timing of cost announcements has been driven by broader political considerations rather than any consideration of Parliamentary privilege. A number of these announcements were made in public meetings before they were announced to Parliament or were delayed to coincide with other high-profile announcements on other matters.

In a similar manner, the 2006 Strategic Action Plan was presented to Parliament on the last day before the Christmas Recess, effectively guaranteeing that no discussion about it would take place.

When Gordon Brown was Chancellor of the Exchequer he appointed Sir James Crosby to lead a public–private forum on identity (Brown, 2006). Sir James undertook a detailed review of the issue and was widely acknowledged as having grasped the key issues underlying any effective identity policy. He wrote a detailed report that gave specific recommendations for the implementation of such a policy. Although the government has frequently claimed that it has incorporated Crosby's recommendations into its identity plans, in practice, the government chose to issue its 2008 Delivery Plan on the same day as Crosby's report was finally released.

Given the differences in emphasis between Crosby's recommendations and those of the Delivery Plan, this was clearly an attempt to bury Crosby by overwhelming the media with the details of the Delivery Plan, a strategy that, to some extent, succeeded (Pieri, 2009).

Although Crosby's recommendations are widely respected in industry the government's attitude to drawing on them can be seen from a Parliamentary answer:

> It is intended that, where it is appropriate, the scheme *once it is in place* should take account in whole or in part of the principles established in Sir James Crosby's report. [WA 219757 emphasis added]

This answer reveals both that Crosby's recommendations have not been taken on board and, more worryingly, a belief that fundamental changes to the implementation of the Scheme can be bolted on at a later time.

Recommendations

Technology-neutral policies rarely are. Rather than continuing with the pretence that identity policies can be developed by presenting enabling legislation with the details to follow, key design decisions (such as whether to have a centralized system or not) must be explicitly written into the legislation and debated as such. Similarly, while implementation details (what exactly is the process for biometric enrolment, what penalties and appeal procedures and forms will be followed?) can be left to secondary legislation, key design decisions should not be left to the limited scrutiny that secondary legislation receives. Instead, these issues should be explicitly addressed and debated during the formal consideration of the main Act.

Where the reporting on costs is mandated by Parliament, government should respect the wishes of Parliament by presenting any significant changes to the costs to Parliament in the first instance. Similarly, for public trust in a policy to grow, key reports and policy changes should not be buried under other news stories that are under the government's control.

Toward an effective identity policy

As this book has shown, there is no shortage of exemplars that address many of the articulated goals of an effective identity policy. There are also many published accounts of the principles that an effective identity policy can draw upon (e.g. IAAC, 2009; Sir James Crosby, 2008). There is also growing awareness of the specific challenges that an effective identity policy must address. Where choices are made between alternative responses to them an explicit rationale must be provided. Amongst the challenges and choices that need to be made is consideration of the following points:

- An identity scheme should be inspired by clear and specific goals (i.e. not as is found in the Act "for the purpose of securing the efficient and effective provision of public services" (s.1(4)(e))). Successful identity schemes embrace clear objectives that facilitate responsive, relevant, and reliable development of the technology. This helps limit the potential for abuse of the scheme.
- An identity policy 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 scheme.
- Identification systems must be transparent. Public trust is maximized when details of the development and operation of an identification system are available to the users.
- 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. Identity disclosure should be symmetrical whereby the person disclosing their identity is satisfied that the person requiring this disclosure is duly authorized to request it. Over-use of an identity scheme will lead to the increased threat of misuse and will erode public trust.
- An identity policy 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 everyday life.
- An identity policy should also serve the private sector. Commercial organizations are the relying parties in the use of a scheme and so need assurance about the enrolment processes used and the authentication procedures provided by the scheme.
- An identity policy should be more than just an identity card and indeed, does not need to be based around a "card" at all. Identity systems must exploit secure and private methods of taking advantage of electronic delivery of benefits and services.
- Personal information should always be controlled by the individual. Any biometrics and personal data associated with an identification system should remain, to the greatest extent possible, under the control of the

individual to whom it relates. This principle establishes trust, maximizes 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 identity credential, the registration process should, to the greatest possible extent, be localized 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 easily.
- To the fullest extent possible, any potential for "function creep" must be designed-out of the scheme. For instance, identity numbers should be invisible and restricted to prevent inappropriate use. Any unique code or number assigned to an individual must be cryptographically protected and invisibly embedded within the identity system. This has the additional advantage of limiting the potential for wide-scale identity fraud.
- It is increasingly necessary for there to be a capability for multiple authenticated electronic identities. An identity scheme 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 sector-based credential can be 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.
- The scheme must be designed in such a way that there is minimal reliance on a central registry of associated data. Wherever possible, in the interests of security and trust, large centralized registries of personal data should be avoided.
- To ensure that the scheme is more reliable, it must permit secure and private backup of associated data. An identity scheme should incorporate a means of allowing individuals to securely and routinely backup data stored on their card. This facility will maximize use of the identity credentials.
- Any identity policy should explicitly address concerns about identity exclusion, which might arise in the enrolment and verification stages. For example, a policy that requires evidence of bank accounts or a stable home address or requires or restricts particular languages or national symbols on identification credentials carries the risk of creating a subclass of identity-excluded individuals who are unable to realize the

benefits of a universal identity scheme. Any national scheme needs to explicitly incorporate consideration of these issues from an early stage.

Innovations arising indirectly from the UK experience

The problems with the UK attempts at introducing a new identity policy described in Chapter 9 open up novel opportunities for implementing a successful, innovative identity assurance scheme. Chapter 9 has highlighted the unintended negative consequences of the UK plans to give the proposed identity cards the same functionality as passports and the problems with linking the enrolment and issuing of identity cards to the enrolment processes for passports. By breaking the link between identity policies and government, conceptually at least, new opportunities for innovative identity policies emerge.

As discussed in Chapter 1, any successful identity assurance policy needs to address a series of potentially conflicting policy drivers while also not introducing new problems and making the situation worse. That is, a successful policy needs to find a way through the complexity of technological, legal, political, and societal issues in a way that minimizes the political risks associated with their implementation.

Starting from the perspective of business (which in this context can include the "service" side of government as well), modern identity credentials are required to enhance trust in commercial interactions. That is, one body (the "relying party") needs to know that the other is who they say they are (or have the attributes that they claim to possess) and they need to know the basis of this assertion (i.e. who is the "identity service provider"?). If this process is a mediated one (e.g. on-line or via the presentation of an identity credential) then there is a further requirement that the person presenting the credential is in fact the person about whom the identity service provider is prepared to support the assertion. Before deciding to interact with the individual, to provide services for them, or to allow them access to some of their resources, the relying party takes a commercial decision based on the identity assertion being made. This commercial (risk) decision may include consideration of what is known about the identity service provider, an evaluation of any mediation activities and consideration of liability/repair issues if problems arise.

The individual perspective on identity management is increasingly driven by privacy concerns and consumer choice. For example, citizens are increasingly aware of risks to their personal data in centralized databases (Pieri, 2009), the problems of irrevocable biometrics (Sir James Crosby, 2008), and frequently have multiple personas on-line (Whitley, 1997). Just as it is no longer accepted that the government is necessarily the best (sole) provider of telephone services or water supplies, so it is not necessarily the case that identity services should be driven by the government. This is particularly the case when much of the biographical enrolment for an identity scheme will draw on data held in commercial databases held by credit reference agencies and others.

Both perspectives, however, share concerns about the visibility and reliability of the initial enrolment processes and both increasingly require authentication processes to be undertaken remotely such as over the internet.

For commercial organizations, particularly those in high assurance environments, there is a particular emphasis on the initial enrolment which might typically (but not necessarily) be tied to government-issued credentials. In such cases, the enrolment process might be described as “identity proofing” and may also incorporate vetting processes. For other organizations, however, this link to nationally issued credentials is less important. Thus, in the case of age-restricted purchases, the relying party needs to trust that the identity document does confirm that the person satisfies the age requirement but this does not necessarily have to be a government-issued document as many other services providers (banks/schools/mobile phone providers etc.) might be prepared to stand behind the age-related assertion.

In other cases, the assertions might be provided by a low-integrity source that is appropriate for that context, so in an on-line game environment, the attribute that another player has particular powers might be provided by no more reliable authority than the game provider.

To these concepts it is important to add the principle of data minimization recommended by the Home Affairs Committee (2008), amongst others. This principle states that organizations “should collect only what is essential, to be stored only for as long as is necessary.” A corollary of this is that even if more extensive data has been collected, the principle of data minimization should also apply to the data that are disclosed and shared.

To illustrate this point, consider again the example of access to age-restricted services given in Chapter 1, such as entering a bar. Here the relying party (the bar manager) needs to know that the person buying the drinks is of legal drinking age and that the person claiming this attribute is the person presenting the identity credential.

In the current UK Scheme, the identity card is intended to also function as a travel document within Europe. This means that the face of the card must contain the required fields for travel documents specified by ICAO. Passports (and hence identity cards that can be used for travel within Europe) have the person's date of birth (and full name and place of birth) on them. In addition, because there will always be occasions when automated passport readers are unavailable, this data must also be readable by humans. This means that this personally identifiable information must be printed on the face of the document.

As a consequence, the use of the identity card as proposed by the UK government will *always* disclose the person's date of birth, full name, and place of birth even if these are not required by the relying party. Moreover, because they are visible on the face of the card, suitable for visual inspection, there is little incentive for introducing readers that will check these details from the chip on the card if it is easier (and cheaper) to check the details by looking directly at the card.

As noted in Chapter 1, personal data like date of birth, place of birth, and full name are incredibly useful elements for undertaking identity-related fraud as they provide useful starting points for identifying other "security" data such as mother's maiden name.

The formal requirement in this situation, of course, is simply authenticating that a particular individual is able to access particular age-related services. A process that includes assessing the basis of the assertion and confirming that the assertion applies to the physical being claiming that attribute. The age satisfying requirement is clearly a function of the relationship between today's date and the person's date of birth. It does not, however, require the disclosure of the date of birth (that is, although a person's date of birth falls within the set of data that would be collected even when following the principle of data minimization, it does not fall within the minimal set of data that needs to be disclosed).

Dave Birch (2009b) provides a charming illustration of how a technologically leveraged identity policies might be implemented to provide identity assurance capabilities while minimizing unnecessary data disclosure. He begins with the idea of Dr Who's "Psychic Paper." This "technology" from the popular TV series has the unique property of displaying whatever the reader expects to see. Thus, if the psychic paper is presented to someone expecting to see a Press Pass they see a Press Pass, if they are expecting to see a theater ticket they see a theater ticket.

What is significant is that the Psychic Paper only discloses the minimum amount of data necessary. In the context of the example above, the Psychic Paper will simply disclose whether or not the person satisfies the age-related condition (over 18) being requested. To ensure that the assertion about age is being made about the correct person, the disclosure might take the form of displaying the photograph of the individual if they are over 18 and not displaying their photograph if they are not.

At a technological level, such an approach offers some intriguing possibilities (Brands, 2000). First, the implementation does not rely on carrying a card, but can be embedded in any technological device. Thus, many individuals might wish to have this functionality implemented as part of their mobile phone, others might choose to offer this functionality in other devices and not necessarily a card. Interestingly an episode of Dr Who featured the Psychic Paper acting as an Oyster travel card, hence demonstrating that it can also mimic an ISO 14443 interface (Birch, 2009a).

Second, it is possible to ensure that control over what information is disclosed remains with the individual. Thus, the individual can control whether or not to disclose that they are over 18 by requiring the bar manager to first authenticate that she is authorized to ask for proof-of-age authentication from bar guests. This allowed-to-confirm-age check can be undertaken in exactly the same way as the proof-of-age check is undertaken. The individual can also control that only confirmation of age data are transferred. This issue of symmetrical checking can be particularly significant for vulnerable groups, such as the elderly greeting someone claiming to be from their electricity company. That person's identity credentials can be checked in the same way and the householder can decide whether to let them into their property based on whether that person's identity credential has been issued by their electricity company.

In other situations, the individual might be prepared to disclose their full name or address for direct entry into the service provider's system. Such user-centric control also allows an individual to revoke the data that might potentially be shared with others and could easily allow for "multiple" identities to be used (e.g. professional identity, social networking identity etc.). Each of these identities might offer limited functionality in some areas. For example, the identity used for an on-line gaming environment might be able to assert that an individual has particular game-playing powers, which could be authenticated by other game players, but would not be able to assert that the individual was over 18 for entering a bar.

Third, because the authentication process takes place over a suitably secure connection and uses cryptographic techniques, there is no need for a centralized database and audit trail of transactions as is found in the current UK plans for on-line identity-checking services. If a record that a particular transaction has taken place is required, this can be kept locally on each device requiring the consent of both parties before it can be disclosed.

In particular situations, it might also be accessed by suitably authorized law enforcement officers.

The processes underlying this minimal disclosure process are infinitely scalable and allow for a market of authentication providers to exist, offering differing levels of authentication assurance. For example, those individuals who simply require the ability to confirm that they are able to access age-restricted services do not necessarily need this functionality to be provided by a government-based identification scheme, instead the age-verification used by the device can be based on, for example, details held by their mobile phone company, bank, or even education provider (school, university). This pushes the responsibility for confirming the date of birth of the individual, for example, onto these other organizations (rather than, for example, the data held on the Register) but given the relatively low level of risk associated with age-verification services, this is a manageable risk that these companies might be prepared to take. For example, a mobile phone company may restrict access to "adult" sites via its phone internet services based on existing age checking and can use the same processes to allow third parties, such as bars, to confirm that the phone user is over 18. One obvious benefit of this market of identity service providers would be a far faster roll-out of electronic identity credentials.

In contrast to the government's current plans for biometrically driven identity cards, these proposals do not necessarily require the storage and processing of biometric data such as fingerprints. Although the UK government has claimed that a key driver for the collection of biometric data is the requirement to guarantee uniqueness on the Register (i.e. using the biometrics to check that the same physical person has not enrolled in the Scheme with two identities), in practice this is not done in other countries and it is unclear whether the proposed means of biometric enrolling and matching will succeed for a population the size of the UK.

Some identity assurance services may require biometric authentication (i.e. a more rigorous check that the credential belongs to the person presenting it than simply displaying a photograph of the person). In such cases, the individual would be able to opt for an identity assurance provider who would provide biometric enrolment services, including the storage of a template of the biometric on the identity device (cf Sir James Crosby, 2008), which can then be used for a one-to-one match against the template of the biometric presented at the authentication stage. However, the choice of whether to enroll biometrics would be left to the individual and, because it is not stored centrally and in template form, would remain under their control.

On academic policy engagement

According to one of the key readings within the literature on policy-making and the policy process, academic engagement with the policy process:

> contributes to public deliberation through criticism, advocacy and education. Good policy analysis is more than data analysis or a modelling exercise; it also provides standards of argument and an intellectual structure for public discourse. Even when its conclusions are not accepted, its categories and language, its criticism of traditional approaches, and its advocacy of new ideas affect – even condition – the policy debate. (Majone, 1989, p. 7)

In a similar manner, Torgerson (1986) describes policy analysis as “those activities aimed at developing knowledge relevant to the formulation and implementation of public policy” (p. 33). In the case of technologically-leveraged policies, this knowledge relevant for the formulation and implementation of public policy should include an understanding of technology and its relation to society more generally.

The systems that are being proposed by technologically leveraged policies exist not as isolated technical systems, whose inputs and outputs can be formally specified in engineering terms, but rather need to operate in complex, messy environments where they interact with users who are best understood as social actors (Lamb and Kling, 2003). In this context, Tim Berners-Lee has called for the creation of a new web-science research institute which would “attract researchers from a range of disciplines to study it as a social as well as technological phenomenon” (BBC News, 2006b). On other occasions, the case for the consideration of the broader social context is not made so clearly; shortly before Berners-Lee made his call for consideration of the social side of technology, Google CEO Eric Schmidt called for “techies to teach governments” and help them understand the internet’s role in society (Broache, 2006). Former Conservative MP Chris Patten noted that “many politicians do not understand the technology issues that could affect government IT schemes.” Instead, he suggested, “they rely on advisors for information on how to implement their broad intentions. You have to hope they’re well advised” (Espiner, 2006). This is an argument that has frequently been made before (e.g. Sarson, 2006; Thompson, 2006).

Thus, following Majone and Torgerson there is a clear need for academics to engage in policy analysis and condition the policy debate by introducing new categories and language, critiques of traditional approaches, and advocacy of new ideas. Second, many of these policy areas in government are driven by technological measures and yet government seems particularly unable to appreciate the complexities of technological systems. Third, although an understanding of the technological features of these systems is important, a broader consideration of the technology in its organizational context is particularly important.

Academics have a particular status in society: they are typically funded by the public purse and have a high degree of autonomy. The principles of academic freedom are enshrined in the tenure process whereby academics are safe from concerns about job security that normally constrain challenges to the status quo. As such, academics have a duty and a responsibility to use their unique status to address policy issues using their particular expertise. The distortion of this privileged position that emphasizes publication in high-status outlets over the creation, preservation, and distribution of knowledge (Lyytinen et al., 2007) may, ultimately, result in reduced scope for academic freedom.

The LSE Identity Project was one attempt that used the unique status of academics to influence the policy process for the UK's identity policies. It had both direct and indirect influences on the policy process.

Direct influences on the policy process

One of the clearest examples of the role that the LSE Identity Project played is the number of mentions its work received in Parliament, with over 200 explicit mentions of LSE reports during the 56 days of Parliamentary debate. When the research was drawn on by Parliamentarians opposed to the Bill, it was referred to favorably, as in this extract from a speech by Conservative MP Edward Garnier during the House of Commons Committee stage:

> My hon. Friend the Member for Newark has, quite properly, referred on a number of occasions to the valuable work done by the team at the London School of Economics. They have spent some time looking carefully at the subject and have reached a number of conclusions. I make no claims of originality; I am relying heavily on the findings of the LSE report. [12 July 2005, Column 229]

When the research was referred to by the government, a rather different tone is found. For example, this statement was made by Home Office minister Baroness Scotland, in the House of Lords:

> There seems to be a basic error. We were surprised to discover, for example, that in the body of the report undertaken by the LSE there was no reference to one of the major reports on biometrics and the way in which that was dealt with in the United States. It is unusual for such a gap not to have been addressed. That is surprising. [19 December 2005, Column 1564]

The work also influenced the public perceptions of the government's arguments for identity cards, as can be seen in this extract of a letter written to *The Times* in November 2006 after a columnist suggested that identity cards could help in the fight against terrorism:

> Sir, Alice Miles says biometric ID cards could help to prevent terrorism (Comment, "We face a terrible threat – so storing my dull, private details is no big deal," Nov 8). However, the London School of Economics reports that: "Of the 25 countries that have been most adversely affected by terrorism since 1986, 80 per cent have national identity cards, one third of which incorporate biometrics." Identity cards clearly do not make countries safe from terrorists. (Watson, 2006)

Perhaps the most humorous example of the direct effect the research had on the Parliamentary process is found during one of the more contentious debates in the House of Commons on 13 February 2006. The Government's front benches jeered on the first mention of the LSE (this was recorded in Hansard as an "interruption") [13 February 2006, Column 1180].

Indirect influences on the policy process

One of the stated purposes of identity cards is to help address problems of identity fraud. However, the analysis of the government's figures for the likely level of identity fraud in the UK has meant that the media rarely reports such figures uncritically (see also Chapter 1 and Pieri, 2009). Indeed, when in 2006 the government announced that identity fraud was costing the UK economy £1.7 billion per year, up from £1.3 billion, a number of media reporters discovered that there were many problems with these revised figures (McCue, 2006) and the skeptical tone continued:

> You cannot open a newspaper these days without being confronted with apocalyptic warnings about identity theft. It is apparently Britain's fastest-growing crime, costs the UK economy an estimated £1.7bn a year and is an invisible menace that can cause damage for months before you realise it has happened to you ... The latest evidence suggests that [evidence of the scale of the problem] is far from clear cut. This week saw the publication of official figures for UK credit and debit card fraud. These include data on levels of card identity theft – which includes crooks using a stolen or fake ID to apply for a card, or raiding dustbins to obtain personal information such as bank details to take over someone's account and run up huge debts. The figures reveal that, rather than shooting up, losses from credit and debit card ID theft fell by 7% during the six months to June 30 this year – from £16.1m to £15m. Losses from lost and stolen cards also fell, as did those for fraud committed with cards stolen before the genuine cardholders receive them. (Jones, 2006)

Other benefits were claimed for the Scheme. However, when the then-Prime Minister Tony Blair wrote about them in 2006, his piece was carefully nuanced about these benefits, arguing that he was:

> not claiming ID cards, and the national identity database that will make them effective, are a complete solution to these complex problems [of illegal immigration, crime, terrorism and identity fraud]. (Blair, 2006)

Written answers about the international obligations that apply to the security of passports have also become more nuanced:

> Travel document standards, including those relating to the minimum security features of such documents are set by the International Civil Aviation Organization (ICAO) in their Document 9303. The United Kingdom passport complies fully with the ICAO standards, both in relation to the travel document specifications and the security features. In relation to the latter, the UK passport surpasses the minimum standard required.
>
> The EU Council Regulation (EC 2252/2004) on standards for security features and biometrics in EU citizens' passports requires Schengen

> states to issue passports that comply with a minimum level of security features, including biometric identifiers. The UK is excluded from this regulation (as it is a Schengen building measure). Nevertheless the UK complies with the measure in relation to security features and the inclusion of the facial image biometric, and intends to comply with the requirement to include fingerprints in passports. [WA 269314]

This suggests that leading politicians and civil servants had realized that they could no longer make the simplistic arguments about the issue and that the LSE report had affected the "standards of argument" used and provided "an intellectual structure for public discourse."

Rigor and relevance

A common theme in the meta-debates about many forms of academic research is the apparent dichotomy between rigorous and relevant research (see, for example, Whitley and Hosein, 2007 and Benbasat and Zmud, 1999). This is typically characterized as differentiating between highly controlled, often experimental research, which may present results that are of limited direct applicability to practice, versus research that has direct relevance to practice but might be based on research methods that are not as rigorous.

In terms of relevance, particularly during the latter stages of the Parliamentary debates, the LSE Identity Project issued a number of reports and briefings often on a weekly basis. For example, between 15 January 2006 and 3 March 2006, the LSE published two reports, three Parliamentary briefings, an opinion-editorial piece for a national newspaper, and a written submission to a Parliamentary Select Committee (see Table 10.1).

More generally, involvement with the Parliamentary debate was ongoing throughout the entire deliberations and members of the project team were frequently called upon by the press to comment on developments. In addition, Parliamentarians from all parts of the political spectrum were regularly asking for additional commentaries.

In terms of rigor the government attempted, on a number of occasions, to dismiss the LSE Identity Project as flawed research. In response the project frequently had to respond by highlighting the detailed, fully referenced research that underlay its findings. The very nature of the work and its high profile required rigor-by-design. Throughout the research and writing process there was an explicit concern about the reaction from friends, "enemies," and the media if even small errors in judgment were made.

Table 10.1 Relevance in practice: Documents produced by the LSE Identity Project, January–March 2006

Date of publication	**Publication**
Sunday 15 January 2006	Second report: *Research status* Report
Monday 23 January 2006	Briefing: Voluntary versus compulsory regimes
Friday 3 February 2006	Submission to Select Committee inquiry
Monday 6 February 2006	Briefing: Identity fraud
Monday 13 February 2006	Briefing: Nothing to hide
Friday 17 February 2006	Newspaper opinion-editorial piece: Hang together – or we will hang separately
Friday 3 March 2006	Third report: Home Office Cost Assumptions

Source: LSE Identity Project (2009).

In standard academic studies it is taken as a matter of faith that the researchers conducted their research with integrity; in the public sphere of media and political campaigns there is no such faith, and the project would have encountered an unforgiving set of forces if it failed to conduct its research with integrity.

More interestingly, another test of rigor was that with every interaction and engagement the project learned more about ontology, epistemology, methodology, and the domain of politics and technology. This constant learning cycle prevented the project members from ever standing up and claiming authority over all other sources of knowledge, unlike its critics.

Policy engagement and action research

Given the direct and indirect influences on the policy process outlined above, members of the LSE Identity Project have, as reflective individuals, spent some time considering the effects of their role on the research process (Alvesson and Skoldberg, 2000). This involvement, however, cannot be accurately described as action research which is a process that depends on the social interaction between observers and those in their surroundings. The main contention of action research is that complex social processes can be studied best by *introducing changes* into these processes and observing the effects of these changes (Baskerville, 1999). During action research, as the researcher and the subjects interact, a shared meaning develops and in some ways the worldview of the researcher approaches that of the subjects (Mårtensson and Lee, 2004).

Although the work did have effects, the LSE Identity Project cannot be described as "introducing changes," nor was the purpose to observe the effects of specific interventions. In a similar manner, although team members spoke extensively with the press about the work, they did not (and could not) create a media campaign on the issue. Thus, although team members were involved as participatory observers, they did not determine the nature of the interventions and had even less control over their consequences. Finally, it was never the intention to introduce changes in the environment to, in turn, study their effects. The point of the activity was simply to engage with the policy-makers, experts, and others to inform debate.

Dangers

Academic participation in the policy process, even in the role of informed advocates, is not a neutral process. Academic studies that are critical of government proposals are unpopular and, as Chapter 3 notes, the LSE experience resulted in ad hominem attacks on key members of the project team and, implicitly, the LSE as a whole.

This would suggest that "outsider" policy engagement of this type should, perhaps, only be contemplated if the university governing body is willing to stand publicly behind its academics and to resist all forms of political pressure. The Identity Project was lucky enough to work in an institution where it received such unwavering support, but one is left wondering how many other like-minded universities are out there. What would have happened if the institution had not stood by its academics? Though some may disagree with the findings, few would doubt the importance of the research and presenting the analyses as effectively as possible.

A special role for information systems academics?

Much information systems research is focused on issues that are of particular relevance to business organizations and here information systems academics are making useful contributions to theory and practice. In addition, information systems researchers have also become more visible in less traditional organizational contexts, including government, not-for-profit organizations, and socially excluded groups, as well as developing countries. However, information systems researchers are not actively participating in an important area where the insights and approaches of information systems research can make important contributions, namely the policy-making process for technologically-leveraged policies.

All too often the leading academic voices in technologically leveraged policies are coming not from information systems academics but from computer scientists, lawyers, or political economists. In each case, these academic contributions are useful and appropriate, but each issue could also draw on the contributions of information systems researchers who are ideally placed for considering the relationship between technology and its wider social and organizational setting. That is, whereas computer science, law, and political economy can be characterized as academic disciplines, information systems is a field that applies insights about the relationship between the technical and the social to specific problem areas. This gives information systems academics particular strengths of interactional expertise that make them strong candidates for the role of informed advocates as described in Chapter 6.

There are many challenges to developing identity policies, but also many opportunities to take advantage of the features of new technologies to provide secure identity assurance policies that benefit citizens and governments. It is up to policy-makers to take advantage of these opportunities. This book is intended to provide them with insights that will enable them in this task.

Acknowledgment

We would like to thank Simon Davies for his work in helping to identify the challenges presented at the start of the chapter. They have been applied to our identity policy work for the Canadian Federal Privacy Commissioner, the U.S. Federal Trade Commission, HM Treasury and the United Nations High Commissioner for Refugees.

Methodological appendix

Orientation

This appendix outlines the many research techniques used in association with the ideas involved in this book. Although researchers invariably become deeply involved with their research, in our case the involvement became one of almost total immersion, at least in the early stages. For example, we were frequently asked to comment on and analyze government statements about the Scheme within hours of these statements being published. This meant that we did not have time to do independent coding of the statements, slowly develop the analysis and then draw the broader implications of what had been said.

Instead, our immersion in the Scheme meant that we quickly developed a perspective on the situation that allowed the important aspects to stand out, while downplaying less significant elements. For example, when the Strategic Action Plan was issued in December 2006 we immediately saw that iris biometrics had, effectively, been dropped from the Scheme.

Another key feature of our involvement was that we were able to develop a longitudinal understanding of the Scheme and its development. Longitudinal case studies have a strong tradition in management research with some authors arguing for the importance of temporal interconnectedness. That is, in order to understand what has happened at any particular point in time, it is important to understand the events that preceded it.

We could only comment on the changes to the Scheme because we knew all that had come before. In many ways this is what qualified us as "experts" on the policy, while others may be experts on the technological or legal issues, we were observers of the policy process over time.

A third distinctive feature of the work presented here is the extensive use of quotations from a variety of official sources and statements, including the official Parliamentary record (Hansard), Parliamentary committees, and official publications by the Home Office and the IPS. These sources were specifically selected because they either reflect "official" views on the issues (each of the formal documents will typically have been reviewed by a number of civil servants before being issued) or because they are based on statements made to Parliament by individuals who typically will have been briefed in advance of making the statements. The official transcripts (e.g. Hansard) of Parliamentary debates are not necessarily a completely true and complete record of exactly what was said in Parliament, as specific norms have been developed for the recording of what was said. The official record does, however, provide a useful resource covering what was said both for and against a particular piece of legislation. Though we attended a number of sessions in Parliament and watched the debates on-line, in real time and after the fact, we still rely on Hansard for the statement of record.

This is both an advantage and problem for the analysis presented in the book. As outlined above, advantages include that the public record contains all statements made during Parliamentary debates and Committees regarding the Scheme. This record is freely available and easily searchable. The main problems, however, arise because of the ways in which the official record is based on naturally occurring speech. Thus, while Parliamentarians may well be carefully briefed, their statements might contain errors and omissions that a printed document would not. Similarly, points that a speaker plans to make might never be made if the flow of argument and debate moves the topic along. Thus, particular care must be taken to contextualize all statements that are analyzed and it is possible that while the gist of an argument might appear throughout a statement, no easily quotable statements can be isolated to readily summarize that argument.

This extensive reliance on what the government said about the Scheme is a direct consequence of the attacks made on the integrity and quality of the research presented in the LSE Identity Project. We did not want to provide any opportunities for our research to be discredited simply because we had attempted to paraphrase the government's position. Indeed, for a number of generalist publications (such as opinion-editorial pieces) we would typically provide two versions, one for public consumption and one with footnotes detailing where all the quotations came from, so that the publication could be assured that there were no problems with what we were claiming.

Data collection

As noted above, our research draws on just about every publicly published piece relating to the Scheme. For example, our first tasks each morning were to search through the Google News service for mentions of the Identity Cards Scheme and check the Parliamentary Written Answers that had been published that day. In the former case, we also relied on an extensive network of colleagues who would forward us relevant news developments and reports as they arose. For the latter, in some cases, it became clear that what was presented in the Written Answer was not intended to be taken quite as literally as it appeared, as in this answer about additional data storage that might be needed to administer the Scheme:

> Until the national identity scheme is up and running it is too soon to determine the amount, if any, of additional storage that will be required to administer the national identity scheme. [WA 185514]

The documents were all archived so that it is easy to search through. For example, we archived all the Written Answers in such a way as to identify details of any statements about the expenditure on consultants associated with the Scheme. Similarly, a complete archive of both sets of Parliamentary debates (in the House of Commons and the House of Lords) about the Scheme has been particularly useful for identifying statements made about the manifesto commitments of the Labour Party or the likely costs of the Scheme.

Despite the fact that the Scheme was a public one, funded by the taxpayer, the amount of detail that was freely published was frustratingly limited and we discuss the implications of this for the democratic oversight of the Scheme in Chapter 10. We were, however, able to work with key Parliamentarians. As a result of detailed briefings about how we understood the Scheme was intended to operate, they were able to pose Parliamentary Questions that sought to obtain detailed Written Answers about key aspects of the Scheme. In addition, some useful information about the Scheme was (eventually) released under Freedom of Information (FOIA) legislation although more often the government would refuse to disclose documents under FOIA because, the government argued, the documents were outside the scope of the Act.

Our special role in relation to the proposals meant that we were invited to participate in many public and private events associated with the Scheme. Numerous reports were issued from such events and they were also added to the corpus of materials gathered about the Scheme.

For those events that we were unable to attend, friends and colleagues sent us notes and summaries. They also directed us to blogs and websites we may not have seen as well as less traditional data sources (for example, on-line copies of planning applications for IPS enrolment centers that included details for “panic rooms”).

A significant feature of the data collection process was the many informal conversations we had with key individuals associated with the Scheme. These would take place in the coffee breaks at conferences and events or in the bar after work. In each case, we were able to gain a better understanding of what these players felt were the most important issues at that time.

It should now be clear that we did not resort to the traditional interview process. In part this is because it would have been an unwelcome encumbrance to the nature of our relationships with the key actors and institutions in this domain. That is, those relationships involved high-intensity discussions about the latest issues about the Scheme, so stopping and taking notes and pausing to develop a structure to the discussion would have been burdensome and possibly would have interfered with the engagement.

Another significant reason why we did not use interviewing techniques is that we did not believe that they would bring more valid knowledge to this domain. We were certainly well positioned to meet with some of the high-level actors in this policy process, on all sides of the debate, including policy-makers and senior civil servants, ministers, and key politicians. We did not believe that an interview setting would result in these individuals divulging any information to us that was not being put into the public domain or released in private meetings. To put it simply, we were not arrogant enough to believe that our interviewing techniques would have resulted in ministers or senior civil servants disclosing to us what they did not already disclose to journalists, industry, or in Parliament. It is also not the role of academics to come out with "breaking news" of this manner; that is truly the task of journalists. Instead we relied on the information that was made available through the policy-making process.

There is one interesting exception to this, however. In all the time that we were involved in this policy area, only once were we taken aback by some of the information that was disclosed to us directly. We were invited, based on our own background work, to debate the Minister in a House of Lords committee room in November 2005. In that debate, attended by peers and key interested parties, while responding to a pointed question from our team, the Minister stated that the estimated costs for the Scheme were the costs to the Home Office agency that would administer the Scheme, not to the other Home Office divisions, let alone the rest of government. This was a significant output of that meeting, and everyone in that room was there to witness that statement, and our insistence that the Minister repeat himself. He contended that this was all covered in the (then) recent KPMG review of the Cost Methodology, which he then refused to make public. The point here is that by convening such meetings for wider participation, rather than relying on the interview setting, we still were able to get additional information but also let it become immediately part of the fabric of the policy deliberation process. The implications of the disclosure are discussed in more detail in Chapter 7.

Interestingly, some key documents about the Scheme have not (yet) been released. Whilst they may not have been released to us, we are a little surprised that they have not found their way into the public domain at all. For example, the KPMG report has been released only in summary form.

Data analysis

The data analysis process took a variety of forms depending on the timescales that were involved. For example, in the early days we were being frequently asked to provide independent academic analysis of government announcements. In many cases these would be for national news programs on the same day as the announcement was made. In these cases, as noted above, we had to read the documents and pick up on the key elements of what was being announced. Moreover, we had to explain these issues in a way that made sense to the lay public, which was by no means a simple task, nor did we achieve this with great splendor. On other occasions, we needed to explain the issues and their implications to journalists in the form of background briefings, so that they could form their own opinions and decide who they needed to interview next to write their "story."

Slightly longer timescales related to submissions to Parliamentary enquiries about the Scheme, such as those undertaken by the Science and Technology Select Committee or the Home Affairs Committee. In these cases, although the deliverable is not in the form of an academic paper, much of the same preparation is undertaken, in terms of identifying the points that the submission is likely to include and then working backwards to identify the data about those points. Preparing to give oral evidence to a Committee requires further data analysis to be undertaken.

Similar analysis was undertaken to address specific questions posed to us by Parliamentarians and journalists, for example, about the claim that the Register would not be attached to the internet. Developing an understanding of this point drew on both the archive of Written Answers and the archive of the Parliamentary debate.

Other issues for this kind of analysis were raised by the six-monthly s.37 cost reports and much of the preparation of the responses to the cost reports was undertaken with an expectation that the material could be developed for academic publication (see, for example, the materials in Chapters 3, 4, and 9).

Finally, as our work began to reflect on the broader, less time-critical aspects of the Scheme, as the reports about the Scheme became more detailed (for example, the draft secondary legislation) and as we began writing for more traditional academic audiences, we began to use more formal qualitative analysis tools in parallel with our perspectives on the documents. For example, Atlas TI software was used to code and analyze the statements made in the various documents, helping both with cross-checking of themes and to develop higher-level concepts.

Reflection and feedback

Throughout this process, our work benefited from various forms of reflection and feedback. When we spoke with the media, we better appreciated the concerns of ordinary citizens rather than just academics, just as we did when speaking with Parliamentarians. We actively sought out audiences who would challenge our perspectives, presenting our work to skeptical as well as friendly audiences. When our assumptions and understandings were challenged by these audiences, we would frequently squirm (at least internally) and use these challenges to develop our thinking further.

Presenting our work to industry audiences made us appreciate which technological concerns were most pressing and which could be addressed with existing technologies. Similarly, when we presented our work to academic audiences we were frequently told about other research approaches and authors that could develop help us develop our work further.

Although most of the people we met with shared our concerns that the Scheme needed greater scrutiny we never took the position of assuming that “we were right.” Instead, we reflected on whether we were just going to a self-selected sample of meetings. In periods of introspection we questioned whether we had missed important aspects of the Scheme and would suddenly appear foolish, our academic credibility in tatters. This meant that we often stood back and asked ourselves if we were conducting ourselves in accordance with (unwritten) academic principles and whether we were choosing our issues and “battles” with sufficient care. It certainly helped to know that if we made an error in judgment some institutions and actors would certainly respond with vigor.

Glossary

Authentication	The act of establishing or confirming that claims made by or about a person or entity are true. Not to be confused with identification.
Biographical enrolment	Enrolment onto an identity scheme by checking a person's "biographical footprint" (e.g. name, date of birth, and address) against information held in other databases such as National Insurance or driving license records or third party, commercial databases.
Biometric enrolment	Enrolment onto an identity scheme by recording biometrics (unique physical or behavioral characteristics, such as your fingerprints).
Cryptography	The practice of keeping information secret by applying mathematical techniques to convert a plain text into something unintelligible. Undoing this encryption typically requires access to a "key."
Digital certificates	An electronic document which uses a digital signature to bind a public key with an identity. The certificate can be used to verify that a public key belongs to particular individual or entity.
Digital signatures	A cryptographic method that gives the receiver of a "digitally signed" message confidence that the message was sent by the claimed sender.
Enrolment	The mechanism by which an individual joins an identity scheme. This can involve biographical and/or biometric enrolment. For some situations, this may also involve the "vetting" of the individual. In high-integrity environments, enrolment may be considered to be "identity proofing."
Failure to acquire rate	In biometric systems the rate where the submitted biometric is too poor for the system to make a reliable decision.

False match rate	In biometric systems the probability that a person's biometric matches the enrolment template of another person.
False nonmatch rate	In biometric systems the probability that a person's biometric fails to match their own enrolment template.
Identification	A process whereby someone's identity is revealed. Not to be confused with authentication.
Identity assurance	A consumer-led concept in which people prove who they are to others, be they retailers, financial institutions, domestic or foreign governments etc.
Identity management	An organization-led concept which is intended to benefit the organizational holder of information.
Mediated assertions	Identity and authentication assertions made indirectly, for example over the internet.
One-to-many match	In the context of biometrics, comparing a presented biometric with all biometrics held.
One-to-one match	In the context of biometrics, comparing a presented biometric with the biometric held on, for example, a presented identity card.
PKI	A public key infrastructure is the set of hardware, software, people, policies, and procedures that are needed to create, manage, store, distribute, and revoke digital certificates.
Remote authentication	Providing authentication services (for example, this person is authorized to access the network) remotely, such as over the internet.
Sector-specific identification number	Identification numbers whose use is limited to a specific sector, such as health. Other sectors, such as education, have their own (distinct) identification numbers for the same individuals
Technologically-Leveraged Policy (TLP)	Police that make innovative use of the capabilities of information and communications technologies.

Technologically-Leveraged Identity Policy (TLIP) Identity policies that make innovative use of the capabilities of information and communications technologies.

Unique national identification numbers The opposite of sector-specific identification numbers, where the same number is used throughout the society to identify a particular individual.

References

All URLs were verified 1 May 2009

ACLU (2009) Anti-REAL ID Legislation in the States. Retrieved from http://www.realnightmare.org/news/105/

Adams C (2005) Ministers deny ID cards will carry a high price *Financial Times* (30 May). Archived at http://www.ft.com/cms/s/0/5e3774e4-d0a6-11d9-abb8-00000e2511c8.html

Agar J (2005) Identity cards in Britain: Past experience and policy implications History and Policy. Archived at http://www.historyandpolicy.org/papers/policy-paper-33.html

Alvarez JE (2002) The new treaty makers. *Boston College International and Comparative Law Review* 25(2), 213–234.

Alvesson M (1993) Organizations as rhetoric: Knowledge-intensive firms and the struggle with ambiguity. *Journal of Management Studies* 30(6), 997–1015.

Alvesson M and Skoldberg K (2000) *Reflexive methodology: Interpretation and research.* Sage, London.

American Immigration Lawyers Association (2005) Summary and Selected Analysis of Provisions (27 January). Archived at http://www.aila.org/content/default.aspx?docid=18678

Amoore L (2008) Governing by identity. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 21–36, Routledge, London.

Angell IO (2005) Letter to Andy Burnham (10 November). Archived at http://ips.gov.uk/identity/downloads/letter-to-burnham.pdf

Anonymous (2004) Aanwijzing uitbreiding identificatieplicht (7 December). Archived at http://www.om.nl/organisatie/beleidsregels/overzicht/openbare_orde/@108095/aanwijzing/

Anonymous (2005) Project de carte nationale d'identite electronique', un rapport part Le Forum des droits sur l'internet' (16 June). Archived at http://www.foruminternet.org/telechargement/documents/rapp-cnie-20050616.pdf

Anonymous (n.d.) Liveness Detection in Biometric Systems. Archived at http://www.biometricsinfo.org/whitepaper1.htm

Arnold B (2007) Australia Card. Archived at http://www.caslon.com.au/australiacardprofile.htm

Arnott S (2005) Experts say ID cards timetable needs rethink *IT Week* (15 June). Archived at http://www.computing.co.uk/computing/news/2138041/experts-say-id-cards-timetable-needs-rethink

Arora S (2008) National e-ID card schemes: A European overview. *Information security technical report* 13(2), 46–53.

Atkins (2009) Citizen Information Project: Technical consultancy for feasibility study and project definition stages. Archived at http://www.eurim.org.uk/activities/pi/data_sharing_case_studies/dscs6_atkins.pdf

Aus JP (2006) Decision-making under pressure: The negotiation of the biometric passports regulation in the council Arena (September) Working Paper 11. Archived at http://www.arena.uio.no/publications/working-papers2006/papers/wp06_11.xml

Australian Financial Review (1987) The genuine problems with The Australia Card (28 August). Archived at http://www.afr.com/home/viewer.aspx?ATL://afnr000020011118dj8s00awj&section=search&title=The+Genuine+Problems+With+The+Australia+Card+

Avgerou C and McGrath K (2007) Power, rationality and the art of living through socio-technical change. *MIS Quarterly* 31(2), 295–315.

Avoine G, Kalach K and Quisquater J-J (2007) Belgian Biometric Passport does not get a pass ... Your personal data are in danger! UCL Crypto Group, Louvain-la-Neuve, Belgium (17 August). Archived at http://www.dice.ucl.ac.be/crypto/passport/index.html

BahaiRights.org (2008) Department of Civil Status leads discrimination against Baha'is (15 July). Archived at http://www.bahairights.org/2008/07/15/department-of-civil-status-leads-discrimination-against-bahais/

Bailey SGM and Caidi N (2005) How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of Information Science* 31(5), 354–364.

Balaban D (2003) Fingerprints missing from Chinese National ID card. *Card Technology* (11 September) Archived at http://www.cardtechnology.com/article.html?id=20050509OMOJ6P68

Balaban D (2004) The Middle East leads the way in National ID cards. *Card Technology* (20 March). Archived at http://www.cardtechnology.com/article.html?id=200505092C0D2IBF

Bara J (2005) A question of trust: Implementing party manifestos. *Parliamentary Affairs* 58(3), 585–599.

Barnes B, Bloor D and Henry J (1996) *Scientific knowledge: A sociological analysis.* Athlone, London.

Barry A (2001) *Political machines: Governing a technological society.* Athlone, London.

Barzelay M (1992) *Breaking through bureaucracy: New vision for managing in government.* University of California Press, Berkeley.

Baskerville R (1999) Investigating information systems with action research. *Communications of the AIS* 2(19), 1–31.

Bassellier G, Benbasat I and Reich BH (2003) The influence of business managers' IT competence on championing IT. *Information Systems Research* 14(4), 317–336.

Bauchspies WK, Croissant J and Restivo S (2006) *Science, technology, and society: A sociological approach.* Blackwell, Oxford.

Bauer A (2005) Audition 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 (12 April). Archived at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CRAUDITIONPIAZZA.pdf

Bayley P (2004) Introduction: The whys and wherefores of analysing parliamentary discourse. In *Cross-cultural perspectives on Parliamentary discourse* (Bayley P, Ed), pp 1–44, John Benjamins, Amsterdam.

BBC News (2005a) £300 price tag on ID cards "mad" *BBC* (16 June). Archived at http://news.bbc.co.uk/1/hi/uk_politics/4099356.stm

BBC News (2005b) ID cards scheme "may cost £18bn" *BBC* (29 May). Archived at http://news.bbc.co.uk/1/hi/uk_politics/4590817.stm

BBC News (2006a) EU driving licence coming in 2013 *BBC* (14 December). Archived at http://news.bbc.co.uk/1/hi/world/europe/6180617.stm

BBC News (2006b) Web inventor fears for the future *BBC* (2 November). Archived at http://news.bbc.co.uk/1/hi/technology/6108578.stm

BBC News (2007a) Clarkson stung after bank prank *BBC* (7 January). Archived at http://news.bbc.co.uk/1/hi/entertainment/7174760.stm

BBC News (2007b) Crime record backlog "a failure" *BBC* (2 March). Archived at http://news.bbc.co.uk/1/hi/uk/6411647.stm

BBC News (2008a) ID card fingerprint errors fear *BBC* (3 July). Archived at http://news.bbc.co.uk/1/hi/uk_politics/7484853.stm

BBC News (2008b) MoD "Facebook generation" warning *BBC* (25 June). Archived at http://news.bbc.co.uk/1/hi/uk_politics/7473818.stm

BBC News (2009a) Absent parents may lose passports *BBC* (27 January). Archived at http://news.bbc.co.uk/1/hi/uk_politics/7852640.stm

BBC News (2009b) ID cards "could use chip-and-pin" *BBC* (7 April). Archived at http://news.bbc.co.uk/1/hi/uk/7986618.stm

Benjamin R, De Long D and Scott-Morton M (1990) Electronic data interchange: How much competitive advantage? *Long Range Planning* 23(1), 29–40.

Berger P and Luckmann T (1966) *The social construction of reality.* Penguin, London.

Berghel H (2000) Identity theft, social security numbers and the Web. *Communications of the ACM* 43(2), 17–21.

Berghel H (2006) Fungible credentials and next-generation fraud. *Communications of the ACM* 49(12), 15–19.

Best J (2003) Chinese ID cards to carry genetic sample *Silicon.com* (2 September). Archived at http://management.silicon.com/government/0,39024677,10005834,00.htm

Bevir M, Rhodes RAW and Weller P (2003) Traditions of governance: Interpreting the changing role of the public sector. *Public administration* 81(1), 1–17.

Beynon-Davies P (1995) Information systems "failure": The case of the London Ambulance Service's Computer Aided Dispatch Systems. *European Journal of Information Systems* 4(3), 171–184.

Bijker WE, Hughes TP and Pinch T (Eds) (1987) *The social construction of technological systems: New directions in the sociology and history of technology,* The MIT Press, Cambridge, MA.

Billings H (2005) MEPs back EU driving permit (23 February). Archived at http://www.theparliament.com/no_cache/inside-parliament/inside-parliament-article/newsarticle/meps-back-eu-driving-permit/

Binder R and Gill M (2005) Identity theft and fraud: Learning from the USA Perpetuity Research & Consultancy International (PRCI) Ltd. Archived at http://www.perpetuityresearch.com/publications.html#idtheftusa

Biometrics Assurance Group (2008) Annual Report 2007. Archived at http://ips.gov.uk/identity/downloads/FINAL-BAG-annual-report-2007-v1_0.pdf

Birch DGW (2009a) I can see an article of some sort. Anyone called David? (14 April). Archived at http://digitaldebateblogs.typepad.com/digital_identity/2009/04/i-can-see-an-article-of-some-sort-anyone-called-david.html

Birch DGW (2009b) Psychic ID: A blueprint for a modern national identity scheme Identity in the Information Society Open Access Journal. Archived at http://dx.doi.org/10.1007/s12394–009-0014–6

Blair T (2005) Prime Minister's Press Conference (27 June). Archived at http://www.number10.gov.uk/output/Page7728.asp

Blair T (2006) We need ID cards to secure our borders and ease modern life *The Daily Telegraph* (6 November 2006). Archived at http://www.telegraph.co.uk/comment/personal-view/3633979/We-need-ID-cards-to-secure-our-borders-and-ease-modern-life.html

Blair T (2007) PM's response to ID cards petition (19 February). Archived at http://www.number10.gov.uk/output/Page10987.asp

Boland RJ (1983) The in-formation of information systems. In *Critical issues in information systems research* (Boland RJ and Hirschheim RA, Eds), pp 363–379, John Wiley and sons, Chichester.

Boland RJ (1991) Information system use as a hermeneutic process. In *Information systems research: Contemporary approaches and emergent traditions* (Nissen H-E, Klein HK and Hirschheim R, Eds), pp 439–458, North-Holland, Copenhagen, Denmark.

Boltanski L and Thevenot L (2006 [1991]) *On justification: Economies of worth.* Princeton University Press, Princeton.

Bowker GC and Star SL (1999) *Sorting things out: Classification and its consequences.* The MIT Press, Cambridge, MA.

Brands SA (2000) *Rethinking public key infrastructures and digital certificates: building in privacy.* The MIT Press, Cambridge, MA.

Breckenridge K (2008) The elusive panopticon: The HANIS project and the politics of standards in South Africa. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 39–56, Routledge, London.

British Telecommunications PLC (2004) Memorandum submitted by British Telecommunications plc to the Select Committee on Home Affairs (January). Archived at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we04.htm

Broache A (2006) Google CEO: Techies must educate governments *ZDNet* (17 October). Archived at http://news.zdnet.com/2100-9588_22-149929.html

Brown CL (2008) China's second generation national identity card: Merging culture, industry and technology. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 57–74, Routledge, London.

Brown G (2006) Chancellor appoints Sir James Crosby to lead Public Private Forum on Identity (11 July). Archived at http://www.hm-treasury.gov.uk/press_51_06.htm

Brown JS and Duguid P (2002) *The social life of information.* Harvard University Press, Boston.

Burnham A (2005) Letter from Andy Burnham to Professor Ian Angell (23 November). Archived at http://ips.gov.uk/identity/downloads/letter-to-burnham.pdf

Burnham A (2006) Identity cards: Briefing letter to Members of the Parliamentary Labour Party (7 February).

Byrne L (2007) Securing our identity: A 21st century public good. Archived at http://ips.gov.uk/identity/downloads/Liam-Byrne-MP-Chatham-House-Speech-19-Jun-07.pdf

Cabinet Office (1999) Modernising government Cm4310. Archived at http://archive.cabinetoffice.gov.uk/moderngov/download/modgov.pdf

Cabinet Office (2002) Identity fraud: A Study. Archived at http://ips.gov.uk/identity/downloads/id-fraud-report.pdf

Cabinet Office (2005) Transformational government: Enabled by technology Cm6683. Archived at http://www.cabinetoffice.gov.uk/media/141734/transgov-strategy.pdf

Cabinet Office (2006) Identity risk management for e-government services. Archived at http://webarchive.nationalarchives.gov.uk/0070603164510/http://www.cabinetoffice.gov.uk/csia/~/media/assets/www.cabinetoffice.gov.uk/csia/id_risk_mgt061127%20pdf.ashx

Cabinet Office (2008a) Cross government actions: Mandatory minimum issues (25 June). Archived at http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf

Cabinet Office (2008b) Data handling procedures in government: Final Report (25 June). Archived at http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/dhr080625.pdf

Callon M (1986) Some elements of a sociology of translation: Domestication of the scallops and the fishermen of St Brieuc Bay. In *Power, action and belief: A new sociology of knowledge?* (Law J, Ed), pp 196–233, Routledge & Kegan Paul, London.

Callon M (1998) An essay on framing and overflowing: economic externalities revisited by sociology. In *The laws of the markets* (Callon M, Ed), pp 244–269, Blackwell, Oxford.

Cameron D (2004) Mistaken identity: A public meeting on the Government's proposed National Identity Card (19 May). Archived at http://www.no2id.net/MistakenIdentity/Mistaken_Identity_05.mp3

Cameron D (2009) News Review interview: David Cameron *The Times* (26 April). Archived at http://www.timesonline.co.uk/tol/news/politics/article6168263.ece

Caminer D, Aris J, Hermon P and Land F (1998) *LEO – The Incredible Story of the World's First Business Computer.* McGraw Hill, New York.

CardTechnology.com (2004) Japan's national ID card falls flat *CardTechnology.com* (8 October). Archived at http://www.cardtechnology.com/article.html?id=200505098OKFPKUN

Carr NG (2003) IT doesn't matter. *Harvard Business Review* 81(5), 41–49.

Carr S (2009) NDP mulls abolishing religious affiliation field in ID cards *Daily News Egypt* (25 March). Archived at http://voiceofthecopts.org/en/articles/ndp_mulls_abolishing_religious_affiliation_field_in_id_cards.html

Cash JI and Konsynski B (1985) IS redraws competitive boundaries. *Harvard Business Review* 63(2), 134–142.

Castells M (1996) *Rise of the network society.* Blackwell, Oxford.

CBC Online (2003) National ID cards slammed at immigration hearing *CBC Online* (11 February). Archived at http://www.cbc.ca/canada/story/2003/02/11/idcard_rxn030211.html

Chalmers M (2004) Hermeneutics, information and representation. *European Journal of Information Systems* 13(3), 210–220.

Chen DW (2003) China readies super ID card, a Worry to Some *The New York Times* (19 August). Archived at http://www.nytimes.com/2003/08/19/world/china-readies-super-id-card-a-worry-to-some.html?sec=technology&&fta=y

China Post News (2008) Over 700,000 fingerprints files of Taipei citizens destroyed *China Post News* (10 August). Archived at http://www.chinapost.com.tw/taiwan/national/national-news/2008/08/10/169382/Over-700000.htm

Chinaview (2008) China opens website for public verification of ID cards *Chinaview* (7 November). Archived at http://news.xinhuanet.com/english/2008-11/07/content_10324062.htm

Ciborra C (1991) From thinking to tinkering: The grassroots of strategic information systems. In *Proceedings of the 12th International Conference on Information Systems*, pp 283–291, New York.

Ciborra C and associates (2000) *From control to drift: The dynamics of corporate information infrastructures.* Oxford University Press, Oxford.

Citizen Information Project Board (2005) Minutes of meeting (18 March). Archived at http://www.gro.gov.uk/cip/Download.asp?CIPPB(05)Minute03_tcm95-26255.pdf

Clark C (2003) Coderre pushes Ottawa to adopt national ID cards *Globe and Mail* (7 February). Archived at http://www.theglobeandmail.com/servlet/ArticleNews/PEstory/TGAM/20030207/UCARDN/national/national/national_temp/5/5/26/

Clarke C (2005) Interview on today programme about July 7 attacks, BBC Radio 4 *The Guardian* (8 July). Archived at http://www.guardian.co.uk/uk/2005/jul/08/politics.terrorism

Clarke R (1987) Just another piece of plastic for your wallet: The "Australia Card" Scheme. Archived at http://www.rogerclarke.com/DV/OzCard.html

Clarke R (1992) The resistable rise of the national personal data system. *Software Law Journal* 29(1), 29–59.

Collingridge D (1992) *The management of scale.* Routledge, London.

Collings T (2008) Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). *Information Security Technical Report* 13(2), 61–70.

Collins H and Evans R (2007) *Rethinking expertise.* University of Chicago Press, Chicago.

Collins H and Kusch M (1998) *The shape of actions: What humans and machines can do.* The MIT Press, Cambridge, MA.

Collins H and Pinch T (1998a) *The Golem at large: What you should know about technology.* Cambridge University Press, Cambridge.

Collins H and Pinch T (1998b) *The Golem: What you should know about science.* Canto, Cambridge.

Collins HM (1981) Stages in the empirical programme of relativism. *Social Studies of Science* 11(1), 3–10.

Collins HM (1992) *Changing order: Replication and induction in scientific practice.* University of Chicago Press, Chicago.

Collins HM, Green RH and Draper RC (1985) Where's the expertise? Expert systems as a medium of knowledge transfer. In *ExpertSystems85* (Merry M, Ed), pp 323–334, Cambridge University Press, Cambridge.

Collins T (2009a) Are passport fees paying for ID cards? *Computer Weekly* (8 April). Archived at http://www.computerweekly.com/Articles/2009/04/08/235570/are-passport-fees-paying-for-id-cards.htm

Collins T (2009b) ID cards: the technology behind the ID card contracts *Computer Weekly* (7 April). Archived at http://www.computerweekly.com/Articles/2009/04/07/235561/id-cards-the-technology-behind-the-id-card-contracts.htm

Communication from the Commission (2005) The Hague Programme: Ten priorities for the next five years. A partnership for European renewal 4. Schengen reaches adulthood (10 May) COM(2005)184final. Archived at http://ec.europa.eu/justice_home/news/information_dossiers/the_hague_priorities/doc/04_schengen_en.pdf

Congress Daily (2009) TSA cites progress enrolling port workers in ID card program (9 March). Archived at http://www.govexec.com/dailyfed/0309/030909cdpm1.htm

Constitution Committee (2009) Surveillance: Citizens and state (6 February). Archived at http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf

Coulter J (1985) On comprehension and "mental representation." In *Social action and artificial intelligence: Surrey conference on sociological* *theory and method; 3* (Gilbert GN and Heath C, Eds), pp 8–23, Gower Publishing, Aldershot.

Council of the European Union (2004) The Hague Programme: Strengthening freedom, security and justice in the European Union. Archived at http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_en.pdf

Council Regulation (EC) (2000) 2000/365/EC concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis (29 May). Archived at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0365:EN:HTML

Council Regulation (EC) (2004) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (13 December). Archived at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:HTML

Crace J (2005) Simon Davies: In a spin *The Guardian* (5 July). Archived at http://www.guardian.co.uk/politics/2005/jul/05/interviews.highereducationprofile

Craig D and Brooks R (2006) *Plundering the public sector: How New Labour are letting consultants run off with £70 billion of our money.* Constable, London.

Sir James Crosby (2008) Challenges and opportunities in identity assurance (6 March). Archived at http://www.hm-treasury.gov.uk/d/identity_assurance060308.pdf

Daily Telegraph (2005) Time has come for ID cards, says Blair *The Daily Telegraph* (28 June). Archived at http://www.telegraph.co.uk/news/1492875/Time-has-come-for-ID-cards-says-Blair.html

Darking ML and Whitley EA (2007) Towards an Understanding of FLOSS: Infrastructures, Materiality and the Digital Business Ecosystem. *Science Studies* 20(2), 13–33.

Davenport S and Leitch S (2005) Circuits of power in practice: Strategic ambiguity as delegation of authority. *Organization Studies* 26(11), 1603–1623.

Davenport TH (1993) *Process innovation: Reengineering work through information technology.* Harvard Business School Press, Boston, MA.

Davies H (2006) Letter to the Prime Minister (20 January). Archived at http://identityproject.lse.ac.uk/daviestoblair.pdf

Davies S (2004) The loose cannon: An overview of campaigns of opposition to National Identity Card proposals. Archived at http://www.privacy.org.au/About/Davies0402.html

De Cock D, Simoens K and Preneel B (2008) Insights on identity documents based on the Belgian case study. *Information security technical report* 13(2), 54–60.

Decree (1986) Decree with the Force of Law No. 10 of 1986.

Decree (2000) Ministerial Decree 116 (19 July). Archived at http://www.cnipa.gov.it/site/_files/ci_Decreto%20del%20MInistro%20Interno%20del%2019%20luglio%202000_c.pdf

Décret n°55-1397 (1955) du 22 octobre 1955 : Décret instituant la carte nationale d'identité. Archived at http://www.legifrance.gouv.fr/texteconsolide/PQHEU.htm

Décret n°87-178 (1987) 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*, 3174–3175.

Department of Homeland Security (2003) Notice allowing ENFORCE/IDENT to collect biometric and biographic data in support of US-VISIT (12 December). Archived at http://edocket.access.gpo.gov/2003/03-30762.htm

Department of Homeland Security (2008) Minimum standards for drivers licenses and identification cards acceptable by federal agencies for official purposes: Final rule (29 January). Archived at http://edocket.access.gpo.gov/2008/08–140.htm

Department of State (2005) Press release: DHS to require digital photos in passports for visa waiver Travelers (15 June). Archived at http://www.state.gov/r/pa/prs/ps/2005/47984.htm

De Volkskrant (2005) Identificatieklucht De Volkskrant (15 January) at http://www.volkskrant.nl/.

Doward J (2005) ID cards to cost £300 per person *The Observer* (29 May). Archived at http://www.guardian.co.uk/politics/2005/may/29/idcards.immigrationpolicy

Drezner DW (2001) On the balance between international law and democratic sovereignty. *Chicago Journal of International Law* 2(2), 321–336.

Duguid P (2005) "The art of knowing": Social and tacit dimensions of knowledge and the limits of the community of practice. *The information society* 21(2), 109–118.

Dunleavy P (2005) Written evidence to the Public Administration Select Committee (24 November). Archived at http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDCard_Nov05WrittenEvidence.pdf

Dunleavy P, Margetts H, Bastow S and Tinkler J (2006) *Digital era governance: IT corporations, the state and e-government.* Oxford University Press, Oxford.

DWP (2007) Home Office working assumptions. Archived at http://www.dwp.gov.uk/foi/2007/apr/assumptions-040407.pdf

Earl MJ (1993) Experiences in strategic information systems planning. *MIS Quarterly* 17(1), 1–24.

EDRIGram (2005) 3.300 ID fines in the Netherlands in 1 month *EDRI* (9 February). Archived at http://www.edri.org/edrigram/number3.3/ID

Edwardes CA, Hosein IR and Whitley EA (2007) Balance, scrutiny and identity cards in the UK. *Criminal Justice Matters* 68(Summer), 29–30.

eGovernment news (2003) Biometric checks illegal in Greece, says Data Protection Authority *eGovernment News* (11 November). Archived at http://www.epractice.eu/en/news/283820

eGovernment news (2004a) Introduction of biometric ID cards and passports to cost up to EUR 700m in Germany *eGovernment News* (18 November). Archived at http://istrg.som.surrey.ac.uk/projects/guide/files/Introduction_of_biometric_ID_cards_and_passports_to_cost_up_to_EUR_700m_in_Germany_2004_11_18.pdf

eGovernment news (2004b) Introduction of Spanish electronic ID cards delayed *eGovernment News* (10 December). Archived at http://ec.europa.eu/idabc/servlets/Doc?id=21699

eGovernment news (2004c) Italy to start distribution of e-government services cards' *eGovernment News* (12 May). Archived at http://ec.europa.eu/idabc/servlets/Doc?id=21725

eGovernment news (2004d) Spanish Government officially launches electronic ID cards *eGovernment News* (16 February). Archived at http://europa.eu.int/idabc/en/document/2154/343

eHealth Europe (2008) German ID card to allow pseudonyms (27 February). Archived at http://ehealtheurope.net/news/3505/german_id_rd_to_allow_pseudonyms

Eisenberg EM (1984) Ambiguity as strategy in organizational communication. *Communication Monographs* 51(3), 227–242.

Eisenberg EM and Witten MG (1987) Reconsidering openness in organizational communication. *Academy of Management Review* 12(3), 418–426.

Elliot R (2006) An early experiment in national identity cards: The battle over registration in the First World War. *Twentieth Century British History* 17(2), 145–176.

Elliott L (2003) ID card plan to top $7 billion *Calgary Sun* (7 October). Archived at http://ca.groups.yahoo.com/group/activist-newsmuse/message/1247

Engbarth D (2005a) Grand justices suspend fingerprinting program *Taiwan news* (11 June).

Engbarth D (2005b) Premier promises to abide by justices' ruling on fingerprints *Taiwan news* (26 May).

Engbarth D (2005c) Vice President takes fight over prints to print *Taiwan news* (24 May).

ENISA (2009) Privacy features of European eID Card specifications (2 February). Archived at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_features_eID.pdf

Enterprise Privacy Group (2008) Report on the National Identity Scheme Consultation Event Belfast 2 October 2008 Identity and Passport Service (16 October). Archived at http://www.privacygroup.org/downloads/fl0000223.pdf

EPIC and Privacy International (2004) Privacy and human rights 2004. Archived at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347–542782& als[theme]=Privacy%20and%20Human%20Rights%20 2004

Espiner T (2006) Chris Patten: Politicians have no grasp of technology *ZDNet* (26 October). Archived at http://news.zdnet.co.uk/security/0,1000000189,39284350,00.htm

Espiner T (2008) India takes step on ID Card road *ZDNet* (11 November). Archived at http://community.zdnet.co.uk/blog/0,1000000567,10009721o-2000331828b,00.htm

Estonia Citizenship and Migration Board (2009) About the ID card. Retrieved from http://www.pass.ee/index.php/pass/eng/id_card

European Commission of Justice and Home Affairs (2009) Making EU visa and residence documents more secure. Archived at http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm

Expatica (2004) Price hike for Belgium's e-ID cards (26 July). Archived at http://dev.expatica.com/be/articles/news/price-hike-for-belgiums-e-id-cards-9874.html

Ferry G (2003) *A computer called LEO: Lyons teashops and the World's first office computer.* Fourth Estate, London.

FIPR (2009) Database state: A report commissioned by the Joseph Rowntree Reform Trust Ltd (22 March). Archived at http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf

Fishenden J (2009) Towards the digITal state (16 April). Archived at http://ntouk.com/papers/towards%20the%20digITal%20state%20-%20V1.pdf

Foreign Affairs and Trade Canada (2003) The Canada–U.S. Smart Border Declaration: Action Plan for creating a secure and smart border the secure flow of people (7 February). Archived at http://www.dfait-maeci.gc.ca/anti-terrorism/actionplan-en.asp

Fountain JE (2001) *Building the virtual state: Information technology and institutional change.* The Brookings Institute, Washington, DC.

Freeman S (2005) Clarke attacks LSE over “£300 ID card” claim *The Times* (16 June). Archived at http://www.timesonline.co.uk/tol/news/uk/article533932.ece

French Government (2004) French e-government strategic plan. Archived at http://www.epractice.eu/files/media/media_282.pdf

Froomkin AM (2007) Creating a viral federal privacy standard. *Boston College Law Review* 55(1), 48.

Froomkin AM (2009) Identity cards and Identity romanticism. In *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (Kerr I, Ed), pp 245–263, Oxford University Press, Oxford.

Fuchs S (1992) *The professional quest for truth: A social theory of science and knowledge*. State University of New York Press, c, Albany.

Galliers RD (1991) Strategic information systems planning: Myths, reality and guidelines for successful implementation. *European Journal of Information Systems* 1(1), 55–64.

Gamson WA and Modigliani A (1989) Media discourse and public opinion on nuclear power: A constructionist approach. *American Journal of Sociology* 95(1), 1–37.

Garfinkel SL (1995) Risks of social security numbers. *Communications of the ACM* 38(10), 146.

Gates K (2008) The United States Real ID Act and the securitization of identity. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 218–232, Routledge, London.

General Register Office (2008) General Register Office transfers to Identity and Passport Service (1 April). Archived at http://www.gro.gov.uk/gro/content/news/general-register-office-transfers-to-identity-and-passport-service.asp

Georgia (2005) House Bill 577. Archived at http://www.legis.state.ga.us/legis/2005_06/pdf/hb577.pdf

Gibbons M, Limoges G, Nowotny H, Schwartzman S, Scott P and Trow M (1994) *The new production of knowledge: The dynamics of science and research in contemporary societies*. Sage, London.

Giroux H (2006) “It was such a handy term”: Management fashions and pragmatic ambiguity. *Journal of Management Studies* 43(6), 1227–1260.

Glass RL (2005) The first business application: A significant milestone in software history. *Communications of the ACM* 48(3), 25–26.

Goffman E (1990 [1959]) *The presentation of self in everyday life*. Penguin, London.

Goldstein J (1996) International law and domestic institutions: Reconciling North American "unfair" trade laws. *International Organization* 50(4), 541–564.

Government Accountability Office (2004) Homeland Security: Risks facing key Border and Transportation Security Program need to be addressed. Archived at http://www.gao.gov/new.items/d04569t.pdf

Government Accountability Office (2005) Homeland Security: Some progress made, but many challenges remain on U.S. Visitor and Immigrant Status Indicator Technology Program General Accounting Office GAO-05-202. Archived at http://www.gao.gov/new.items/d05202.pdf

Government Accountability Office (2007) Homeland Security needs to immediately address significant weaknesses in systems supporting the US-VISIT Program (July) GAO-07-870. Archived at http://www.gao.gov/new.items/d07870.pdf

Government Accountability Office (2008a) Limitations with Department of Homeland Security's plan to verify departure of foreign nationals (28 February). GAO-08-458T Archived at http://www.gao.gov/new.items/d08458t.pdf

Government Accountability Office (2008b) State Department: Comprehensive Strategy Needed to Improve Passport Operations (July). Archived at http://www.gao.gov/new.items/d08891.pdf

Graham P (1990) The Australia Card: A technology driven policy? Griffith University: Unpublished MPhil thesis.

Grant I (2008) Steria latest bidder to pull out of ID card project *Computer Weekly* (28 February). Archived at http://www.computerweekly.com/Articles/2008/02/28/229628/steria-latest-bidder-to-pull-out-of-id-card-project.htm

Greek Data Protection Authority (2000) Hellenic Republic Authority for the Protection of Personal Data report to the Ministry of Public Order and Ministry of Internal Affairs (15 May)

Greenleaf G (1987) The Australia Card – Towards a National Surveillance System. *Law Society Journal* 25(9), 24–30.

Greenleaf G (2002) Submission on the smart ID card and the Registration of Persons (Amendment) Bill 2001 University of Hong Kong Faculty of Law (28 October).

Greenleaf G (2007) Australia's proposed ID card: Still quacking like a duck. *Computer Law and Security Report* 23(2), 156–166.

Greenleaf G (2008) Hong Kong's "smart" ID card: Designed to be out of control. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 75–92, Routledge, London.

Gregor S (2006) The nature of theory in information systems. *MIS Quarterly* 30(3), 611–642.

Grint K and Woolgar S (1997) *The machine at work: Technology, work and organization.* Polity Press, Cambridge.

Guinto JF (2005) DILG chief pushes national ID system against terrorism *Philippine Daily Inquirer* (18 February).

Haas PM (1989) Do regimes matter? Epistemic communities and Mediterranean pollution control. *International Organization* 43(3), 377–403.

Habermas J (1970) *Toward a rational society: Student protest, science and politics.* Beacon press, Boston.

Habermas J (1984) *The theory of communicative action: Part 1: Reason and the rationalization of society.* Heinemann Education, London.

Habermas J (1987) *The theory of communicative action: Part 2: Lifeworld and system: a critique of functionalist reason.* Polity, Cambridge.

Hammer M (1990) Re-engineering work: Don't automate obliterate. *Harvard Business Review* 68(4), 104–112.

Hammer M and Champy J (1993) *Reengineering the corporation:a manifesto for business revolution.* Harper Business, New York.

Hanseth O, Monteiro E and Hatling M (1996) Developing Information Infrastructure: The Tension between Standardization and Flexibility. *Science, Technology, & Human Values* 21(4), 407–426.

Harrison D (2005) Alternative ID card costs ten times less than the government version *The Daily Telegraph* (5 June). Archived at http://www.telegraph.co.uk/news/uknews/1491412/Alternative-ID-card-costs-10-times-less-than-the-government-version.html

Hearing (1998) Blas F Ople petitioner vs Ruben D Toerres,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. Phillipines G R . No 127685

Heath N (2009) ID card "chip and PIN" proposal raises security fears *ZDNet* (16 April). Archived at http://news.zdnet.co.uk/security/0,1000000189,39640836,00.htm

Heath W (2008) Vorsprung durch Privatlebennotwendigkeitbewußtsein (27 February). Archived at http://www.idealgovernment.com/index.php/blog/comments/vorsprung_durch_privatlebennotwendigkeit bewusstsein/

Heise Online (2007) Social Democratic Party drops its objections to fingerprints in ID cards (10 October). Archived at http://www.heise.de/english/newsticker/news/97169

Hencke D and Dodd V (2006) Defence expert undermines Blair on safety of ID cards *The Guardian* (13 February 2006). Archived at http://www.guardian.co.uk/politics/2006/feb/13/idcards.immigrationpolicy

Hickley M (2008) British identity cards will be covered in EU symbols *Daily Mail* (26 September). Archived at http://www.dailymail.co.uk/news/article-1061761/British-identity-cards-covered-EU-symbols.html

Hillier M (2008) Letter to the editor: A modern means to confirm and protect identity *Financial Times* (22 February). Archived at http://www.ft.com/cms/s/0/409d0dfe-e0e8-11dc-b0d7-0000779fd2ac.html

Ho AT-K (2002) Reinventing local government and the e-government initiative. *Public administration review* 62(4), 434–444.

Holder D (2008) More than just a card: Intrusion, exclusion and suspect communities: implications in Northern Ireland of the British National Identity Scheme Northern Ireland Human Rights Commission (15 October). Archived at http://www.nihrc.org/dms/data/NIHRC/attachments/dd/files/104/More_than_just_a_card_FINAL.pdf

Holtfreter RE and Holtfreter K (2006) Gauging the effectiveness of U.S. identity theft legislation. *Journal of financial crime* 13(1), 56–64.

Home Affairs Committee (2004) Identity Cards: Fourth report of session 2003–04. Archived at http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130.pdf

Home Affairs Committee (2008) A surveillance society? (8 June). Archived athttp://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf

Home Office (2002) Entitlement Cards and Identity Fraud: A Consultation Paper CM 5557. Archived at http://www.homeoffice.gov.uk/documents/entitlement-cards?view=Binary

Home Office (2004) Regulatory Impact Assessment. Archived at http://www.homeoffice.gov.uk/documents/ria-identity-cards-bill-251104?view=Binary

Home Office (2005a) An assessment of awareness and demand for the Identity Cards Scheme (12 October). Archived at http://ips.gov.uk/identity/downloads/2005-10-12-Trade-Off-final-report.pdf

Home Office (2005b) Home Office response to The London School of Economics' ID Cards cost estimates & alternative blueprint. Archived at http://identityproject.lse.ac.uk/HomeOffice_ResponseTo_LSE_AlternativeBlueprint.pdf

Home Office (2005c) Identity cards briefing (May). Archived at http://ips.gov.uk/identity/downloads/Id-Cards-Briefing.pdf

Home Office (2005d) Identity Cards Scheme: Benefits overview. Archived at http://ips.gov.uk/identity/downloads/2005-06-27-Identity-Cards-Scheme-Benefits-Overview.pdf

Home Office (2005e) Regulatory Impact Assessment. Archived at http://ips.gov.uk/identity/downloads/Identity-cards-bill-regulatory-impact.pdf

Home Office (2006) Updated estimate of the cost of identity fraud to the UK Economy (2 February). Archived at http://ips.gov.uk/identity/downloads/FINAL-estimate-for-annual-cost-of-fraud-table-v1–2.pdf

Home Office (2008) New estimate of Cost of identity fraud to the UK economy (October). Archived at http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006–07.pdf

Home Office (2009) Benefits of ID cards for Manchester (29 January). Archived at http://press.homeoffice.gov.uk/press-releases/Benefits-ID-cards-manchester

Hood C (1996) Exploring variations in public management reforms of the 1980s. In *Civil service systems in comparative perspective* (Bekke HAGM, Perry JL and Toonen TAJ, Eds), Indiana University Press, Bloomington, IN.

Hosein IR (2004) The sources of laws: Policy dynamics in a digital and terrorized world. *The Information Society* 20(3), 187–199.

Hosein IR, Tsiavos P and Whitley EA (2003) Regulating architecture and architectures of regulation: contributions from information systems. *International Review of Computing Law and Technology* 17(1), 85–97.

House of Commons and House of Lords (2006) Conventions of the UK Parliament. Report of Session 2005–06 Joint committee on conventions: HL Paper 265-I/265-II HC 1212-I/1212-II. Archived at http://www.publications.parliament.uk/pa/jt200506/jtselect/jtconv/265/265.pdf and http://www.publications.parliament.uk/pa/jt200506/jtselect/jtconv/265/265ii.pdf

House of Lords (2008) Bills and how they become Law. Archived at http://www.parliament.uk/documents/upload/HofLBpBillsandhow.pdf

Houtekamer C and Verkade T (2008) Dutch plan single database for biometric data *NRC Handelsblad* (13 November). Archived at http://www.nrc.nl/international/Features/article2059482.ece/%20Dutch_plan_single_database_for_biometric_data

Huff SL, Maher PM and Munro MC (2006) Information technology and the board of directors: Is there an IT attention deficit? *MIS Quarterly Executive* 5(2), 1–14.

Hungarian Constitutional Court (1991) Decision on privacy rights Decision No.15-AB (13 April). Archived at http://www.uoou.cz/judik_hungarian_constitutional_court.pdf

IAAC (2009) Identity assurance concluding report Information Assurance Advisory Council (7 February). Archived at http://www.iaac.org.uk/Default.aspx?tabid=105

ICAO (2003) Technical advisory group on machine readable travel documents. Fourteenth meeting International Civil Aviation Organisation

(6–9 May). Archived at http://www2.icao.int/en/MRTD/Downloads/TAG-MRTD%20Reports/TAG-MRTD_14%20Report.pdf

ICAO (2004) Biometrics deployment of machine readable travel documents International Civil Aviation Organisation (21 May) ICAO TAG MRTD/NTWG. Archived at http://www.policylaundering.org/archives/ICAO/Biometrics_Deployment_Version_2.0.pdf

Identity Theft (2009a) Protect yourself. Retrieved from https://www.identitytheft.org.uk/protect-yourself.asp

Identity Theft (2009b) What if it happens to you? Retrieved from https://www.identitytheft.org.uk/what-if.asp

Ikenberry GJ (1996) The future of international leadership. *Political Science Quarterly* 111(3), 385–402.

InfoWorld (2005) U.S. Security expert sues Japanese government (25 January). Archived at http://www.keylogger.org/news-world/u-s-security-expert-sues-japanese-government-328.html

Introna LD (1997) *Management, information and power: A narrative of the involved manager.* Macmillan, Basingstoke.

Introna LD and Nussenbaum H (2009) Facial recognition technology: A survey of policy and implementation issues (April). Archived at http://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf

IPCC (2008) IPCC independent investigation report into loss of data relating to Child Benefit Independent Police Complaints Commission (25 June). Archived at http://www.ipcc.gov.uk/final_hmrc_report_25062008.pdf

Ives B and Learmonth GP (1984) The information system as a competitive weapon. *Communications of the ACM* 27(12), 1193–1201.

Johnston HR and Carrico SR (1988) Developing capabilities to use information strategically. *MIS Quarterly* 12(1), 37–48.

Johnston HR and Vitale MR (1988) Creating competitive advantages with inter-organizational information systems. *MIS Quarterly* 12(4), 153–165.

Johnston P (2007) 200 questions to get your passport *The Daily Telegraph* (22 March). Archived at http://www.telegraph.co.uk/news/uknews/1546211/200-questions-to-get-your-passport.html

Johnston P (2008) We'll be able to sign up for ID cards at Tesco *The Daily Telegraph* (12 May). Archived at http://www.telegraph.co.uk/comment/columnists/philipjohnston/3558253/Well-be-able-to-sign-up-for-ID-cards-at-Tesco.html

Joint Select Committee (1986) Towards fairness and equity: the Australia card program / submission by the Government of Australia to the Joint Select Committee on an Australia Card. Australian Government Publishing Service.

Jones M (2000) The moving finger: The use of social theory in WG 8.2 Conference Papers, 1975–1999. In *Organizational and social perspectives on information technology* (Baskerville R, Stage J and DeGross JI, Eds), pp 15–32, Kluwer, Aalborg, Denmark.

Jones R (2006) Identity crisis? What identity crisis *The Guardian* (11 November 2006). Archived at http://www.guardian.co.uk/money/2006/nov/11/insurance.moneysupplement

JUSTICE (2004) Information resource on identity cards (December). Archived at http://www.justice.org.uk/images/pdfs/idcardcc.pdf

Kabatoff M and Daugman J (2008) Pattern recognition: Biometrics, identity and the state – An interview with John Daugman. *Biosocieties* 3(1), 81–86.

Kallender P (2005) Japanese government, U.S. security expert meet in court *Computerworld* (27 January). Archived at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=99271

Karake-Shalhoub Z (2008) Population ID card systems in the Middle East: The case of the UAE. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 128–142, Routledge, London.

Keil M (1995) Pulling the plug: Software project management and the problem of project escalation. *MIS Quarterly* 19(4), 421–447.

Kent W (1978) *Data and reality: Basic assumptions in data processing reconsidered.* North-Holland, Amsterdam.

King WR (1978) Strategic planning for management information systems. *MIS Quarterly* 2(1), 27–37.

Kite M and Freinberg T (2004) Howard faces Tory rebellion over ID cards *The Daily Telegraph* (18 December). Archived at http://www.telegraph.co.uk/news/uknews/1479362/Howard-faces-Tory-rebellion-over-ID-cards.html

Klein HK and Myers MD (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly* 23(1), 67–94.

Knight W (2001) Malaysia pioneers smart cards with fingerprint data *New Scientist* (21 September). Archived at http://www.newscientist.com/article/dn1331-malaysia-pioneers-smart-cards-with-fingerprint-data.html

KPMG (2005) Cost methodology and cost review: Outline business case review: Published extract. Archived at http://ips.gov.uk/identity/downloads/2005-11-7-KPMG-Review-of-ID-Cards-Methodology.pdf

Kubosova L (2005) EU driving licence hammered out EUObserver (24 February). Archived at http://euobserver.com/?aid=18488

Lakoff G and Johnson M (1980) *Metaphors we live by*. University of Chicago Press, Chicago.

Lamb R and Kling R (2003) Reconceptualizing users as social actors in information systems research. *MIS Quarterly* 27(2), 197–235.

Latour B (1987) *Science in action: How to follow scientists and engineers through society*. Harvard University Press, Cambridge, MA.

Latour B (1999) *Pandora's hope: Essays on the reality of science studies*. Harvard University Press, Cambridge, MA.

Latour B (2004) *The politics of nature: How to bring the sciences into democracy*. Harvard University Press, Cambridge, MA.

Latour B (2005) *Reassembling the social: An introduction to Actor-Network-Theory*. Oxford University Press, Oxford.

Lee A (1994) Electronic mail as a medium for rich communication. *MIS Quarterly* 18(2), 143–157.

Lessig L (1999) *Code and other laws of cyberspace*. Basic Books, New York.

Lettice J (2006) "RFID tag" – the rude words ID card ministers won't say *The Register*. Archived at http://www.theregister.co.uk/2006/01/30/burnham_rfid_evasions/

Levi M and Burrows J (2008) Measuring the impact of fraud in the UK. *British journal of Criminology* 48(3), 298–318.

Libbenga J (2005) Belgians in cunning misspelt ID card plan *The Register* (26 May). Archived at http://www.theregister.co.uk/2005/05/26/belgian_id_card_plan/

Lichtblau E and Markoff J (2004) Accenture is awarded U.S. contract for borders *The New York Times*. Archived at http://www.nytimes.com/2004/06/02/business/accenture-is-awarded-us-contract-for-borders.html?sec=&spon=&pagewanted=all

Liebenau J and Backhouse J (1991) *Understanding information*. Macmillan, Basingstoke.

Lin W-c (2005) Wrong tack taken on ID card law *Taipei Times* (5 June). Archived at http://www.taipeitimes.com/News/editorials/archives/2005/06/05/2003258063

LSE Identity Project (2005a) *Interim Report*. Archived at http://identity project.lse.ac.uk/InterimReport.pdf

LSE Identity Project (2005b) LSE Team responds to Home Office's Criticisms of The Identity Project Report London School of Economics and Political Science (5 August). Archived at http://identityproject.lse.ac.uk/LSE_ResponseTo_HomeOffice.pdf

LSE Identity Project (2005c) *Main Report* (27 June). Archived at http://identityproject.lse.ac.uk/identityreport.pdf

LSE Identity Project (2006a) *All party briefing for report stage: Voluntary v. compulsory regimes* (23 January). Archived at http://identityproject.lse.ac.uk/voluntarybriefing.pdf

LSE Identity Project (2006b) *Home Office Accounting Report* (March) Archived at http://identityproject.lse.ac.uk/accountingreport.pdf

LSE Identity Project (2006c) *Research Status Report* (15 January). Archived at http://identityproject.lse.ac.uk/statusreport.pdf

LSE Identity Project (2008) Security briefing London School of Economics and Political Science. Archived at http://identityproject.lse.ac.uk/securitybriefing.pdf

LSE Identity Project (2009) *Identity Project Resources* Retrieved from http://identityproject.lse.ac.uk

Lyytinen K (1985) Implications of theories of language for information systems. *MIS Quarterly* 9(1), 61–74.

Lyytinen K, Baskerville R, Iivari J and Te'eni D (2007) Why the old world cannot publish? Overcoming challenges in publishing high-impact IS research. *European Journal of Information Systems* 16(4), 317–326.

MacKenzie D (1993 [1990]) *Inventing accuracy: A historical sociology of nuclear missile guidance.* The MIT Press, Cambridge, MA.

MacKenzie D and Wajcman J (1999) Preface to the Second edition. In *The social shaping of technology* (Mackenzie D and Wajcman J, Eds), pp xiv–xvii, Open University Press, Buckingham.

Majone G (1989) *Evidence, argument, and persuasion in the policy process.* Yale University Press, New Haven.

Makin K (2003) Ontario farmer challenges driver's licence photo *Globe and Mail* (15 October). Archived at http://www.theglobeandmail.com/servlet/story/RTGAM.20031015.wlicence1015/BNStory/National/

Mansfield T, Kelly G, Chandler D and Kane J (2001) Biometric product testing Final Report National Physical Laboratory (19 March). Archived at http://www.cesg.gov.uk/policy_technologies/biometrics/media/biometrictestreportpt1.pdf

Mansfield T and Rejman-Greene M (2003) Feasibility study on the use of biometrics in an entitlement scheme National Physical Laboratory. Archived at http://dematerialisedid.com/PDFs/feasibility_study031111_v2.pdf

Marche S (1991) On what a building might not be: A case study. *International Journal of Information Management* 11(1), 55–66.

Marron D (2008) "Alter reality": Governing the risk of identity theft. *British journal of Criminology* 48(1), 20–38.

Mårtensson P and Lee AS (2004) Dialogical action research at Omega Corporation. *MIS Quarterly* 28(3), 507–536.

Martins LL and Kambil A (1999) Looking back and thinking ahead: Effects of prior success on managers' interpretations of new information technologies. *Academy of Management Journal* 42(6), 652–661.

Marzouki MM (2005) Audition 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 (9 May). Archived at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CRAUDITIONPIAZZA.pdf

Matsumoto T, Matsumoto H, Yamada K and Hoshino S (2002) Impact of artificial "gummy" fingers on fingerprint systems (15 May). Archived at http://cryptome.org/gummy.htm

McCue A (2006) Government ID fraud claims – are they what they seem? Costs UK £1.7 bn a year? Figures "not an exact science" ... *Silicon.com*. Archived at http://www.silicon.com/publicsector/0,3800010403,39156140,00.htm

McFarlan FW (1984) Information technology changes the way you compete. *Harvard Business Review* 62(3), 64–71.

Mehmood T (2008) India's new ID card: Fuzzy logics, double meanings and ethnic ambiguities. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 112–127, Routledge, London.

Melville N, Kraemer K and Gurbaxani V (2004) Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly* 28(2), 283–322.

Milne GR and Culnan MJ (2002) Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998–2001 U.S. web surveys. *The information society* 18(5), 345–359.

Ministerie van Justitie (2005) Report (28 April). Archived at http://www.justitie.nl/images/uitgebreide%20identificatieplicht_3872_tcm34-74198.pdf

Mitev N (2000) Toward social constructivist understandings of IS success and failure: introducing a new computerized reservation system. In *Proceedings of 21st International Conference on Information Systems*, pp 84–93, Brisbane, Australia.

Mlcakova A and Whitley EA (2004) Configuring peer-to-peer software: An empirical study of how users react to the regulatory features of software. *European Journal of Information Systems* 13(2), 95–102.

Modine A (2009) Real ID law to receive makeover under Obama *The Register* (11 March). Archived at http://www.theregister.co.uk/2009/03/11/real_id_changes_napolitano_nga/

Monsters and Critics (2008) Superstition causes change in Taiwan ID card numbers with "4" *MonstersandCritics.com* (26 January). Archived at http://www.monstersandcritics.com/news/asiapacific/news/article_1388538.php/Superstition_causes_change_in_Taiwan_ID_card_numbers_with_&quot4%22

Monteiro E (1998) Scaling information infrastructure: The case of next-generation IP in the internet. *The information society* 14(3), 229–245.

Monteiro E and Hanseth O (1995) Social shaping of information infrastructure: On being specific about the technology. In *Information technology and changes in organizational work* (Orlikowski WJ, Walsham G, Jones MR and DeGross JI, Eds), pp 325–343, Chapman & Hall, London.

Moon MJ and Norris DF (2005) Does managerial orientation matter? The adoption of reinventing government and e-government at the municipal level. *Information Systems Journal* 15(1), 43–60.

Mosse B and Whitley EA (2009) Critically classifying: UK E-government website benchmarking and the recasting of the citizen as customer. *Information Systems Journal* 19(2), 149–173.

Myhr T (2008) Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution. *Information Security Technical Report* 13(2), 76–82.

National Audit Office (2000) The cancellation of the Benefits Payment Card project (18 August). HC 857 Archived at http://www.nao.org.uk//idoc.ashx?docId=ad57d1a3-921f-4347-9a25-7722ef0f4396&version=-1

National Audit Office (2007) Identity and Passport Service: Introduction of ePassports (5 February) HC 152. Archived at http://www.nao.org.uk//idoc.ashx?docId=9d292469-3491-4390-b171-0e46c21d98c1&version=-1

New Straits Times (2004) Privacy of MyKad holders to be protected by law (19 May).

Newkirk HE, Lederer AL and Srinivasan C (2003) Strategic information systems planning: Too little or too much? *Journal of Strategic Information Systems* 12(3), 201–228.

NIST (2005) The myth of goats: How many people have fingerprints that are hard to match? National Institute of Science and Technology NISTIR 7271. Archived at http://www.itl.nist.gov/iad/894.03/pact/ir_7271.pdf

NO2ID (2008) NIS options analysis outcome. Archived at http://identity-project.lse.ac.uk/NIS_Options_Analysis_Outcome.pdf

Noiriel G (2005) Audition Commission Nationale de l'Informatique et des Libertés (15 February). Archived at http://www.cnil.fr/fileadmin/

documents/approfondir/dossier/CNI-biometrie/CRAUDITIONNOIRIEL.pdf

Oates J (2005) Malaysia to fingerprint all new-born children *The Register* (4 May). Archived at http://www.theregister.co.uk/2005/05/04/malaysia_dabs_kids/

Office of Government Commerce (2003) Entitlement Cards OGC Gateway review: 0 – Strategic Assessment (23–25 June). Archived at http://ips.gov.uk/identity/downloads/Home_Office_ID_cards_programe_Gate_0_Report_June_2003.pdf

Office of Government Commerce (2004) Identity Cards OGC Gateway review: 0 – Strategic Assessment (26–29 January). Archived at http://ips.gov.uk/identity/downloads/Home_Office_ID_cards_programme_Gate_0_Report_January_2004.pdf

Office of Government Commerce (2009) OGC Gateway Review for Programmes & Projects. Retrieved from http://www.ogc.gov.uk/what_is_ogc_gateway_review.asp

Ogasawara M (2008) A tale of the colonial age, or the banner of a new tyranny? National identification card systems in Japan. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 93–111, Routledge, London.

Openbaar Ministerie (2005) 3300 keer geen identificatie op zak (2 February). Archived at http://www.om.nl/algemene_onderdelen/uitgebreid_zoeken/@140444/3300_keer_geen/

Organ J (2003) The Coordination of e-Government in Historical Context. *Public policy and administration* 18(2), 21–36.

Organization Science (1990) Special issue: Longitudinal field research methods for studying processes of organizational change. *Organization Science* 1(3), 213–337.

Otjacques B, Hitzelberger P and Feltz F (2007) Interoperability of e-government information systems: issues of identification and data sharing. *Journal of management information systems* 23(4), 29–52.

Palmer M and Burns J (2008a) Companies abandon ID card project *Financial Times* (23 January). Archived at http://www.ft.com/cms/s/05ec0a02-c9f5-11dc-b5dc-000077b07658.html

Palmer M and Burns J (2008b) Uncertainty at timing of ID cards sees BAE and Accenture pull out *Financial Times* (24 January). Archived at http://www.ft.com/cms/s/0/ce032b28-ca1e-11dc-b5dc-000077b07658.html?nclick_check=1

Parool H (2005) Al bijna acht ton boetes id-plicht (13 April). Archived at http://www.afautrecht.antifa.net/archief120405.html

Pascoe-Watson G (2005) Cost of ID card trebles *The Sun* (30 May).

People's Daily (2004) China starts to launch second-generation ID cards (30 March). Archived at http://english.people.com.cn/200403/30/print20040330_138863.html

Perri 6 (2005) Should we be compelled to have Identity Cards? Justifications for the legal enforcement of obligations. *Political Studies* 53(2), 243–261.

Perritt Jr., Henry H. (1998) Symposium on the Internet and legal theory: The Internet is changing international law. *Chicago-Kent Law Review* 73(4), 997–1054.

Pettigrew AM (1990) Longitudinal field research on change: Theory and practice. *Organization Science* 1(3), 267–292.

Piazza P (2005) Audition Commission Nationale de l'Informatique et des Libertés (8 April). Archived at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CRAUDITIONPIAZZA.pdf

Piazza P and Laniel L (2008) The INES biometric card and the politics of national identity assignment in France. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 198–217, Routledge, London.

Pieri E (2009) ID cards: A snapshot of the debate in the UK press ESRC National Centre for e-Social Science (23 April). Archived at http://www.ncess.ac.uk/Pieri_idcards_full_report.pdf

PIU (2002) Privacy and data sharing: Performance and Innovation Unit. Archived at http://www.cabinetoffice.gov.uk/media/cabinetoffice/strategy/assets/piu%20data.pdf

Porter ME (1985) *Competitive Advantage. Creating and Sustaining Superior Performance. Competition on the Internet: Aggregation Strategies.* The Free Press, New York.

Porter ME and Millar VE (1985) How information gives you competitive advantage. *Harvard Business Review* 66(4), 149–160.

Poster M (1990) *The mode of information: Poststructuralism and social context.* Polity Press, Cambridge.

Postman N (1992) *Technopoly: The surrender of culture to technology.* Vintage Books, New York.

Pounder C (2008) Evidence on the surveillance state and Parliamentary scrutiny of the decision to the use of the National Identity Register as a Population Register. Archived at http://identityproject.lse.ac.uk/Pounder.doc

Poynter K (2007) Poynter Review Initial Report (17 December). Archived at http://www.hm-treasury.gov.uk/d/poynter_review171207.pdf

Poynter K (2008) Poynter Review Final Report (17 December). Archived at http://www.hm-treasury.gov.uk/d/poynter_review250608.pdf

Privacy International (2005) Threats to privacy. Archived at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543674

Privacy Rights Clearing House (2007) How many identity theft victims are there? What is the impact on victims? Recent surveys and studies from Javelin Strategy & Research, Better Business Bureau, Identity Theft Resource Center, Federal Trade Commission, Gartner, and Privacy & American Business. Archived at http://www.privacyrights.org/ar/idtheftsurveys.htm

Privy Council Office (2004) Securing an open society: Canada's National Security Policy (April). Archived at http://www.pco-bcp.gc.ca/docs/information/Publications/natsec-secnat/natsec-secnat-eng.pdf

Raab D (2009) *The assault on Liberty: What went wrong with rights.* Fourth Estate, London.

Ramasoota P (1998) Information technology and bureaucratic surveillance: a case study of the Population Information Network (PIN) in Thailand. *Information Technology for Development* 8(1), 51–64.

Reid J (2007) Security is on the cards *The Guardian* (10 May). Archived at http://www.guardian.co.uk/commentisfree/2007/may/10/securityisonthecards

Republic of Estonia (2009) ID card: Making life easier. Archived at http://www.pass.ee/index.php/pass/eng/id_card/what_is_the_id_card

Ricoeur P (1981) *Hermeneutics and the Human Sciences: Essays on Language, Action and Interpretation.* Cambridge University Press, Cambridge.

Riley J (2005a) ID fraud on budget hit-list *Australian IT* (10 May).

Riley J (2005b) Privacy "risk" in national ID plan *The Australian* (21 January).

Romanosky S, Telang R and Acquisti A (2008) Do data breach disclosure laws reduce identity theft? In *Seventh Workshop on the Economics of Information Security*, Hanover, NH.

Royal Academy of Engineering and British Computer Society (2003) The challenge of complex IT projects. Archived at http://www.bcs.org/upload/pdf/complexity.pdf

Rule J (1974) *Private lives and public surveillance: Social control in the computer age.* Schocken books, New York.

Sarson R (2006) Techno world has MPs beat *The Guardian* (9 March). Archived at http://www.guardian.co.uk/technology/2006/mar/09/idcards.insideit

Sauer C and Willcocks LP (2001) *Building the e-business infrastructure.* Business Intelligence, London.

Sauer C and Willcocks LP (2007) Editorial: Unreasonable expectations – NHS IT, Greek choruses and the games institutions play around mega-programmes. *Journal of Information Technology* 22(3), 195–201.

Schick S (2004) The IT in your ID *ITBusiness.ca* (19 July). Archived at http://www.itvendorsdirectory.ca/Online-Resources/the-it-in-your-id-001.html

Science and Technology Select Committee (2006) Identity Card technologies: Scientific advice, risk and evidence House of Commons Sixth report of Session 2005–06. Archived at http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf

Searle JR (1969) *Speech acts: An essay in the philosophy of language*. Cambridge University Press, Cambridge.

Searle JR (1995) *The construction of social reality*. The Penguin Press, London.

Secretary of State (2003) Telegram to all Diplomatic and Consular Posts. Enhanced Border Security and Visa Entry Reform Act of 2002–ALDAC No. 1, on Executive Order 12958 (14 March). Archived at http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html

Sensenbrenner Jr. F. James (2005) 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, (7 April). Archived at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347–234812

Shannon CE and Weaver W (1949) *The mathematical theory of communication*. University of Illinois Press, Chicago.

Simon M and Houghton SM (2003) The relationship between overconfidence and the introduction of risky products: Evidence from a field study. *Academy of Management Journal* 46(2), 139–150.

Sismondo S (2004) *An introduction to science and technology studies*. Blackwell, Oxford.

Slaughter A-M (2000) Building global democracy. *Chicago Journal of International Law* 1(2), 223–229.

Somogyi EK and Galliers RD (1987) Applied information technology: From data processing to strategic information systems. *Journal of Information Technology* 2(1), 30–41.

Sørensen C, Whitley EA, Madon S, Klyachko D, Hosein IR and Johnstone J (2001) Cultivating recalcitrance in information systems research. In *Realigning Research and Practice in IS Development: The Social and Organisational Perspective* (Russo N, Fitzgerald B and De Gross JI, Eds), pp 297–316, Kluwer, Boise, Idaho.

Spiller S (2007) ID cards will give “false” data *BBC* (31 July). Archived at http://news.bbc.co.uk/1/hi/programmes/file_on_4/6922882.stm

Stamper R (1973) *Information in business and administrative systems*. Batsford, London.

Standing Committee on Citizenship and Immigration (2003) A national identity card for Canada? Archived at http://www2.parl.gc.ca/content/hoc/Committee/372/CIMM/Reports/RP1085068/cimmrp06/cimmrp06-e.pdf

Stanton JM (2008) ICAO and the biometric RFID passport: History and analysis. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 253–267, Routledge, London.

Star SL and Ruhleder K (1996) Steps toward an ecology of infrastructure: Design and access for large information space. *Information Systems Research* 7(1), 111–134.

Swanson EB (2003) Talking the IS innovation walk. In *Global and organisational discourse about information technology* (Wynn EH, Whitley EA, Myers MD and De Gross JI, Eds), pp 15–32, Kluwer, Boston.

Swanson EB and Ramiller N (2004) Innovating mindfully with information technology. *MIS Quarterly* 28(4), 553–584.

Te'eni D (2001) Review: A cognitive-affective model of organizational communication for designing IT. *MIS Quarterly* 25(2), 251–312.

Tempest M (2005) Clarke dismisses report on £300 ID cards *The Guardian* (16 June). Archived at http://www.guardian.co.uk/politics/2005/jun/16/immigrationpolicy.idcards

The Hindu (2008) Unique Identity Number to be issued from 2010 (10 November). Archived at http://www.hindu.com/thehindu/holnus/000200811102211.htm

The Labour Party (2005) Manifesto 2005. Archived at http://www.labour.org.uk/index.php?id=manifesto

The Local (2007) European ID "must be accepted in Sweden" The Local: Sweden's news in English (19 July). Archived at http://www.thelocal.se/7942/20070719/

The Star Online (2007) No more filling passport forms (5 October). Archived at http://thestar.com.my/news/story.asp?file=/2007/10/5/nation/19084229&sec=nation

The Sun (2005) Charles Clarke's ID rage (17 June). Archived at http://www.thesun.co.uk/sol/homepage/news/article108710.ece

The Sunday Times (2006) Emails from Whitehall officials in charge of ID Cards *The Sunday Times* (9 July). Archived at http://www.timesonline.co.uk/tol/news/uk/article684968.ece Now also available officially from http://ips.gov.uk/identity/downloads/foi/3905_URN_129.pdf

The Sydney Morning Herald (2005) Free speech suit filed against Japan (27 January). Archived at http://www.smh.com.au/news/Breaking/

American-files-freespeech-suit-against-Japan/2005/01/27/1106415700622.html?oneclick=true

Thompson B (2006) How to legislate against hackers *BBC* (13 March). Archived at http://news.bbc.co.uk/1/hi/technology/4799338.stm

Thompson S (2008) Separating the sheep from the goats: The United Kingdom's National Registration programme and social sorting in the pre-electronic era. In *Playing the identity card: Surveillance, security and identification in global perspective* (Bennett CJ and Lyon D, Eds), pp 145–162, Routledge, London.

Torgerson D (1986) Between knowledge and politics: Three faces of policy analysis. *Policy sciences* 19(1), 33–59.

Treasury Committee (2007a) Counting the population: Volume II Written Evidence (11 December). Archived at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmtreasy/183/183ii.pdf

Treasury Committee (2007b) Counting the population: Volume III Oral Evidence (11 December). Archived at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmtreasy/183/183ii.pdf

TWIC (2009) About TWIC. Retrieved from https://twicprogram.tsa.dhs.gov/TWICWebApp/AboutTWIC.do

U.S. Department of Health Education and Welfare (HEW) (1973) *Records, computers and the rights of citizens: report of the Secretary's Advisors Committee on Automated Personal Data Systems.* U.S. Government Printing Office, Washington.

UKIPS (2006a) s.37 1st Cost Report October 2006 (9 October). Archived at http://ips.gov.uk/identity/downloads/costreport37.pdf

UKIPS (2006b) Strategic Action Plan for the National Identity Scheme: Safe guarding your identity (19 December). Archived at http://ips.gov.uk/identity/downloads/Strategic-Action-Plan.pdf

UKIPS (2007a) Basic passport checks. Archived at http://ips.gov.uk/identity/downloads/BasicPassportChecks.pdf

UKIPS (2007b) NIS strategic supplier framework prospectus. Archived at http://www.ips.gov.uk/identity/working-suppliers-framework.asp

UKIPS (2007c) s.37 3rd Cost Report November 2007 (8 November). Archived at http://ips.gov.uk/identity/downloads/2007-11-06-Identity-Cards-Scheme-Cost-Report-November-2007.pdf

UKIPS (2008a) Delivery Plan 2008 (6 March). Archived at http://www.ips.gov.uk/identity/downloads/national-identity-scheme-delivery-2008.pdf

UKIPS (2008b) Front Office Services Prospectus: An opportunity to partner with one of the UK's most trusted brands – The British Passport (6 November). Archived at http://ips.gov.uk/identity/downloads/FrontOfficeServiceProspectus.pdf

UKIPS (2008c) Identity Cards Act Secondary Legislation: A consultation (21 November). Archived at http://ips.gov.uk/identity/downloads/NIS_Legislation.pdf

UKIPS (2008d) Identity Cards for Foreign Nationals: General Guidance Level 1 (25 September). Archived at http://ips.gov.uk/identity/downloads/IDCardsForForeignNationalsGeneralGuidance.pdf

UKIPS (2008e) Introducing the National Identity Scheme: How the Scheme will work and how it will benefit you (6 November). Archived at http://ips.gov.uk/identity/downloads/introducing_the_national_identity_scheme.pdf

UKIPS (2008f) IPS appoints five suppliers for the National Identity Scheme (23 May). Archived at http://www.ips.gov.uk/identity/press-2008-05-23.asp

UKIPS (2008g) National Identity Scheme Delivery Plan 2008: A response to consultation (6 November). Archived at http://ips.gov.uk/identity/downloads/ConsultReportv2.pdf

UKIPS (2008h) National Identity Scheme Tracking Research Wave 4: May 2008. Archived at http://ips.gov.uk/identity/downloads/IPS-Omnibus-Report-Wave-4.pdf

UKIPS (2008i) National Identity Scheme Tracking Research Wave 5: August 2008. Archived at http://ips.gov.uk/identity/downloads/STracking-Wave5.pdf

UKIPS (2008j) Passport validation service: Financial services industry. Archived at http://ips.gov.uk/passport/downloads/financial_services_brochure.pdf

UKIPS (2008k) s.37 4th Cost Report May 2008 (6 May). Archived at http://ips.gov.uk/identity/downloads/IPS-Identity-Cards-Scheme-Cost-Report-May2008.pdf

UKIPS (2008l) Thales awarded National Identity Scheme contract (1 August). Archived at http://www.ips.gov.uk/identity/press-2008-08-01.asp

UKIPS (2009a) Benefits at a glance. Retrieved from http://www.ips.gov.uk/identity/benefits-glance.asp

UKIPS (2009b) The interview process. Retrieved from http://www.ips.gov.uk/passport/interviews-process.asp

UKIPS (2009c) Proving your age. Retrieved from http://ips.gov.uk/identity/how-idcard-daily-proving.asp

UKIPS (2009d) What are the aims of the scheme? Retrieved from http://www.ips.gov.uk/identity/faqs-general-aims.asp

Unisys (2009) Unisys case study on the Government of Malaysia. Archived at http://www.unisys.com/public_sector/clients/featured_case_studies/malaysia_smart_card_.htm

Van Alsenoy B and De Cock D (2008) Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card. *Datenschutz und Datensicherheit* 32(3), 178–183.

Various (2002) Konferenz der Datenschutzbeauftragten des Bundes und der Länder (7–8 March). Archived at http://www.bfd.bund.de/information/DS-Konferenzen/63dsk_ent1.html.

Various (2005) INES de la suspicion au traçage generalise 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). Archived at http://www.iris.sgdg.org/actions/ines/argument-petition-ines.pdf

Verizon Business (2008) 2008 Data breach investigations report. Archived at http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Wadham J, Gallagher C and Chrolavicius N (2006) *Blackstone's guide to the Identity Cards Act 2006.* Oxford University Press, Oxford.

Walsham G (1993) *Interpreting information systems in organisations.* John Wiley & Sons, Chichester.

Walsham G (2006) Doing interpretive research. *European Journal of Information Systems* 15(3), 320–330.

Wang P and Ramiller NC (2004) Community learning in information technology fashion. In *Proceedings of the 25th International Conference on Information Systems*, pp 39–52, Washington, DC.

Watson A (2006) Letter to the Editor: ID cards will not help to counter terrorism *The Times.* Archived at http://www.timesonline.co.uk/tol/comment/letters/article630276.ece

Watson J (2004) Talks consider use of ID cards for business *VNUNet.com.* Archived at http://www.vnunet.com/computing/news/2071304/talks-consider-id-cards-business

Wenger E (1999) *Communities of practice: Learning, meaning, and identity.* Cambridge University Press, Cambridge.

West DM (2004) E-Government and the transformation of service delivery and citizen attitudes. *Public administration review* 64(1), 15–27.

Westrup C (1994) Practical understanding: Hermeneutics and teaching the management of information systems development using a case study. *Accounting, Management and Information Technologies* 4(1), 39–58.

Whitaker R (2006) Ping-pong and policy influence: Relations between the Lords and Commons, 2005–06. *Parliamentary Affairs* 59(3), 536–545.

Whitley EA (1996) Confusion, social knowledge and the design of intelligent machines. *Journal of experimental and theoretical artificial intelligence* 8(3/4), 365–381.

Whitley EA (1997) In cyberspace all they see is your words: A review of the relationship between body, behaviour and identity drawn from the sociology of knowledge. *Information technology and people* 10(2), 147–163.

Whitley EA (2009) Perceptions of government technology, surveillance and privacy: the UK identity cards scheme. In *New Directions in Privacy and Surveillance* (Neyland D and Goold B, Eds), pp 133–156, Willan, Cullompton.

Whitley EA and Hosein IR (2001) Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill. In *Realigning Research and Practice in IS Development: The Social and Organisational Perspective* (Russo N, Fitzgerald B and De Gross JI, Eds), pp 415–438, Kluwer, Boise, Idaho.

Whitley EA and Hosein IR (2005) Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy* 29(11), 857–874.

Whitley EA and Hosein IR (2007) Policy engagement as rigourous and relevant information systems research: The case of the LSE Identity Project. In *Proceedings of the 15th European Conference on Information Systems (ECIS2007), 7–9 June 2007, St. Gallen, Switzerland* (Österle H, Schelp J and Winter R, Eds), pp 1301–1312, University of St. Gallen, St. Gallen.

Whitley EA and Hosein IR (2008) Departmental influences on policy design: How the UK is confusing identity fraud with other policy agendas. *Communications of the ACM* 51(5), 98–100.

Whittle A and Spicer A (2008) Is actor network theory critique? *Organization Studies* 29(4), 611–629.

Willcocks LP and Griffiths C (1997) Management and risk in major IT projects. In *Managing Information technology As A Strategic Resource* (Willcocks L, Feeny D and Islei G, Eds), pp 203–237, McGraw Hill, Maidenhead.

Willcocks LP and Kern T (1998) IT outsourcing as strategic partnering: The case of the UK Inland Revenue. *European Journal of Information Systems* 7(1), 29–45.

Willcocks LP, Petherbridge P and Olson N (2003) *Making IT count: Strategy, delivery, infrastructure*. Butterworth, Oxford.

Willcocks LP and Whitley EA (2009) Developing the information and knowledge agenda in information systems: Insights from philosophy. *The Information Society* 25(3), 190–197.

Wilson D (2008) The politics of Australia's "Access Card." In *Playing the identity card: Surveillance, security and identification in global* *perspective* (Bennett CJ and Lyon D, Eds), pp 180–197, Routledge, London.

Winnett R (2005) "Bullying" by Whitehall on ID card report *The Times* (3 July). Archived at http://www.timesonline.co.uk/tol/news/uk/article539887.ece

Winograd T and Flores F (1986) *Understanding computers and cognition: A new foundation for design.* Addison Wesley, Reading, MA.

Wittgenstein L (1956) *Philosophical investigations.* Basil Blackwell, Oxford.

Woolf M (2005) Benefits of national identity cards were oversold, admits minister. Archived at http://www.independent.co.uk/news/uk/politics/benefits-of-national-identity-cards-were-oversold-admits-minister-501394.html

Yau C (2002) Letter to Editor *South China Morning Post* (25 January).

Yearley S (2005) *Making sense of science: Understanding the social study of science.* Sage, London.

Young T (2008) ID cards catch first victim *Computing* (10 December). Archived at http://www.computing.co.uk/computing/news/2232357/id-cards-scheme-snags-first

Zetter K (2005) Lawmaker rips RFID passport plans *Wired News* (4 May). Archived at http://www.wired.com/politics/security/news/005/05/67418

INDEX

Unless otherwise specified, all items relate to issues surrounding the UK Identity Cards Scheme. For identity policies in particular countries, see Identity policies, country name.