# Envisioning Technology through Discourse:

## *A case study of biometrics in the National Identity Scheme in the United Kingdom*

Aaron K. Martin

Information Systems and Innovation Group

Department of Management

London School of Economics and Political Science

Thesis submitted for the degree of Doctor of Philosophy

September 2011

# Declaration

I certify that the thesis I have presented for examination for the PhD degree of the London School of Economics and Political Science is solely my own work.

I warrant that this authorization does not, to the best of my belief, infringe the rights of any third party.

# Envisioning technology through discourse: A case study of biometrics in the National Identity Scheme in the United Kingdom

## Abstract

Around the globe, governments are pursuing policies that depend on information technology (IT). The United Kingdom's National Identity Scheme was a government proposal for a national identity system, based on biometrics. These proposals for biometrics provide us with an opportunity to explore the diverse and shifting discourses that accompany the attempted diffusion of a controversial IT innovation. This thesis offers a longitudinal case study of these visionary discourses.

I begin with a critical review of the literature on biometrics, drawing attention to the lack of in-depth studies that explore the discursive and organizational dynamics accompanying their implementation on a national scale. I then devise a theoretical framework to study these speculative and future-directed discourses based on concepts and ideas from organizing visions theory, the sociology of expectations, and critical approaches to studying the public's understanding of technology. A methodological discussion ensues in which I explain my research approach and methods for data collection and analysis, including techniques for critical discourse analysis. After briefly introducing the case study, I proceed to the two-part analysis. First is an analysis of government actors' discourses on biometrics, revolving around formal policy communications; second is an analysis of media discourses and parliamentary debates around certain critical moments for biometrics in the Scheme.

The analysis reveals how the uncertain concept of biometrics provided a strategic rhetorical device whereby government spokespeople were able to offer a flexible yet incomplete vision for the technology. I contend that, despite

being distinctive and offering some practical value to the proposals for national identity cards, the government’s discourses on biometrics remained insufficiently intelligible, uninformative, and implausible.

The concluding discussion explains the unraveling visions for biometrics in the case, offers a theoretical contribution based on the case analysis, and provides insights about discourses on the ‘publics’ of new technology such as biometrics.

# Acknowledgements

In completing this PhD, I have relied on the support and love of many wonderful people, without whom I would not have been able to see this project through.

First and foremost, I want to thank my supervisor, Edgar Whitley, for his relentless encouragement and guidance. Thank you for believing in me and being there during times of need and uncertainty. You have been a beacon of assurance the past five years. I hope this is just the beginning of a long and rewarding relationship.

Next I want to express my utmost gratitude to Gus Hosein, who has been an amazing teacher, colleague, and friend. You have gone out of your way to help me during this trying period. I cannot thank you enough for your expertise, generosity, and companionship. You truly are an inspiration.

I also want to thank my PhD examiners, Professor Martin Bauer and Dr. Neil Pollock, for their extensive feedback on ways to improve the first submission of this document.

I owe so much to my family for the moral and emotional support they continue to provide. While great distances often separate us, you are always there for me and I hope one day I can repay all you have done.

I could not have made it through this phase of my life without the companionship, support, and encouragement of my extended network of friends in London and abroad: Martin Garthwaite, Ramon Sabes-Figuera, Daniel Bernhard (especially for the proofreading and feedback), Maria-Martina Yalamova, Sofía Goldchluk, Matthew L. Smith, Jeffrey Stottlemyer, Azusa Sato, Katie Johnson, Nikos Gorgolis, Solon Barocas, and many others. You guys rock and I love you like family. And three great friends, in particular, deserve special recognition: Ian Reiley, Natalie Renew, and John Quattrochi. Your friendship is inestimable. I love y'all.

To my many friends and colleagues in the Information Systems and Innovation Group at the LSE – you know who you are – thank you for creating such a rich environment in which to study.

The International Development Research Centre had the courage to bring me on to work on certain of their research projects, thus providing me with both an opportunity to broaden my research profile and funding that was absolutely critical to completing this PhD project. In particular, I want to thank Heloise Emdon and Chaitali Sinha for these opportunities. I hope we are able to continue this important work in the future.

I also want to thank the funders, organizers, and participants of the *Everyday Life of Surveillance* seminar series, which introduced me to the ideas and debates from surveillance studies that undoubtedly influenced the direction of this dissertation.

This thesis is dedicated to my mother, Karen, for instilling in me the values of education and always encouraging my pursuit of knowledge, no matter where it takes me.

# Table of Contents

# List of Figures and Tables

# List of Abbreviations

| | |
|---|---|
| 9/11 | September 11, 2001 |
| AIT | Advanced Imaging Technology |
| ANPR | Automatic Number Plate Recognition |
| ARC | Application Registration Card |
| BIA | Border and Immigration Agency |
| CCTV | Closed-circuit television |
| COI | Central Office of Information |
| CRB | Criminal Records Bureau |
| DfT | Department for Transport |
| DHS | Department of Homeland Security |
| DNA | Deoxyribonucleic acid |
| EEA | European Economic Area |
| EEG | Electroencephalography |
| FCCC | Faith Community Consultation Consortium |
| FMR | False match rate |
| FNMR | False non-match rate |
| FRT | Facial recognition technology |
| FTC | Failure to capture |
| FTE | Failure to enroll |
| HMRC | Her Majesty’s Revenue and Customs |
| ICAO | International Civil Aviation Organization |
| ID | Identification |
| IP | Internet Protocol |
| IPS | Identity and Passport Service |
| IRIS | Iris recognition immigration system |
| ISAP | Independent Scheme Assurance Panel |
| IS | Information Systems |
| IT | Information Technology |
| LSE | London School of Economics and Political Science |
| NICRAS | Northern Ireland Community for Refugees and Asylum Seekers |

| | |
|---|---|
| NIR | National Identity Register |
| NIST | National Institute of Standards and Technology |
| NIS | National Identity Scheme (or National Identity Service) |
| RFID | Radio frequency identification |
| PIN | Personal identification number |
| PUS | Public understanding of science |
| PKI | Public key infrastructure |
| STS | Science and technology studies |
| TSA | Transportation Security Administration |
| UAE | United Arab Emirates |
| UK | United Kingdom |
| US | United States |
| US-VISIT | United States Visitor and Immigrant Status Indicator Technology |

# Chapter 1: Introduction

> A biometric is a unique identifying physical characteristic. Examples include facial recognition, iris patterns and fingerprints. (Home Office 2004c, p.36)

The above quotation is as seemingly straightforward and simple a definition of biometrics as one will find. It appeared in a United Kingdom (UK) government consultation document on identity cards, published in April 2004 by the Home Office[1], prior to six years of drawn-out and highly visible public and parliamentary debates on the merits and shortcomings of a national biometric identity system. Government officials provided other descriptions of the technology before and after the consultation, in various government policy documents and public statements. This one describes biometrics as ‘unique’, ‘identifying’, and ‘physical’, while explaining them in terms of ‘characteristics’. Accompanying the definition is a series of common examples of biometrics, which presumably are listed to help elucidate what is a new and uncertain concept. At first glance there appears nothing problematic about this basic explanation of a novel technology.

However, an informed and critical interpretation of the quotation reveals a number of perplexities. What if biometrics were not always unique? Would they still be effective? What if their ability to identify an individual was not a

[1] The Home Office is the UK government department responsible for immigration control, security, and policing.

given, but rather a complex and uncertain outcome, dependent on both high technology and considerable organizational resources? Would they be more dependable than other means of identification and authentication? And could biometrics also include non-physical dimensions (e.g., behavioral measurements)? In short, we might ask ourselves: could biometrics be otherwise?[2]

These initial rhetorical questions raise a subset of questions and concerns that this thesis aims to address. How do organizational actors, and in particular government spokespeople, communicate details of new technology in innovation processes? How do we capture important aspects of technology in policy discourses such that their nuances and uncertainties can be more fully appreciated, debated, and deliberated? More generally, what is the role of technological language in modern policy initiatives?

The aim of this study, therefore, is to explore *how* the UK government portrayed the role of multiple biometrics in its proposals for a national identity system. It examines the organizational and discursive dynamics attending the commencement, legislation, and implementation of biometrics in the UK's National Identity Scheme (NIS) – one of the official names given to the government's program for biometric identity cards. Motivated by innovative

[2] I return to these and related questions in the analysis and discussion chapters.

research approaches for studying technological controversies and social movements (Bauer 2002), this project draws on data from multiple sources, including discourses from the policy and media arenas. In particular, I critically analyze the visionary, promissory, and expectations-laden discourses on biometrics from a wide range of government policy texts, including official reports, legislative documents, public speeches, and other formal and informal communications. I also incorporate into the analysis both mass media discourses (from national broadsheet, business, and tabloid newspapers) as well as the discourses that emerged during the extended debates in Parliament about the government's identity cards program.

My overarching aim is to problematize common understandings of a specific technology (i.e., 'biometrics') in order to expose inherent tensions in the concept, and in doing so question how such concepts are leveraged in policy discourses comprising innovative information technology (IT) projects. I hope to contribute to academic understandings of technological innovation and policy processes around new technology. To achieve these goals, I conducted a longitudinal qualitative case study of a biometric identity system that eventually failed through the currents of political change. As fate would have it, this analysis was completed as the failed IT system actually underwent its demise. This study of the now-abandoned NIS in the United Kingdom thus serves as an opportunity to explore the diverse, contested, and politicized discourses that escort certain kinds of government IT.

The timing of the development of the case was such that the Conservative-Liberal Democrat coalition government scrapped the NIS as I was finishing my analysis and writing up the results. This provided me with an important and unusual degree of hindsight. Normally, a PhD study has to guess at evaluation; however I was able to view the unexpected outcomes of the NIS as they emerged during the completion of the thesis. As it were, the technological expectations that constituted the case were never held to account and so the complete story of implementing multiple biometrics on a national scale remains to be told.

In the remainder of this chapter I introduce contemporary debates about identity and identification (ID) in the information society. Afterwards I review some of the information technologies that are being introduced to address these problems. Focusing on biometrics, I then ask how researchers may go about creatively studying a technology that is often invisible to the public. Following this initial methodological reflection, I provide some detail on the history of national ID in the UK, the case of the NIS itself, and the broader research context, before transitioning into a critical review of the academic literature on biometrics.

## 1.1 Identity, policy, and technology

With the advent and popularization of the Internet and global diffusion and adoption of information and communication technologies, there are increasing concerns about the interrelated problems of identity, trust, and access on-line. These issues include concerns about the misuse of personal information by malicious or rogue actors, the development of reliable mechanisms for building trust relationships and facilitating trustworthy transactions in mediated environments, and attempts to restrict access to services only to those who are indeed entitled to them. 'Identity management' is also important in facilitating international mobility. Governments gather considerable amounts of personal information from citizens and visitors and issue identity documents to facilitate travel, based on internationally agreed standards and technologies.

However, behind these various scenarios lie fundamentally different problems and different levels of risk, which require different policy responses and, following from these policies, different technologies. An identity system for regulating access to a municipal swimming pool, for example, is likely inappropriate for international travel purposes.

In particular, there are important differences between the concepts of *identity*, *identification*, and *authentication*. Lyon distinguishes between identity and identification. While acknowledging that, in practice, we tend to treat the terms as synonyms, he understands the former concept as deeply personal and relational and the latter as connoting more technological concerns (2009, pp.8-12). Whitley and Hosein (2010) further distinguish between identification and authentication. Identification is understood as a process by which a person's identity is revealed (e.g., "This is Aaron Martin"). This is different from authentication, although in the common vernacular the two concepts are often conflated. Authentication strictly involves the confirmation of a request or granting of access to something and, importantly, does not require the revelation of an identity or personally identifiable information. For example, some typical authentication requests include:

- "Is this person a British citizen?" (e.g., at a border crossing),
- "Is this young person at least 18 years old?" (e.g., when proving whether someone is of legal age to consume alcohol),
- "Is the person an inhabitant of Camden Council?" (e.g., when accessing a restricted local service).

At no point in these requests does the person's identity (or components thereof – i.e., his or her name, ID number, or date of birth) need to be revealed. Authentication is therefore, fundamentally, a 'yes/no' type of request (i.e., it relies on the minimal disclosure of personal information in a transaction). Identification and authentication are thus distinct activities – motivated by different policy drivers – and need to be treated differently by systems that manage identity information. The over-identification of users, especially in contexts in which only authentication is required, can over time lead to the creation of extensive data profiles (or ‘data doubles’ (Haggerty & Ericson 2000; Lyon 2007)), which include information on people’s behaviors, activities, preferences, and future prospects, thereby triggering public concerns about unwarranted surveillance (Clarke 1994b).

Governments are trying to leverage new tools for identity management. Among these tools of identification and authentication are a range of different technologies and techniques – some well-established, others still emerging. The most obvious examples are the identity documents that most people are accustomed to, including identity cards, visas, and passport credentials. This paper documentation of yesteryear is being enhanced with new information technologies such as machine-readable zones, computer chips, and radio frequency identification (RFID) technologies (DHS 2006). Supported by encryption techniques (such as digital certificates and public key infrastructure (PKI)), these new ‘smart’ cards are said to be more reliable and secure than traditional paper documents, enabling better government identity management. They also require extensive technical infrastructures and organizational routines to be effective, as well as co-operation amongst government authorities. Moreover, there are internationally co-ordinated efforts to include biometrics in these documents in order to further secure government identity systems. What are we, as scholars, to make of these fast-moving and technologically complex efforts?

## 1.2 The dawn of a biometric era?

The widespread introduction and diffusion of biometrics into society by way of a compulsory national identity scheme, as was proposed in the UK, would arguably represent a sea change in identification. For one, unlike other identification technologies, biometric systems require the capture and digitization of analogue signals of the human body. This sort of bodily information is qualitatively different from, for example, the information that is used in a bar coding scheme to keep inventory at the local grocer. Its use also implicates various ethical concerns (Alterman 2003). Some argue that biometrics are highly personal information, the breach of which would present novel problems. Unlike stolen national insurance, social security, or credit card numbers, compromised biometric data are virtually irreplaceable: fingerprints cannot be cancelled or reissued in the case of theft.[3] Moreover, a government-sponsored scheme for biometrics brings with it an unavoidable political dimension, which most non-governmental identification systems lack. These politics are particularly important to the current case study, where government surveillance and data collection became especially high-profile

[3] There are technical mechanisms to alleviate some of these issues related to privacy and revocability. I discuss them in the next chapter.

issues during the research study, and which were frequently reported on in the mainstream press (Whitley 2009).

As these debates play out, popular business journals are steadily generating excitement around and interest in the use of biometric technologies. For example, a 2009 Business Week report entitled “The Dawning of the Biometric Age” implores readers to “say goodbye” to personal identification numbers (PINs) and old, photo-based ID cards. As evidence of this new era, the article points to the case of Switzerland, where in a 2009 national referendum voters decided in favor of including digital fingerprints in passports (Gibson 2009). (The article fails to note that the final result of the vote was extremely tight: 50.1% of the population voted in favor of the motion and 49.9% against).

Despite such journalistic enthusiasm, the technologies and techniques of biometrics are by no means proven or completely mature. Recently, they were subject to skepticism by a research body in the US. A National Academies report on biometrics, published in September 2010, illustrates the relevant concerns about the state of the art. Among the principal findings of this extended policy analysis were reminders that biometric systems are “inherently probabilistic” and “inherently fallible”, and that “the chance of error can be made small but not eliminated”. The report also argues that the scientific basis for biometrics is relatively weak and that more comprehensive evaluations are needed, which test not just technical aspects, but also operational and social dimensions of systems (Pato & Millett 2010). When these findings were first publicized the biometrics industry promptly responded, taking issue with some of the report's claims and providing its own evidence of the "real world" successes of biometrics implementations (International Biometrics & Identification Association 2010). Such ongoing impressions management is reminiscent of other controversial industries, such as biotechnology, in which public relations and corporate communications serve an important function in setting the public agenda (Bauer 2002, p.148). These controversies also set the stage for this research project.

## 1.3 How to study biometrics?

These ongoing debates about biometrics lead us to wonder about how social scientists may go about researching them. As marketers, vendors, and journalists tell us that biometrics are a technology whose time has come – that they are 'ready for prime time' –, and as critics contest the readiness, reliability, ethics, and motivations behind their use, on what basis can we study these innovations? Outside of the emergent and inconclusive findings from laboratory-based technical research, it is not clear what we actually know about biometrics. Minimal non-experimental empirical research on biometric technologies has been undertaken; in particular, the empirically based social science literature is especially bare.

There is a partial explanation for this: biometric systems are often spoken about, but rarely experienced. This is partly to do with their novelty as well as the difficult political and technological environments in which they are usually pursued. While politicians speak with excitement about the possibilities of biometrics in achieving varying policy objectives, and technologists busily try to build the perfect environments for their solutions, few systems actually see the light of day in large-scale, real-world implementations. These are complex technologies that require vast technological, human, and operational resources to operate seamlessly. As a result, there are few cases of biometrics being used 'in the wild' and, therefore, the social science-based investigations that typically study such systems once they are up and running have failed to materialize in substantial numbers. When biometrics are actually implemented, typically in immigration applications (e.g., the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system, which collects the biometrics of foreigners entering the United States; the Iris Recognition Immigration System (IRIS) operating in select UK airports; or iris biometric systems in use at UAE ports of entry) there is a void of information about their effectiveness and impacts, excluding the somewhat zealous press releases from the companies awarded the contracts to build the systems.

How then can we study such ‘invisible’ technologies? One way is to instead focus on the discourses around the proposals, rather than waiting for the systems themselves to appear. These discourses can tell us a lot about the beliefs, desires, and motivations of the actors involved, as well as how the technologies are conceptualized and understood in particular socio-political contexts. Previous critical research on the public’s understanding of science and the sociology of expectations provides approaches and concepts on which to initiate such a pursuit. These studies show us how to capture and analyze the invisible and imaginary.

To situate these thoughts on researching biometrics, I now provide some important historical background to the study. The case of biometrics in the NIS cannot be meaningfully presented without at least a minimal consideration of the history of identity cards in the UK. It is this history that fed much of the social and political resistance to the most recent Scheme.

## 1.4 A brief history of identity cards in the UK

The former Labour government's proposals for identity cards were not the first instance of an identity program in the UK. Historians note that ID cards were a reality well before former Home Secretary David Blunkett's pursuit of them. During both the First and Second World Wars, Britain introduced a form of national identity card. Agar (2005) explores these experiences and their relevance to the more recent proposals for the NIS.

According to Agar, the first ever national identity card and population register in the UK was a failure. It was introduced during the First World War as a means of determining the extent of the male population in the country. Existing government records were considered incomplete and ineffective for the purposes of developing a policy for conscription. Once the count had been completed and the government knew how many men were available to serve, political interest in national registration and identification cards waned, and the system was soon abandoned.

However, as Agar notes, the promise of a national identification system was not forgotten by the civil service, who during the Second World War re-introduced the idea of identity cards, primarily as a way of identifying aliens and managing the allocation of food rations.

> Crucial to the operation of the second National Register was its intimate connection to the organisation of food rationing. In order to renew a ration book, an identity card would have to be produced for inspection at a local office at regular intervals. Those without an identity card, would within a short period of time no longer be able, legally, to claim rationed food. This intimate connection between two immense administrative systems was vital to the success of the second card - they were not forgotten by members of the public - and provides one of the main historical lessons. (Agar 2005)

As identity cards became a facet of everyday life, they started being used for additional purposes (a phenomenon negatively referred to as 'function creep'), including identity checks by police officers. This use continued even after the war had ended. Eventually, liberal-minded citizens began questioning these practices and, in 1950, a man named Clarence Willcock disputed the police's routine check of ID cards. Willcock's legal challenges were not successful, but in the case's written judgment Lord Goddard (the Lord Chief Justice) criticized the police for abusing identity cards. And by 1952 Parliament had repealed the legislation that made national identity cards a reality in the UK.

As many observers have noted, including some civil society groups (Privacy International 1997), the civil service has since been regularly captivated by the idea of re-introducing national identity cards in the UK, with the aim of solving a diversity of policy problems, ranging from streamlining tax administration to ‘fixing’ immigration, among others. By the early 2000s they had tried again. In 2002, the Labour government, under Prime Minister Tony Blair, proposed a new national ‘entitlement card’ scheme. This proposal was then re-branded as a national ‘identity card’ scheme in 2004. Following failed attempts to pass the legislation, as well as a general election in the UK (in which the Labour party was again victorious), Parliament passed the *Identity Cards Act 2006* on 30 March, which enabled the first national identity card program since the Second World War.

However, this new Scheme was different from previous ones in several ways. The proposals were for a system of unprecedented size and complexity, comprising a centralized National Identity Register (NIR) (the electronic database on which the population’s identity data would be held), the collection and recording of over 50 pieces of personal information from individuals, and the issuing of identity cards and passports based on a new technology called “biometrics”.

Moreover, a number of features distinguished this Scheme from those in other countries. These features included the extensive use of biometrics both for enrolment (to ensure that no individual was entered onto the Register more than once) and verification; the proposed use of a single identification number across government and the private sector (Otjacques et al. 2007); and an ‘audit trail’ that was expected to record details of every instance that an identity was verified against information stored on the Register.[4]

The successful implementation of the Scheme, therefore, would have required technological expertise in the development of large scale, highly secure databases, advanced computer chip technologies for ID cards, sophisticated data collection mechanisms for the ‘biographical footprint’ checking during the enrolment process, system integration skills to combine all the different aspects of the Scheme, and specialist skills in biometric enrolment and verification.

The government’s program for identity cards went through various transformations after the Bill became law. The configuration of the NIR, for example, underwent several changes. In its original conception, the NIR was to be a brand new, central store of data. This changed in December 2006 when the Identity and Passport Service (IPS) – the sub-department of the Home Office responsible for implementing the Scheme – released its *Strategic Action Plan* and set out a revised database schema for the Register. The idea was to separate the biographic, biometric, and administrative information, and

[4] This requirement for a personal audit trail would prove to be particularly controversial amongst activists, who viewed it as a dangerous tracking device.

store them on different databases. The stated reasons for this segregation were to improve security and make use of “the strengths of existing systems” (IPS 2006c, p.10). However, some argued that this change was a poorly disguised attempt to reduce costs. The government’s proposals for ID cards went through various other changes over the course of Scheme’s lifespan, primarily motivated by concerns about managing costs and achieving observable successes. I will return to this discussion in chapter 5, focusing in particular on the history of biometrics in the Scheme, as these are the main focus of the analysis.

For now it suffices to observe how impressive and audacious the government’s plans were for the Scheme and biometrics. The collection of *multiple* biometrics, including fingerprints and irises, from tens of millions of citizens and foreigners was a project that had not been undertaken before as part of a national identity system. The plans for real-time, on-line biometric identification against a centralized, government-managed database were also a major innovation. While other countries already operated their own national ID systems, the proposed use of these biometrics, in this way – and on this scale – was something that had not been attempted before.

Before outlining the structure of the research thesis, I want to provide a brief overview of the wider social and political context in which the debates on, and activities for, the National Identity Scheme took place. This discussion exposes some important external factors that affected the trajectory of discourses in the case.

## 1.5 Broader research context

This research project was further motivated by a number of developments that relate to the particular period and place in which the NIS was proposed and pursued. On the one hand, these contextual factors complicated the empirical project, but on the other hand they also enriched it.

First, there were countless other e-government systems that were proposed and implemented contemporaneously as the NIS. Many of these programs incorporated similar techniques and technologies (such as identity verification or biometrics) and generated similar levels of public debate and resistance. As one followed these various debates in policy discourses and media coverage, it was sometimes difficult to determine exactly what policies or technologies were being talked about and disputed. For example, in certain media reporting the relevant issues were often lumped together as a general critique of government surveillance or poor data security practices. Drawing a line around the ‘case’ required effort and care. Indeed, even on the issue of identity cards the Home Office often blurred the distinction between identity cards for foreign nationals (which are, in fact, just detached visas, and fall under different legislation – I explain this fact in detail later on) and the identity cards that British nationals were invited to adopt.

Here I list just a few of the many e-government systems that were concurrent to the Scheme.[5]

- e-Borders – a Home Office system for recording information on everyone who enters and exits the UK
- Biometric residence permits for non-EEA foreign nationals (informally known as 'identity cards' for foreign nationals)
- Iris recognition immigration system (IRIS) – the iris biometrics-based, registered passenger program in place in certain UK airports
- National DNA Database – a forensic database that holds DNA information on those convicted or suspected of certain classes of crimes, plus volunteer samples
- ContactPoint – a national index of all children under the age of 18 in England
- Communications Database – a database of communications surveillance created under the Interception Modernisation Programme
- National Childhood Obesity Database – a UK government database for tracking overweight and obese children
- National Health Service's National Programme for IT, which involved the centralization of patient records
- Automatic Number Plate Recognition (ANPR) systems – a video surveillance method that uses optical character recognition to read the license plates on vehicles

Second, concurrent with the rise in government systems and databases, there was an increasingly vocal public debate about whether and to what extent the

[5] For an extended list and discussion on these systems see the Database State report (2009).

UK is becoming a “surveillance society” (Ball et al. 2006; Surveillance Studies Network 2010). It was, and still is, not uncommon to see these debates represented on the front pages of national broadsheets and tabloid newspapers (Whitley 2009), including most recently national scandals involving voicemail and phone hacking. The topics of government surveillance and privacy are thus entering the mainstream like never before. The Conservative Party even made it a point to take a political stand on these issues, releasing a paper prior to the general election of 2010 entitled “*Reversing the rise of the surveillance state*” in which, among other things, they called for the abolition of the National Identity Register. And following the demise of the NIS, activist groups are now rallying around the larger fight against the “database state”, which lends credence to the argument that the information and communication technologies central to these systems are appearing in political discourses in a qualitatively different manner than in the past.

In situating this case study, one also should not underestimate the extent to which regular government data breaches contributed to critical debates around the government’s use of citizens’ data. Public controversy following Her Majesty’s Revenue and Customs’ (HMRC) loss of two computer discs containing the personal details of all families in the UK with a child under the age of 16 (totaling 25 million records) led to unprecedented public debates around data security and even entered discussions about the future of the NIS and the role of biometrics therein. Following the announcement of the lost discs, it was suggested by officials that the inclusion of biometric identifiers in the HMRC dataset would have prevented or lessened the impact of the security breach. The main point for now is that the case of the NIS cannot be treated in isolation, but rather must be appreciated as part of a larger socio-political context in which privacy, surveillance, and security were increasingly salient themes.

## 1.6 Overview of the research

The remainder of this research thesis is structured as follows:

Chapter 2 presents a critical review of the extant literature on biometrics, spanning computer science, the social sciences, and information systems and management studies. These disparate fields naturally approach the study of biometrics in dissimilar ways and offer different insights on the technologies and the organizations that pursue them. After noting the relative strengths and weakness of each body of literature, I draw attention to a lack of longitudinal case studies, and particularly ones that explore the discursive and organizational dynamics that accompany the implementation of multiple biometrics on a national scale.

In chapter 3 I devise a theoretical framework for studying the speculative and future-directed discourses that constituted the case. This framework incorporates aspects of the discursive processes of framing, and draws on concepts from organizing visions theory, the sociology of expectations, and critical approaches to studying the public's understanding of science. These provide a conceptual path for an extensive analysis of the stock of public discourses that accompanied the roll-out of biometrics in the Scheme.

With this framework in place, I pose three inter-related research questions:

1. How did government spokespeople portray a vision for biometrics in the National Identity Scheme, and to what extent did this vision organize efforts and mobilize actors to innovate?
2. How did policy debates and media reportage discursively capture biometrics, and what were the limitations of these technological discourses in revealing the complexities and perplexities of biometrics?
3. How were the 'publics' of biometrics portrayed in these discourses?

Chapter 4 is a methodological discussion in which I justify and explain my research strategy (i.e., the case study strategy), tell the story of my methodological experiences, review my data collection methods (exploratory focus groups interviews and methods for collecting policy communications and media reports), and flesh out my analysis technique, namely critical discourse analysis.

Chapter 5 initiates the analysis by briefly re-introducing the case study, describing the range of actors involved and focusing, in particular, on the critical moments in the short-lived history of biometrics in the NIS. These six critical or ‘watershed’ events mark important moments in the Scheme’s roll-out when either the system as a whole, or the biometric component specifically, was subject to increased public scrutiny and debate. In one instance, the designated critical moment marks a ‘non-event’ (that is, the gradual, discursive withdraw of iris biometrics in the Scheme, which goes unremarked for quite some time).

In chapters 6 and 7 I present the two-part critical discourse analysis. Chapter 6 includes the analysis of the government discourses on biometrics found in formal communications, such as policy documents, legislative texts, and public presentations. This presentation of government discourses is structured around seven dimensions of new technology as outlined by Orlikowski and Gash (1992). These dimensions are 1) organizational philosophy towards technology, 2) issues around initiation, 3) implementation concerns, 4) issues concerning use, 5) success criteria, 6) perceived impacts, and 7) relations with other players in the computing social world.

Chapter 7 offers an analysis of media discourses and parliamentary debates, which is presented around the previously identified critical moments for biometrics in the Scheme. These data provide another prospective with which to understand the discursive dynamics that shaped the biometric concept in the case study.

The final chapter reflects on the major findings from the analysis, including the reasons for problematic visions for biometrics in the case. It extends organizing visions theory in light of the findings from the case analysis, focusing on the themes of the ontology of visions, temporality, and resistance. It also offers insights about discourses on the publics of new technology. It concludes by reflecting on the limitations of the case study and looking forward to new research opportunities emerging from the dissertation.

# Chapter 2: Critical literature review

## 2.1 Introduction

In this chapter I review the wide-ranging and multi-disciplinary literature on biometrics. This critical literature review highlights the strengths of the existing research on biometrics and exposes some important shortcomings; specifically, the lack of an extensive, longitudinal study of the development of discourses about biometrics in a specific context, and how these discourses interplay to constitute a vision for new technology.

The academic literature relating to biometrics can be categorized under three main rubrics. These are 1) computer science and electrical engineering explorations of biometrics, biometric techniques, and related technologies, 2) social science and ethical analyses of biometrics, which are often focused on surveillance, privacy, and security concerns, and 3) studies of user acceptance of biometric technologies, usually undertaken by management and information systems scholars. These acceptance studies are uniformly set within the context of a business organization or corporation, and typically neglect the larger social forces that influence perceptions and acceptance of, or resistance to, biometrics.

Of course, these rubrics are convenient categorizations that overlap significantly; by no means are they meant to be mutually exclusive. For example, studies of biometrics acceptance inevitably enter into discussions on privacy, surveillance, and security. Broadly speaking however, these accounts clearly differ from more sociologically inclined treatments in terms of their point of departure, analytical focus, and intellectual objectives.

## 2.2 Techniques and technologies of biometrics

A thorough literature review on biometrics cannot escape a voluminous and important body of technical research. Although this thesis is more concerned with the social implications of introducing biometrics on the national scale, it is prudent to begin this review with this literature as biometrics are, at base, impossible without these technologies. Therefore the following review addresses this technical literature, doing so critically, while suspending judgment about any claimed certainties about biometrics.

The vast majority of the academic literature on biometrics originates in the inter-related fields of computer science, human-computer interaction, and electrical engineering. In the pragmatic tradition of applied mathematics and statistics, this literature seeks to improve upon the perceived problems facing existing biometric methods, technologies, and applications. Researchers work to solve various technical problems ranging from faults in pattern recognition software (Jain et al. 2000), to fusing multiple (multi-modal) biometrics (Ross & Jain 2004), to improving the efficiency of biometric database search (Mhatre et al. 2005), among various other research areas.

Scope limitations prevent an exhaustive review of this literature. Moreover, the highly technical nature of this corpus does not lend itself to an overtly social science focused analysis of biometric identity schemes. Exploring such technical minutiae for several different biometric methods (e.g., fingerprinting, iris scanning, and facial recognition) would distract us.[6] However, certain work from this literature should be reviewed in detail, so as to inform a general discussion about biometrics, their strengths, and the various problems and uncertainties that surround the technologies.

## Basics of biometrics

Dictionary definitions of biometrics invariably state that they are physiological or behavioral measurements meant to identify someone or verify an identity. The former type of biometric includes facial geometry (facial recognition), fingerprinting, hand geometry, vein pattering, iris patterning, and DNA profiling, among an array of other emerging and prospective techniques such as ear and nose biometrics (Burge & Burger 2000; Moorhouse et al. 2009). Behavioral biometrics include techniques such as signature recognition,

[6] For readers interested in a comprehensive introduction to the different biometric modes, see Bowyer et al. (2008) for iris biometrics; Jain et al. (2010) for fingerprinting; and Bowyer (2004) for facial recognition.

keystroke dynamics recognition, gait recognition, and speech or voice recognition[7], and have been referred to in the literature as "behaviometrics" (Nisenson et al. 2003, pp.363-364). Unlike conventional methods that rely on what you know (such as passwords, personal identification numbers (PINs) or cryptographic keys) or what you possess (e.g., identity tokens or access cards), biometrics depend on facets of the human body, specifically what you are and what you do (O'Gorman 2003), and are thus believed to be stronger or better technologies as they cannot be forgotten or misplaced.

Within the literature it is generally agreed that a bodily measurement must satisfy certain requirements before it can qualify as a 'biometric': it must be 1) universal, 2) distinct, 3) relatively permanent, and 4) collectable (Jain et al. 2004, p.4).

'Universality' means that all participants in a given population possess the characteristic. Otherwise, not everyone can use the system. If a certain biometric is not universal across a population of users, then multiple biometrics might be used, as was originally proposed in the National Identity Scheme (NIS) (with at least four different biometrics (i.e., iris, face, fingerprint, and signature) considered).

[7] Usually characterized as a behavioral biometric, voice does have an underlying physiological component (O'Gorman 2003).

The ‘distinctiveness’ requirement aims to avoid cases in which more than one individual shares the same characteristic. For example, to rely solely on height as a biometric identifier would make it difficult to distinguish between otherwise unique people. ‘Permanence’ is important because a rapidly changing identifier would result in a live biometric not matching its stored record, thus requiring the regular re-enrollment of biometric information. This could undermine the system wholesale, depending on its scale, as large numbers of re-enrollees could prove administratively burdensome, and regular re-enrollment unacceptable to users. ‘Collectability’ is understood as the quantitative measurability of a characteristic (Jain et al. 2004, p.4). An immeasurable bodily feature cannot be used as a biometric. Most biometric measurements are of external characteristics and thus are easily measured, but biometrics may also use internal features of the body such as measuring the vein patterns inside one’s hands.

## Enrollment

A basic process applies to all systems that seek to identify individuals using biometrics. This is the enrollment process. These steps include the initial capture of biometric data, the subsequent processing or conditioning of these data for storage purposes, the extraction of certain features in the data, and the generation of a biometric template. A template can be defined as “a compact description of a biometric sample” (Ross et al. 2007, p.544). Jain et al. (2004, p.5) illustrate this enrollment phase (for fingerprints) as follows:

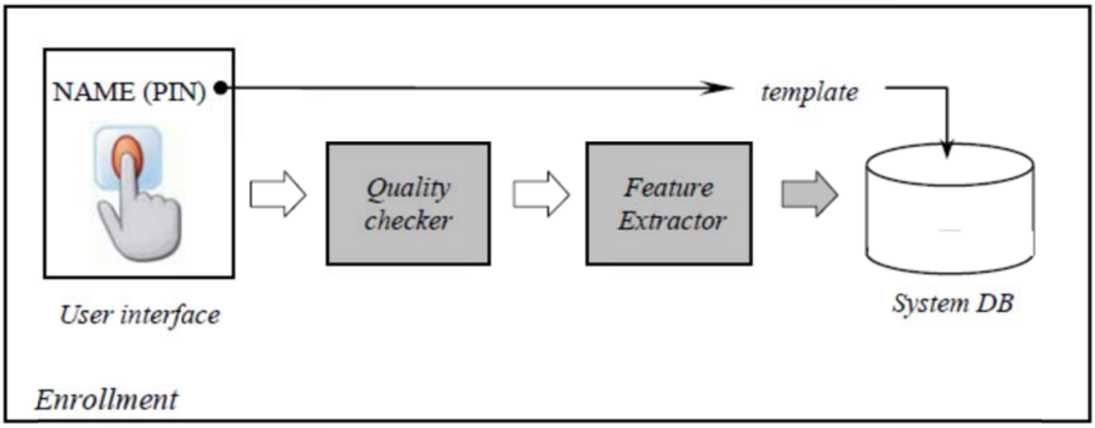


Figure 2.1: Enrollment process for fingerprints (Jain et al. 2004)

Note that while the actual ‘raw’ biometric images may be saved for administrative reasons (in the event that they need to be re-processed so that a new template can be generated at a later date following a technology upgrade, for example), most often it is the compressed, feature-extracted templates that are stored and compared against the ‘live’ data that is captured. In other words, it is not the ‘actual’ fingerprint (or iris image, etc.) that is stored and used, but rather a digital code (i.e., the template). Depending on the context, this comparison occurs in one of two different modes: verification or identification (Jain et al. 2004, p.4).

## Verification

Biometric verification is the process by which a claimed identity is authenticated against a previously recorded biometric template. An individual presents her/himself as being someone (e.g., "I am Aaron Martin.") and in response, the biometric system seeks to answer the query: "Is this person who s/he claims to be?" More succinctly, verification is the one-to-one comparison of captured live data against a stored template. Wayman associates this mode with what he calls 'positive recognition', the aim of which is to prevent multiple people from using the same identity (2001, pp.93-94). Jain et al. (2004, p.5) depict this phase - again, for fingerprints - as follows:

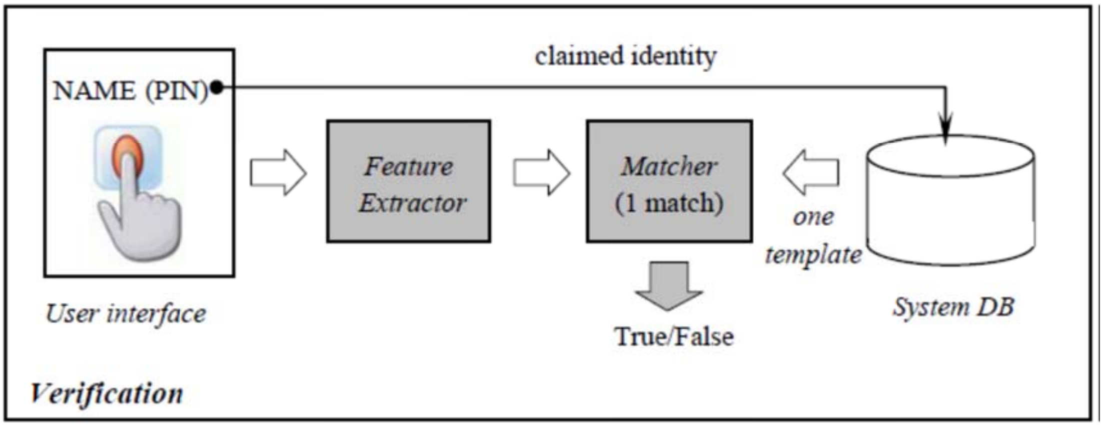


Figure 2.2: Verification process for fingerprints (Jain et al. 2004)

## Identification

Biometric identification involves the comparison of live biometric data against a larger database of biometric records. It aims to answer the question: "Whose biometric information is this?" (Jain et al. 2004, p.5). Identification therefore seeks to establish identity by means of a one-to-many comparison.

According to Wayman, this method is important in ‘negatively recognizing’ individuals. During a process of negative recognition, the system establishes whether a person is who s/he denies to be. The purpose of negative recognition is to prevent individuals from using multiple identities (2001, p.94). Importantly, this sort of negative recognition is only possible if the person’s biometrics have been previously enrolled on a database. Jain et al. (2004, p.5) depict this phase (for fingerprinting as well) as follows:

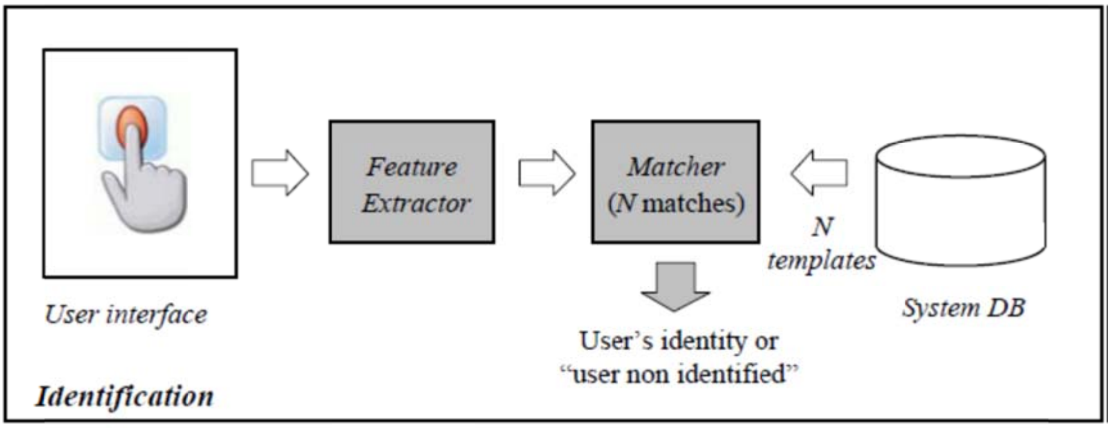


Figure 2.3: Identification process for fingerprints (Jain et al. 2004)

Jain et al. (2004) identify three further requirements that should be satisfied by a functioning biometric system. These are performance, acceptability, and circumvention. Performance encompasses such factors as the accuracy and speed of recognition, the computational resources needed for accurate and quick processing, and operational and environmental conditions (such as trained staff and proper lighting). Acceptability is the extent to which the user population is willing to use the system – an important factor in the current study – while circumvention refers to the susceptibility of the system to fraudulent use (Jain 2004, p.4).

## System errors

There are multiple ways that a biometric system can malfunction. Imperfect imaging conditions (e.g., a dirty sensor) may prevent a true match from being recognized as such. Ephemeral physiological changes may also affect data capture and template matching, such as when a cut or bruised finger prevents a system from enrolling or authenticating a fingerprint record, or when a week-old beard confuses a facial recognition system. The role of ambient conditions such as room temperature and humidity must also be taken into consideration when assessing a system's performance, along with the inevitable vagaries and inconsistencies of users' interactions with a scanner or sensor (Jain et al. 2004, p.6).

For a study of public discourses about biometrics, we should review the different types of system error that may occur as a result of the abovementioned issues and other performance problems. No biometric system is ever perfect; exploring the various ways in which biometrics may not work is a crucial benchmark without which we cannot fully appreciate or comprehend public discourses of how they are *supposed* to work. The impossibility of perfect identification is an oft-repeated criticism aimed at governments that try to use biometrics to uniquely identify everyone. However, errors are inescapable. It is thus important to see how actors interpret and talk about these errors. As Prabhakar et al. (2003) remark, the “lack of understanding of the error rates is a primary source of confusion” about biometrics (p.35).

## Enrollment errors

As previously stated, before someone can use a biometric system s/he must first be enrolled. This involves providing the appropriate biometric identifiers for storage on either a database or some other storage device such as a ‘smart’ card. During this phase, a user’s biometric characteristic is scanned and that information is usually converted into a digital representation of the original input. The representation is quality checked to ensure that it can be reliably processed at successive stages. Further processing takes place to generate a compressed but expressive representation, known as a template (Jain et al. 2004, p.6).

Enrollment is vulnerable to two types of error: failure to capture (FTC) errors and failure to enroll (FTE) errors. FTC errors result when a system cannot read a physical characteristic because it cannot locate a signal of satisfactory quality (Jain et al. 2004, p.7). FTE errors generally arise when a system rejects an input because it is deemed to be of poor quality. A system’s FTE *rate* represents the frequency with which users are unable to join a system. Importantly, enrollment failures of this sort present numerous socio-economic problems related to inclusion and exclusion, which are discussed throughout this thesis.

### Matching errors

FTE errors relate to two further types of error: false matches (also known as false acceptances or false positives) and false non-matches (alternatively called false rejections or false negatives). A false match is when a system mistakenly accepts the biometric input of one person by identifying them as somebody they are not. False matches involve mistakenly accepting a person who has no previous record in the database or matching a previously enrolled user to someone else's record. On the other hand, a false non-match is when a system mistakenly reports that someone's biometric is not in its records, when in fact it is – false non-matches dispute that you are you. Each of these errors is associated with a probability that a given user will be incorrectly accepted or rejected – falsely identified either way. These are known as false match rates (FMRs) and false non-match rates (FNMRs), respectively.

If one plotted the FMR and FNMR to a graph, what is known as the 'threshold value' would be the point at which decision-makers find the prevalence of both acceptable for a given biometric system. The higher the threshold value is set, the higher the FNMR becomes and the more secure the system is said to be. In this case, the system will occasionally reject an enrolled user, aiming to err on the side of caution, and is less likely to accept a fraudulent input as valid. If the threshold value is lowered and the system is made less sensitive - more tolerant of input variations and noise – the FMR grows. Low threshold value systems are often preferred in low-security environments, where the nuisance of a false rejection outweighs the consequences of a false match. Ultimately, decision-makers take a stand on this tradeoff based on the system's requirements and intended purpose.

One final piece of technical vocabulary worth presenting is what is known as a matching score: a value produced by the system estimating the likelihood that two biometric inputs originate from the same user. This is always a measure of probability. Jain et al. graphically depict the relationship between the FMR, FNMR, threshold value, and matching score (see Figure 2.4).

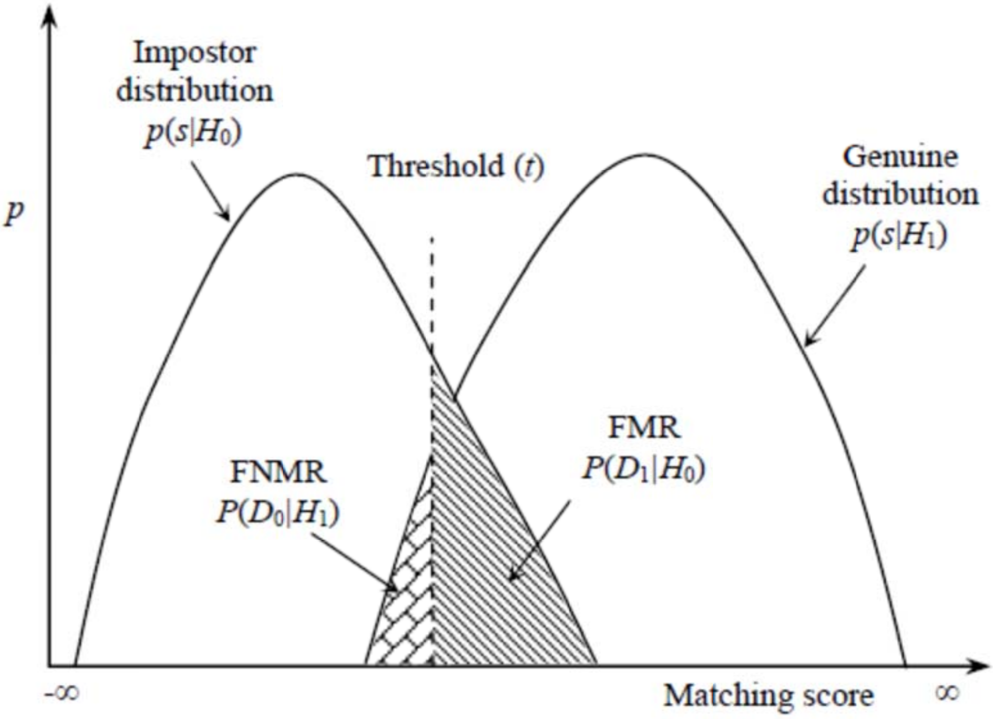


Figure 2.4: Relationship between false match rate, false non-match rate, threshold value, and matching score (Jain et al. 2004)

## Limitations of biometrics

Besides these generic error rates and the inherent limitations of biometrics, every biometric system is plagued by certain performance problems related to the specific bodily characteristic being measured. For example, it is well-established that manual laborers and older people tend to encounter problems with fingerprint biometric systems, as intensive manual labor (handling concrete, for example) and the aging process wear down fingerprints (Jain et al. 2010, p.41).

For many years, those in the technical community believed that iris biometrics were static throughout life. It was argued that, unlike fingerprints, which wear with age, or faces, which might change drastically with wrinkles or facial hair, irises were for life and thus could potentially solve the permanence problem permanently (Miyazawa et al. 2008; Monro et al. 2007; Thornton et al. 2007). Recent research by Bowyer et al. (2009), however, calls into question this and other “accepted truths” of biometrics.

The previous consensus held that normal aging does not noticeably affect an iris biometric template, preventing the need for periodic re-enrollment. Because re-enrollment would require users to prove their identity independently again, at their own inconvenience, and also adds to the administrative cost of the system, a one-time, permanently valid biometric would make biometric systems exponentially more practicable (Bowyer et al. 2009). However, Bowyer et al. find that the FNMR of iris biometrics might increase over time, potentially indicating that irises are not as unchanging as was previously thought.

Bowyer et al. dispel other “accepted truths” of iris biometrics, including the effects of pupil dilation on a system’s ability to correctly match iris biometrics to the appropriate user’s identity record and whether wearing contact lenses can affect the accuracy of iris recognition. In both cases, the accepted truth (i.e., that neither pupil dilation nor wearing contact lenses affect system accuracy) turned out to be false. These emerging findings on the limitations of biometrics reflect the ongoing uncertainty of the science and technical methods involved. The policy implications of these uncertainties are significant and merit further exploration, especially considering ongoing attempts by governments around the world to employ biometric techniques in large-scale civil implementations. We must also consider how such uncertainties manifest themselves in public discourses on biometrics, as many of these discourses feed into policy processes.

Other anomalies find their way into technical evaluations of biometric systems. The National Institute of Standards and Technology (NIST) recently tested the performance of two-dimensional still-image facial recognition algorithms – the largest public evaluation of the performance of facial recognition systems ever conducted (Grother et al. 2010). Of the report's many peculiar findings: men were more easily recognized by facial recognition systems than women; heavier people were easier to recognize than more slender subjects; and Asians were more easily recognized than Caucasians. Furthermore, certain algorithms had difficulties recognizing young people as compared to elderly people, whereas for other algorithms the opposite was true (Grother et al. 2010). The implications of this technological unreliability – and its exclusionary effects – are explored in the next section on sociological interpretations of biometrics.

## Images versus templates

As noted, the literature explains that featured-extracted templates of biometric images are stored. These digital approximations, rather than actual biometric images, are used to identify users. Many systems collect and store information about, or a representation of, the fingerprint, facial measurements, or a binary iris code, rather than collecting and storing an entire image of the finger, face, or iris. This distinction matters because it is commonly argued that using templates or representations, rather than actual images, is more privacy-friendly and secure. If these data are lost, then users need not worry about being falsely impersonated, it is said.

However, depending on the application, biometric systems do not rely exclusively on templates. For example, forensic applications store original images (Faundez-Zanuy 2005, p.14). For expansive and complex systems like nation-wide biometric identification schemes, it may be necessary to record and retain original images to prevent the need for wholesale re-enrolment in the event that decision-makers choose to switch to another system in the future, or make significant changes to their existing infrastructure (including updating algorithms, templates, scanners, middleware, and databases). The lack of generally accepted biometric standards means that new templates would have to be reprocessed from the original images.

## Innovations in biometrics

Though the practice is largely untested, recent computer science research has shown that it might be possible to reconstruct or regenerate fingerprint images from the stored biometric templates. Following work that tried to reverse engineer facial biometrics from their accompanying templates (Adler 2003), Ross et al. (2007) were able to demonstrate a technique for rebuilding fingerprints with only the so-called minutiae points of the template. While not a perfect recreation (i.e., more information is needed to reconstruct the fingerprint image entirely), such demonstrations do speak to outstanding concerns about the potential privacy concerns around new biometric technologies – if ‘raw’ inputs could be manufactured from stored biometric templates, then stolen templates would suddenly acquire colossal value for identity thieves everywhere. One could steal a template, recreate an original image, and ‘be’ somebody they are not.

In response to these and related concerns, other researchers have attempted to design what they call ‘cancellable’ biometrics (Bolle et al. 2002). One of the main criticisms of biometrics is that people have a limited number of biometric identifiers (i.e., most of us only have two eyes, ten fingers, and one face). In the event that biometric data are compromised, it would be very difficult if not near impossible to revoke these data. Unlike a credit card number or national identity number, which can be replaced, if lost or stolen, a biometric compromised is a biometric neutralized: it cannot be replaced and so it cannot be used any longer. Thus, one of the properties that make biometrics so attractive for identification or authentication purposes (i.e., that that they are relatively permanent and do not change over time) is also one of their drawbacks.

The idea behind cancellable biometrics is to intentionally distort recorded biometrics, systematically and repeatedly. If for whatever reason a stored variant of the original biometric is compromised, a new variant of the same biometric can be produced, the change documented, and the identity re-secured. These researchers also aim to make the transformation technique non-invertible so the original biometric image cannot be recovered even with full knowledge of the distortion process (Bolle et al. 2002, p.2735). The authors argue that this method could be applied to all biometrics. See Figure 2.5 for an example using face biometrics.

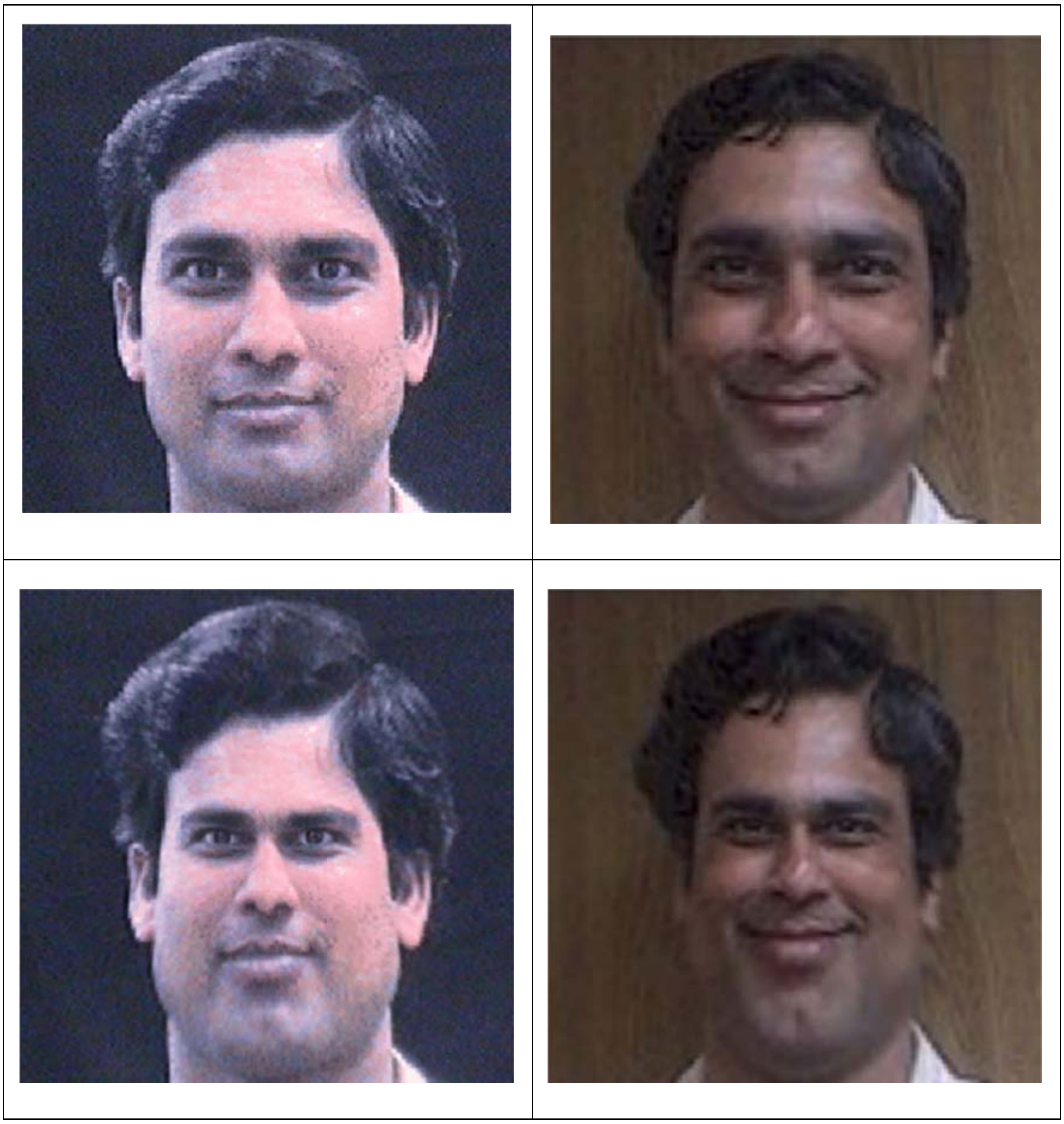


Figure 2.5: Example of "cancellable biometrics", using facial images. The images in the top row are photos of the same person. The images in the bottom row have been distorted in the same manner; the bottom images appear similar to the human eye but would be recognized by a computer as a biometric match (Bolle et al. 2002)

Another recent technical innovation attempts to improve the accuracy of facial recognition software, which is notoriously shoddy, by "averaging" different facial images of the same individual (Jenkins & Burton 2008). Automatic facial recognition systems often cannot recognize a face from all angles or with the many variations in day-to-day appearance that are necessary for such technology to be successfully implemented on a large scale. Errors frequently occur. Image averaging would theoretically solve this problem by determining identity from a software-produced composite of several images, instead of just one. This stabilizes the image of the face, removing aspects of images that are not diagnostic of identity (such as shadows and pose). Averaged images ostensibly capture the essence of a person's face while improving its machine-readability. In their 2008 article in *Science*, Jenkins and Burton claim 100% accuracy in their tests. Figure 2.6 exemplifies this technique using images of Bill Clinton.

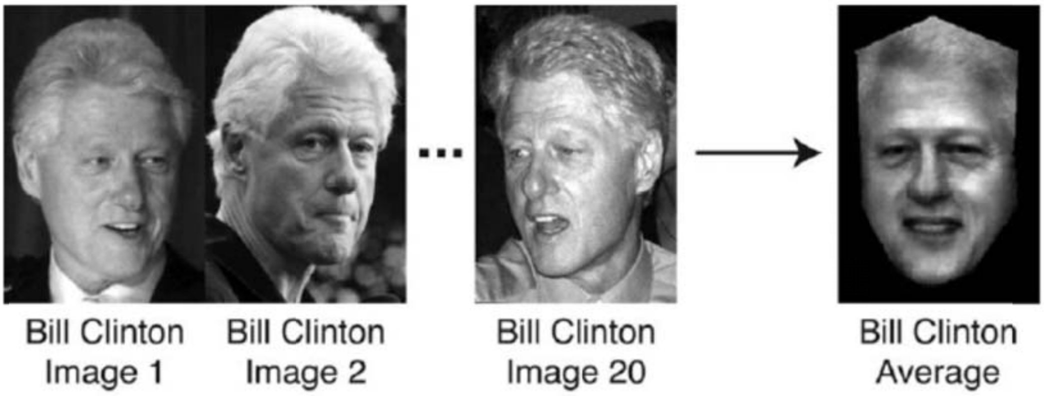


Figure 2.6: Process of "averaging" Bill Clinton's face to make it more machine-readable (Jenkins & Burton 2008)

## Multi-modal biometrics

It is widely reported in the technical literature that the systems that use multiple (multi-modal) biometrics for recognition are more reliable than systems that use only a single (uni-modal) trait (Jain & Ross 2004; Lazarick 2005). It is said that multiple, distinct modes of biometrics can be combined to resolve the various problems that affect biometric systems. Such problems include hacking (Faundez-Zanuy 2004) – having to hack multiple biometric sensors is more difficult than hacking just one; spoofing (Matsumoto et al. 2002) – multi-modal systems increase the volume and difficulty of the forger's travails; and the non-universality of particular biometric features in a population (Jain & Ross 2004, pp.37-38). Thus, someone without hands who is obviously incapable of providing fingerprints might present her/his irises to a biometric reader instead, so long as both options are available.

Multi-modality has also been heralded as a pro-privacy innovation. Faundez-Zanuy argues that certain privacy concerns may be resolved by "using a multi-modal biometric system, where the user can freely decide between several biometric identifiers, and reject the system that he considers may reveal private information" (2005, p.15). This, of course, assumes a degree of choice in the operation of the systems, and that the user knows enough to make a sound judgment about which system is less vulnerable than the alternatives. Making some biometrics optional for cultural or religious reasons, for example, would also have an impact on the performance and security of an identity system, as not all biometrics perform the same, nor are they equally immune to hacking.

Technical research on multi-modal biometrics continues. The apparent solution to the limitations of biometrics is to collect and use more of them.

However, added volume begets added complexity, and its lifelong companions: vulnerability, the potential for privacy violations and identity fraud, and other forms of exploitation. Given the well-established imperfections of biometric systems discussed above – technological error, vulnerability, and trade-offs that affect the accuracy of systems – the prospect of buttressing biometrics in with more biometrics raises the specter of trying to solve a problem by expanding, emboldening, and invigorating the problem itself; but is more always better?

## 2.3 Biometrics in the social science literature

Apart from the technical writings, another major category of literature is a rapidly expanding corpus of social science scholarship on biometrics. Within this broad category of research I include those accounts that emphasize sociological, political, ethical, cultural, or economic issues pertaining to the general use of biometrics in society and the implications of biometrics-based identity systems.

We might begin by considering work by van der Ploeg (2003), inspired by the science and technology studies (STS) tradition, on how biometric technologies are strategically portrayed by different actors in public debates. While van der Ploeg is primarily concerned with the privacy component of portrayals of biometrics (i.e., whether they are a violation or enhancement of privacy), her arguments can be applied to a broader, more meaningful discussion about the characteristics or values of biometrics. Instead of taking a side in the privacy debate, van der Ploeg aims to understand how differing public assessments of biometrics contribute to their continuous social construction. She argues that

> Such diverging assessments of biometric technology involve different conceptualizations and constructions of the technology in terms of its delineation as a stabilized object. The presumed nature of the technology varies, first, according to the imagined, assumed, feared, or hoped-for practical and material configurations of which the technology will become part, and, second, it varies according to where the boundary is drawn between the technology as a stabilized object and the contingent environment in which it is situated. (2003, p.88)

She observes that there is a politics to the conceptualization of biometrics (2003, p.99), for those who view the technology as an embryo of contingency – an ongoing work in progress – and also for those who see it as a stable set of artifacts, products, specifications, and properties – as something ready-made. Van der Ploeg argues that the perceived possibility of intervention and influence in a technological trajectory varies depending on the degree to which a technology is perceived as stable, and as well as on how people (such as activists or government officials) attribute agency to a socio-technical network (2003, p.100).

> A construction of technology stressing human agency and the heterogeneous nature of technological practices and developments is more enabling and empowering for those wanting to influence and steer the direction of technological development, whereas the reified version of technology, with its attribution of agency to technology rather than people or other causal factors, renders it a deterministic force happening upon

> us and to which any attempt to resist (or support as the case may be) appears futile. (2003, p.100)

One might worry that this sort of interpretive flexibility about biometrics (cf. Pinch & Bijker 1984) leaves the technology insusceptible to evaluation, criticism, or political engagement. Indeed, this is a classic dilemma in science and technology studies. Yet van der Ploeg argues that “the extent to which a certain technology can be evaluated, criticized, or even talked about, depends to a significant extent on the degree to which it can be identified as a stable object, or fixed practice” (2003, p.100). She stresses that the reification of a particular stabilized form of biometric technology, while temporarily sidelining important complexities, does facilitate meaningful discussion about it. She appears to be advocating a sort of local or case-based assessment of biometrics, avoiding general, hypothetical debates about the technology. These initial points on the politics of theorizing biometrics lead us into diverse analyses and critiques of biometrics by social scientists.

## Biometrics and identity: the machine-readable body

One such critique, offered by van der Ploeg herself (1999), concerns the philosophical relationship between the body, biometrics, and identity. She argues that the use of biometrics prioritizes the body in matters of identity, identification, and information technology. The body becomes the ultimate source of truth, supposedly containing a complete record of who we are and what we intend to do.

There is an important and unresolved empirical debate about whether biometrics are qualitatively different from other means of bodily identification. We have always relied on the body to help us recognize friend or foe. For example, there is a long history of the police branding criminals, thereby tattooing a social condition and a personality trait directly onto the body for all to see forevermore. And there is, of course, the spotted history of anthropometry, a system of criminal identification devised by Alphonse Bertillon in the late 1800s, which relied on various “scientific” bodily measurements and markers (cf. Lyon 2001, pp.291-292). Nose measurements and tattooing in Nazi Germany provide another example in the ugly history of biometrics. Torpey argues that the difference between these techniques and new methods lies in the degree of sophistication and reliability.

> Techniques for ‘reading off the body’ have become more and more sophisticated over time, shifting from unreliable subjective descriptions

> and anthropomorphic measurements to photographs (themselves at first considered unreliable by police), fingerprints, electronically scanned palm-prints, DNA fingerprinting, and the retina scans dramatized in the recent film version of *Mission: Impossible*. (1999, p.17).

Indeed, modern biometrics rely on computers and information technology to identify subjects. Van der Ploeg argues that the academic literature on identity inadequately theorizes biometrics, for the centrality of the body in biometrics and the embodied nature of subjectivity are rarely taken into account. She stresses that we must better understand "what *kind* of body the biometric body is" (van der Ploeg 1999, p.43, emphasis added). She believes it is a body that does not and cannot exist independently of technology.

> Unlike the body rendered knowable in the biomedical science, biometrics generates a readable body: it transforms the body's surfaces into digital codes and ciphers to be read by a machine… [T]he meaning and significance of the biometric body will be contingent upon context, and the relations established with other texts… [W]e might say that the contexts giving meaning to biometrics are constituted by the practices it is part of, while its meaning in an intertexual sense will be brought about by the data to which it is going to be linked electronically (van der Ploeg 1999, p.43).

Thus one may argue that, in this sense, modern biometrics are different from previous, non-computerized methods of bodily identification. Biometrics easily link the body to dispersed sets of information stored across innumerable databases; only then do digital biometrics 'mean' anything.

## Biometrics privacy-enhancing or privacy-eroding?

If people's primary identity in a biometric society must be verified by machines in order to be 'true' – if we are not ourselves without mechanical confirmation that our codified bodies match some previously recorded information – then repeated validation of our corporeal specifications becomes an increasingly important activity in social life. This is a process of expansive and expanding disclosure. It is for this reason that several authors have considered the relationship between biometrics and privacy and civil liberties (Davies 1998; Zorkadis & Donos 2004; Johnson 2004; Anonymous 2007a; Liu 2009; Sprokkereef & De Hert 2007). These articles usually discuss whether and how biometric systems threaten privacy. More often than not, these are broad-stroked critiques of biometrics, which are removed from context and ignore the important contingencies and local realities that van der Ploeg implores us to consider when assessing the technologies. We can understand the central thrust of this branch of the literature by reviewing two of its more well-known contributions in depth: namely the writings of Clarke (2001) and Alterman (2003).

In his overview of biometrics and privacy, Clarke (2001) argues that biometric technologies threaten to remove society's last remaining protection against governments and corporations: their systemic inability to reliably and consistently identify citizens and customers, respectively. If biometric identification ever becomes a universal and normal requirement of everyday life, he argues, this final bulwark would collapse. Clarke outlines ten specific threats to privacy posed by biometric technologies.

1. *Privacy of the person*. Biometrics necessarily involve the collection of information of the person, which Clarke argues is particularly sensitive.
2. *Privacy of personal data.* Collecting biometrics in conjunction with other personal data enhances the risk of increased control over a population.
3. *Privacy of personal behavior*. Monitoring people's movements and actions through biometrics increases the transparency of their behavior to organizations. This fear is about biometrics being the missing link in a ubiquitous surveillance society.
4. *Multi-purpose and general-purpose identification*. Because biometric identification schemes are expensive, organizations are motivated to share costs by using the systems for multiple purposes, thus threatening privacy through increased data-sharing.
5. *Denial of anonymity and pseudonymity*. With the advent of biometric technologies, the capacity to associate identities with previously anonymous or pseudonymous activities is increased.
6. *Masquerade*. Imposters might produce means to trick biometric devices.
7. *Permanent identity theft.* While masquerading is a single event, a thief could theoretically pose as another person indefinitely. The aura of accuracy and reliability surrounding biometrics would make it difficult for rightful owners to reclaim their identities.
8. *Automated denial of identity*. Using biometrics, organizations could deny those who are deemed suspicious access to certain facilities or services, based on any characteristic they choose to exclude.
9. *Effect on freedom and democracy*. The use of biometrics runs counter to the freedoms and liberties of an open and democratic society.
10. *Dehumanization*. The use of biometrics can be seen as treating human beings as simple objects, manufactured goods or livestock, with no other distinguishing or individuating characteristics of relevance other than their bodies.

In response to these perceived threats to individual privacy, Clarke considers five potential safeguards against biometric intrusion. The first of these, self-regulation, he discounts as insufficient considering the current business and security environment in which governments – both traditionally repressive and sophisticatedly security-conscious types – seek out vendors to supply them with technologies to serve their purposes. Suppliers almost never object on principle. Or worse, as Lyon argues, technologies companies are actively pursuing governments to pitch their wares. These are what he calls ‘card cartels’ (Lyon 2009, chap.3). Equally trivial are attempts to outline an industry code of conduct. Another safeguard against malignant uses of biometrics could be a compulsory social impact assessment. According to Clarke, this would require:

- full public disclosure of the technologies of interest and their envisaged applications;
- a suitably funded social impact analysis;
- publication and consultation of results;
- active public participation during the design phase; and
- in-built controls.

Clarke seems to envision these impact assessments as pre-emptive mechanisms to mitigate the privacy concerns of emerging biometric applications, and to do so in the full light of day. However, as he notes, very few countries require such social impact assessments. In the United States, the Office of Technology Assessment served this function until 1995, when it was disbanded as part of government cutbacks.

A third potential safeguard – existing privacy and data protection law – also fails to satisfy Clarke. Such generic laws are “far too naïve and weak to represent any kind of curb on the explosion of biometric technologies” (Clarke 2001). Alternatively, legislators might choose to regulate biometrics specifically, based on a number of principles. These are:

- the storage of encrypted biometric templates, instead of actual biometric images (a version of this recommendation was included in an influential government-initiated report on identity assurance in the UK (Crosby 2008, p.7));
- the prohibition of centralized storage of biometric information;
- privacy-sensitive design standards for biometric devices;
- the legal prohibition of manufacturing or using non-compliant devices;
- a practice of continuous compliance auditing; and
- two-way device authentication (so that information is not transmitted to devices without users’ knowledge).

Failing this, Clarke argues for a moratorium on the application of biometrics until a comprehensive set of design requirements and privacy protections is in place. However, this moratorium has yet to materialize, and, considering the current state of biometric technologies across the globe, we would be wise not to expect its arrival anytime soon.

Alterman (2003) distinguishes between two “ethical” issues related to biometric identification, both concerning privacy. He asks: Are biometrics immune to the privacy vulnerabilities that plague other forms of identification? And are there any privacy concerns that are specific to biometric identification?

In reply to the first question, Alterman considers four arguments which are often put forth to defend biometrics against accusations of privacy–infringement.

1. *Technical limitations argument*. Large user populations mean that the technology will often fail in practice.
2. *Balkanization argument*. A lack of standards and poor system interoperability mean that data remain localized and restricted.
3. *Co-operation argument.* Abuse is difficult because biometric technology typically requires the co-operation of users.
4. *Security argument*. The algorithms for biometric templates are secure because technology vendors have a vested commercial interest in protecting their proprietary knowledge. This is basically the “security through obscurity” argument, which has repeatedly been criticized (see Mercuri & Neumann 2003).

Alterman holds that the technical limitations argument is weak because biometric systems are subject to “rapid technological advances” (p.141). We cannot rely on biometric systems remaining faulty forever. Likewise, the industry is slowly de-balkanizing, especially with organizations like the International Civil Aviation Organization (ICAO) making great efforts to harmonize standards (Hosein 2004) and the US National Institute of Science and Technology promoting common file formats to all vendors.

The co-operation argument is more convincing; in their current state biometrics still, by and large, require user co-operation to work properly. This is changing, however. New innovations like automated facial recognition software are gradually entering the market (National Police Improvement Agency 2006), and some vendors are promising to deliver systems that perform iris recognition “at-a-distance” or “on-the-move” (Sarnoff Corporation 2010), without user consent or co-operation. Gait recognition, still a zygotic technology in terms of its large-scale deployment, would also defeat the co-operation argument if successfully developed in the future.

Alterman also finds faults with the security argument: that biometric technologies are secure because vendors have a proprietary interest in protecting their assets. He imagines a variety of nightmare scenarios involving the leakage of biometric data:

- The unauthorized and unethical sale of biometric data by those responsible for overseeing the databases;
- a data breach resulting from a technical error that releases decrypted biometric data from a corporate network;
- a disgruntled member of the IT staff altering data so that colleagues’ or customers’ biometrics are rejected by a system;

- law enforcement agencies demanding the disclosure of biometric data and the associated algorithms from private companies; and
- computer hackers gaining access to sensitive data and posting them online (Alterman 2003, p.142).

Alterman thus concludes that biometrics are, in fact, not immune to the normal threats to information privacy that face other personal data.

Having shown that biometrics are probably vulnerable to the same privacy concerns as other identity technology, Alterman moves on to biometric-specific privacy concerns: privacy issues brought about by biometric technologies that go above and beyond the complex vulnerabilities of normal identification. Viewing the concept of privacy as control over how and when information about us is presented to others, Alterman picks up on key three dimensions in particular: property, embodiment, and self-representation. He claims that as moral agents we have a greater interest in controlling representations about our body as opposed to indexical data (such as identity numbers, home addresses, etc.), as bodily information has an internal relation to the embodied person.

A complicating factor to such an argument, however, is photography. Alterman claims that while photography has its own share of important ethical issues (pornography and video surveillance among them), biometrics are qualitatively different from photographs because they “are unique to the individual and positively identify that individual, within an ever larger population as the technology improves” (p.145). He claims that biometrics are more irreversible, more reliable, and more efficient than photographs, and so they are logically distinguishable and present their own unique set of ethical and privacy problems.

The problem with this and similar assessments is that they uncritically accept what is a relatively arbitrary distinction between photography and biometrics. For example, face biometrics are, in many ways, simply digitized versions of facial photographs, subject to certain data standards. Iris biometrics rely on photos of the eyes; fingerprints are visual representations of information from the fingers. Granted, information technology plays an important role in contemporary biometrics implementations, without which large-scale systems would be impossible. Perhaps this helps to distinguish between photography and biometrics but in some cases a ‘biometric check’ might not require any computing technology at all, such as when a border agent compares a passport holder’s face with the image printed on the document. For now, rather than try to establish decisively the differences between ‘traditional’ photography and ‘modern’ biometrics for the sake of grounding an ethical critique, it suffices to acknowledge this conceptual tension. It will re-emerge in later sections, as actors in this case study strive to makes sense of biometrics.

## Biometrics and the politics of security

Since identification technologies are most often used in international and domestic security contexts, biometrics feature occasionally in academic writing on international relations and political science: Hosein (2004; 2005) critically analyzes the international mechanisms through which policy decisions regarding biometric travel documents are being made and the politics behind the development of the US-VISIT biometric program; Zureik and Hindle (2004) address governance mechanisms relating to biometrics; Amoore (2006) and Epstein (2007) tell about biometrics and borders; Liberatore (2007) details the processes of pluralistic debate and deliberation about biometrics in the EU; and Gates (2005; 2006) explores the connection between biometrics and security from a cultural studies perspective. Here I review one of her recent articles.

Gates (2006) explores the emergence of facial recognition technology (FRT) as a hi-tech solution to the difficult security problem of international terrorism following the attacks of 11 September 2001 (9/11). She asks why biometric technologies such as FRT were deemed a solution to these problems. How did they arrive on the political agenda? She also explores what had to be neglected or glossed over about facial recognition technology for it to be seen as an appropriate security solution to the complex and multi-faceted problems of combating terrorism (p.418).

Gates identifies and traces three main factors that contributed to the rush to adopt FRT immediately after 9/11. First she considers the “securitization of identity” (Rose 1999, p.240), which preceded 9/11 by decades, and was escalated suddenly in a virtually unprecedented embrace of high-technology initiatives, including the implementation of identification technologies such as biometrics. Identity was seen as a problem in need of a technological solution. Technology companies were more than willing to sell their wares as a key component of the new standard of security being implemented, and the press gave considerable coverage to the topic of biometrics and to those groups pitching solutions. Gates argues that rather than just being offered as a solution to identifying terrorists, these technologies soon served to define the concept of ‘homeland security’, with “political and governmental problems of security provision [being] defined in technical terms, tightly articulated to specific technical solutions” (Gates 2006, p.423).

Second, as biometrics vendors promised that FRT could identify suspect individuals at a distance and in real-time, government homeland security objectives soon began stressing that the prevention of future attacks relied on the ability to identify terrorists at a distance and in real-time. That is, the solution began to define the threat. Some vendors and politicians even went so far as to argue that automated facial biometrics could have prevented the

9/11 attacks (Gates 2006, p.424). However, such proclamations ignored the very experimental nature of the technologies in question, and also eschewed “a realistic accounting of tensions and contradictions that such a technology would have to embody in order to work effectively in practice” (Gates 2006, p.426). What is worrying for Gates is that these technologies can also be seen as the latest manifestation of ongoing attempts to tame the fundamentally unstable social construct of individual identity and stabilize it as a simple constant.

Finally, she picks up on the rhetoric surrounding ‘the faces of terror’. Political rhetoric often describes terrorism as an asymmetric, unidentifiable threat. Yet, following the attacks of 9/11, the media abounded with mug shots of the accused. These and other images of suspected and accused Islamic terrorists led to the impression that terrorism is a visible quality. Abu Hamza al-Masri, the former imam of the Finsbury Park Mosque in London, was one such symbol of supposedly visible evil. His portrait – glass eye, hook hand and all – was almost invariably appended to news items reporting on the vitriolic sermons that ultimately landed him in jail. These images were seen to embody the previously amorphous and unidentifiable terrorist threat by giving it a more or less fixed image, fetishizing it as something that could be pinpointed and prevented with the right technology: in this case, facial recognition systems. Gates’ contribution is to document how policy problems and their supposed technological solutions are not sequentially ordered, but are rather subject to a chicken and egg dilemma of the most intransigent kind.

## Biometrics as digital surveillance

Lyon provides us with important academic work on biometrics and their potential surveillance capacities. He sees the use of biometric technologies, particularly in identity documents and as part of larger identity systems, as a means of “social sorting”. With biometric ID cards on the mind, Lyon argues that

> [n]ew ID cards are part of a large-scale trend towards ‘social sorting’—classifying and profiling groups of people in order to provide different services, conditions or treatment. Specifically, new ID cards are intended to include those designated as ‘eligible members’ of nation-states and to exclude undesirable others. (Lyon 2004a, p.2)

In this sense, biometrics are a tool for executing an intentional process of categorization and discrimination. Lyon understands the increased uptake of biometrics as part of the erection of internal boundaries, or as he puts it, “ubiquitous borders” (Lyon 2004b), in which there is a perceived need to identify potentially threatening individuals and treat them differently.

Elsewhere, Lyon (2001) undertakes a social-historical account of biometrics as a means of bodily surveillance. While acknowledging that bodily surveillance is nothing new, he points out the subtle increase in the technological sophistication of modern biometric systems and the growing number of applications of biometric technology: from identifying potentially criminal individuals to categorizing and sorting general populations of citizens and consumers. Lyon contends that these technologies turn the body into a “password”, and make it both a site of surveillance and a source of surveillance data.

Arguably, the use of digital technologies like biometric identity systems represents a striking change in surveillance techniques. Analogue methods and technologies, such as the first generation of closed-circuit television (CCTV) cameras, are being replaced and upgraded with digital systems whereby information can be stored affordably and indefinitely and recalled and reprocessed based on a limitless number of discriminatory criteria. Elaborating this point, Graham and Wood (2003) critically explore the implications of digital technologies on the so-called “new surveillance” (Marx 1998; 2004). The digitization of surveillance is considered a significant development for two reasons. First, it facilitates the watching, prioritization, and categorization of people and things over great geographical spaces and without significant time delay (Graham & Wood 2003, p.228). This collapsing of space-time distanciation involves interconnecting and integrating databases so that various data can be stored and compared. Second, digitization facilitates the automation of sorting, identifying, prioritizing, and tracking subject populations, in terms of their bodies, behaviors, and characteristics. As a result, the role of the human operator in the surveillance mission shifts from direct watching and decision-making based on local cues, to the design, programming, management, and maintenance of pseudo-autonomous technological systems (Graham & Wood 2003, p.228). They argue that when the move to automation involves the incorporation of algorithmic software, further ethical questions arise in relation to the removal of human discretion from surveillance.

Graham and Wood review the use of algorithmic facial recognition software in video surveillance cameras. In spite of the historically poor performance of such systems in preventing and solving crimes, the authors observe that official justifications for the continued investment in and use of these systems now, more than ever, resort to arguments about how they can *deter* crime. And while Graham and Wood view these performance issues as important topics of debate, for them there is an even greater need for informed debate about the ways in which facial recognition systems and other biometric systems reinforce the categorization of certain socio-spatial risks such as high crime neighborhoods, known criminals, or ‘dangerous’ groups (p.237). They call for further research on the ways social and political assumptions become embedded into the algorithmic software that facilitates post-human surveillance.

Introna and Wood (2004) respond to this call in their investigation of the politics of algorithmic surveillance. Inspired by the work of Winner (1980), Latour (1991), and Introna and Nissenbaum (2000), they assert “that the silent nature of information technology makes it difficult for society to scrutinize it” (2004, p.184). Analyzing the ‘biases’ in the software algorithms of facial recognition systems, they show how certain ‘political’ values can be embedded into the biometric artifact itself, including, for example, a propensity to over-identify men compared to women, older people compared to younger people, and Asian and black people compared to white people (c.f. Givens et al. 2003). These biases resemble the aforementioned ‘anomalies’ in the recent NIST report on facial recognition, which was reviewed in the section on the technical research on biometrics.

Interpreting these anomalies, Introna and Wood argue that biometric artifacts cannot be understood in isolation, but rather as objects embedded within larger socio-technical networks in which their micro-politics may be multiplied and seized upon in a multitude of implementations and practices.

Last, drawing on feminist and post-structuralist theories in the social sciences, Ball (2005) develops a politics of resistance to biometric surveillance in the workplace. She wants to challenge the fixities assumed and engendered by bodily surveillance (2005, p.104). She argues that, by neglecting the body’s continuous reconstitution and inherent instability, proponents of biometric surveillance cannot justifiably defend digital surveillance as a source of authenticity and truth.

Ball offers strategies of resistance to what she clearly sees as a problematic practice, including "disrupting flows of information from the body to the information system, disrupting the time it takes to encode the body, coding the body in an alternative way, and moving the interface/boundary between the body and surveillance system" (2005, p.104). In practice, this might mean intentionally altering one's typing pattern to confuse keyboard recognition biometrics or devising ways of resisting drug tests given at the workplace. In closing, Ball concedes that bodily surveillance at the workplace or elsewhere need not always be viewed negatively. Rather it is when it goes unquestioned and unchallenged locally that such techniques of resistance become necessary (2005, p.105).

## Biometrics and social inclusion and exclusion

As with other questions related to the supposed values of biometrics, whether biometrics are inclusionary or exclusionary is ambiguous. Recall that researchers within the computer science tradition see biometrics as a means of reducing exclusion, particularly through multi-modal biometrics, with the hope that if enough different biometrics are enrolled in an identity system, everyone will be able to participate in it and redundancy will keep the system going if one biometric process malfunctions. Lyon, on the other hand, sees biometrics as a form of social sorting which is inherently exclusionary.

From Lyon's description of how biometrics affect social systems emerges obvious questions of ethics: is this exclusion morally justifiable? Wickins (2007) argues that it is unequivocally unethical, though he admits that with the increasingly widespread use of biometric technology, social exclusion is inevitable. Wickins understands social exclusion as "any unfair restriction or removal of access to the range of social goods and activities that other members of that society do, or could, take for granted" (2007, p.52). These goods and activities include healthcare and social security, among others. Among those most likely to be disadvantaged by the use of biometrics are people with physical or learning disabilities, people with mental illnesses, the elderly, people of certain races, people of certain religious groups and the homeless (2007, pp.50-51). He dismisses arguments in favor of biometric identity cards based on the idea that they promote the public interest, noting that "almost anything can be justified by saying that the rights of the many outweigh the rights of a few" (2007, p.52).

The problem, however, is that his ethical critique (and others like it) is technologically deterministic ("biometrics is a field whose time has come"

(Wickins 2007, p.46)) and ignores many important subtleties of biometrics. Wilkins speaks of biometrics as though they were a single thing, when in fact they are a series of different technologies and techniques that pose different scientific and ethical quandaries. This case study will expose many of these uncertainties and explore their policy and ethical implications.

## 2.4 Biometrics in the information systems literature

Somewhat predictably, the information systems literature on biometrics is dominated by research on user acceptance and surveys of public perceptions of biometrics. As previously noted in the review of the technical literature, the acceptance of biometric systems by targeted user groups is considered by many authors to be an important requirement for “successful” systems. It is believed that without user acceptance, perfectly functioning systems are doomed to fail. As technology acceptance is one of the more well-established streams of research within information systems, many projects have sought to identify these enablers and barriers to user acceptance. I will review these acceptance studies shortly, but first I summarize the modicum of exceptions to this research trend.

Of the few studies within the field that do not focus on end-user acceptance, work by Scott et al. (2005) that explores the applicability and potential future use of biometrics for e-government services is particularly relevant to the current case study. They examine the attitudes of management personnel within the Irish Department of Communications, Marine, and Natural Resources, who are responsible for making policy decisions about biometrics. In particular, Scott et al. are interested in managerial attitudes towards the feasibility of using biometrics to deliver e-government services. They find that officials consider the accuracy, strength, effectiveness, and usability of biometrics, as well as privacy, trust, and international developments, as important factors influencing their possible deployment (2005, p.280). Scott et al. call for further research on citizen acceptability and citizen trust in biometrics, noting that such studies would significantly enhance current public debates (2005, p.283).

Another notable information systems study comes from Davis and Hufnagel (2007), who take a different tack. Their research is on the ways in which the automation of expert fingerprint analysis within forensics labs changes the nature of work and related organizational dynamics. They explore how new, complex systems with sophisticated search and match algorithms (what they describe as the “ghost in the machine”) affect analysts’ perceptions of their work, the distribution of tasks and roles within labs, and organizational values and norms.

Finally, while both Clarke (1994a) and Otjacques et al. (2007) discuss biometrics in their studies of human identification in information systems and EU public organizations' management and sharing of identity data, respectively, neither study focuses on biometrics in a substantial way.

## Acceptance and perceptions of biometrics

Returning to the literature on user acceptance and perceptions, different types of study focus on what has been termed the "people" side of biometrics (e.g., Chau et al. 2004, p.1). The technology acceptance model (TAM) (Davis 1989) and its revisions (TAM2) (Venkatesh & Davis 2000) influences much of this literature. A lot of it lacks a theoretical grounding. Virtually all of it is survey-based and hypothetical in nature. Respondents are typically asked to opine about biometrics without context or substantial engagement with the technologies in question.

Deane et al. (1995) appear to have conducted the first study of user acceptability of biometrics, based on a questionnaire completed by workers from the banking sector and university administration. In this initial study, biometric systems were perceived as less acceptable than traditional password-based security systems. Behavioral biometrics were considered less acceptable than physiological ones.

Since then there have been a series of these types of study, mostly involving surveys of university students, staff, or faculty. Table 2.7 summarizes these articles in terms of their theoretical focus (or lack thereof) and methodological approach.

| Author(s) (Year) | Title of article | Theory | Method |
|---|---|---|---|
| Deane et al. (1995) | Perceived acceptability of biometric security systems | None | Survey with 76 respondents |
| Furnell et al. (2000) | Authentication and supervision: A survey of user attitudes | None | Survey with 175 respondents |
| Clarke et al. (2002) | Acceptance of subscriber authentication methods for mobile telephony devices | None | Survey of 161 mobile subscribers |
| Ho et al. (2003) | Biometric authentication adoption issues | Technology acceptance model | None |
| Chau et al. (2004) | Biometrics acceptance – perceptions of use of biometrics | Technology acceptance model | None |
| Moody (2004) | Public perceptions of biometric devices – the effect of misinformation on acceptance and use | None | Survey with a sample of 300 |
| Weerakkody (2006a) | A comparative analysis of opinions of American, Australians, and Malaysians on the use of biometric devices in workplaces for security and monitoring of worker productivity | "Critical theory" | Survey with convenience sample of 230 Australians, 408 Malaysians, and 300 Americans |
| Weerakkody (2006b) | A comparison of Australian and Malaysian views on the use of biometric devices in everyday situations | "Critical perspective" | Survey with the same sample of 230 Australians and 408 Malaysians |

| Author(s) (Year) | Title of article | Theory | Method |
|---|---|---|---|
| Ng-Kruelle et al. (2006) | Biometrics and e-Identity (e-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation | Organizational theory (Hofstede) | Survey of 269 MBA students from the UK, Germany, Spain, Greece, and Denmark |
| James et al. (2006) | Determining the intention to use biometric devices: an application and extension of the technology acceptance model | Technology acceptance model | Survey of university faculty, staff, and students |
| Perakslis and Wolk (2006) | Social acceptance of RFID as a biometric security method | None | Survey of 141 university students |
| Heckle et al. (2007) | Perception and acceptance of fingerprint biometric technology | None | Experiment involving 24 participants |
| Jones et al. (2007) | Towards understanding user perceptions of authentication technologies | Technology acceptance model | Survey of 115 university students |
| Furnell and Evangelatos (2007) | Public awareness and perceptions of biometrics | None | Survey with 209 respondents |

Table 2.7: Summary of IS literature on user acceptance and perceptions of biometrics

An example of one of the TAM-inspired studies of biometrics is by Ho et al. (2003), who develop a biometrics acceptance model in which the traditional TAM concepts of ‘perceived usefulness’ and ‘perceived ease of use’ are modified to better fit what they deem to be the particularities of biometric systems. Based on a reading of the literature, they identify a number of theoretical factors that could potentially contribute to perceptions of usefulness and ease of use. Figure 2.8 shows the resulting acceptance model (2003, p.8).

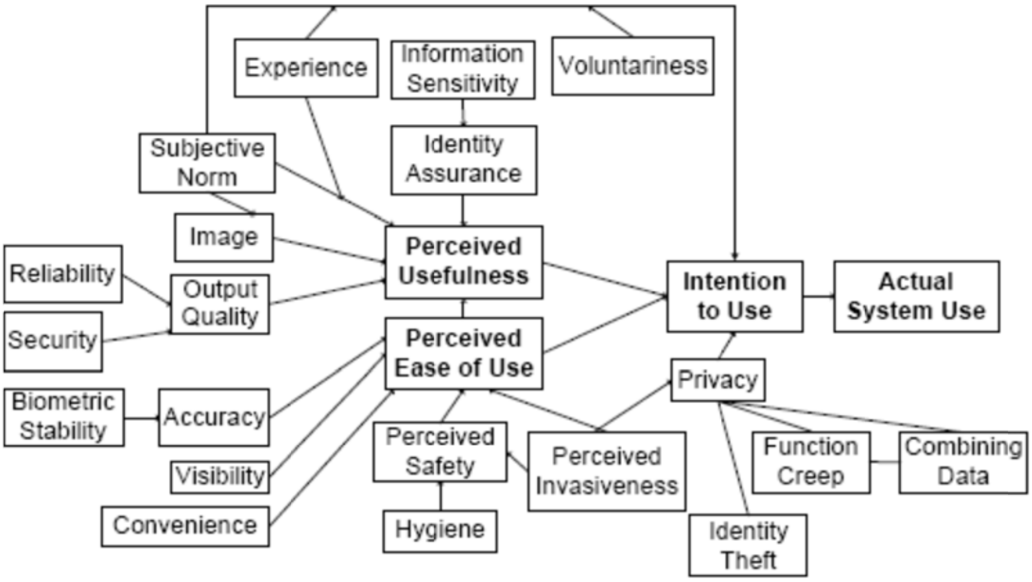


Figure 2.8: Example of a biometrics acceptance model (from Ho et al. 2003)

One of the principal aims of these analyses of biometrics acceptance is to understand user resistance in order to overcome it, often through “better” marketing and information campaigns to “educate” uninformed consumers about the benefits of biometrics (Chau et al. 2004, p.2). There is a normativity to many of these studies, which view resistance to biometrics as a problem or as irrational – the result of misunderstandings about the technology that ought to be corrected.

One grapples to make sense of the sometimes-contradictory findings of the different studies. While some of them conclude that most users are ready to accept and use biometrics (Ponemon Institute 2006), others note ongoing reluctance and potential resistance (Moody 2004). Some try to confront the unclear and contradictory nature of public opinion regarding these issues (Moody 2004; Heckle et al. 2007), noting that understanding context and how exactly biometrics will be used by organizations is important. However, the instrumental view of public acceptance, perceptions, and understanding adopted in these studies, which tend to treat context as an abstract variable rather than an inextricable part of the technologies and the attendant processes and practices, leaves one wanting. These typically one-off studies seek to understand views about biometrics at a certain point in time, without considering how such views emerge from, and are influenced by, recent events, political dynamics, and other contextual factors. Some of these studies also acknowledge that many people are simply unaware of the term and concept of biometrics, but they do not explore philosophically what this lack of awareness means in terms of public acceptance.

Whereas most IS studies of biometrics have failed to engaged with the richness of the contexts into which biometrics are being deployed, this study will directly and deeply engage the context-based public discourses that led up to and accompanied proposals for a national biometric identity program in the UK.

## 2.5 A research opportunity

The review of literature on biometrics has highlighted a number of strengths in the academic research, including a considerable appreciation of their *potential* benefits and risks. It is believed that, if designed, implemented, and managed properly, biometrics can be used to alleviate many challenging problems related to citizen and consumer identity. The threat of identity theft, for example, is one such problem area. It is commonly argued that identity-related fraud could be reduced with the appropriate use of biometrics. But of course, this is not guaranteed. Others claim that using more data such as biometrics is not the answer and that we are too quick to embrace technological solutions when confronted with complex social challenges.

In reviewing the literature on biometrics, I exposed shortcomings that this project seeks to address. For example, the vast majority of the technical research on biometrics is largely experimental in its design and testing, and leaves much to be desired in terms of understanding how biometric systems emerge within real-world contexts, the motivations behind their use, how they ‘come to life’ discursively (or socio-materially (Orlikowski & Scott 2008; Orlikowski 2010)), and how they take on particular social meanings (whilst resisting others).

This is more than a problem of accurately simulating real-world environments in trials of biometric systems (which is, no doubt, a daunting task). Rather, the experimental nature of these studies precludes the emergence of the full range of meanings and discourses that technologies such as biometrics afford when launched in different contexts. These are organizational or societal contexts where diverse values, politics, and expectations about the future affect decisions about what technologies to pursue, for what purposes, and involving whom, to name just a few of the many important issues.

A shortcoming of the sociological and ethics literature on biometrics is that, in critiquing the technology which is often in a prospective or unsettled form, it treats it as a reified, accomplished thing whose outcomes are well-defined and predictable. Indeed, it is often based on, as Alterman admits in his ethical critique, “the ideal assumption that biometric systems can uniquely identify an individual within an arbitrarily large population” (2003, p.144), without questioning these enormous assumptions.

This literature rarely sees the technology itself as deserving much attention. It largely overlooks the important differences between different types of biometric system (fingerprint versus iris versus facial recognition versus DNA, etc.) as well as within the same types of system (e.g., still-face recognition systems as opposed to recognition-from-video systems; or single fingerprint biometric systems that store only templates verses ten-fingerprint systems that record original images). Authors writing in this tradition tend to lump these different technologies together under the umbrella of ‘biometrics’ before launching into their critique.

Indeed, this tendency to take for granted the information technologies that are central to so many modern policy initiatives is not unique to the case of biometrics. It is emblematic of many sociological and criminological critiques, particularly within the emerging field of surveillance studies. Studies of surveillance largely neglect or fail to take account of the important role that technological artifacts play in both the experience of surveillance and the organizational dynamics of surveillance work. However, this tendency extends far beyond surveillance policies and certainly applies to most IT-leveraged policy (Whitley & Hosein 2010).

Finally, this sociological literature also tends to neglect the important details of the assorted contexts into which biometric technologies can be implemented and used. For example, many sociological and ethical critiques do not distinguish between the issues that arise around biometric systems mandated for use at the workplace and those that accompany biometric schemes that form part of standardization initiatives for international travel documents.

Schools and nurseries are yet further contexts where these issues and debates take on a different character.

We also found that previous research on biometrics originating in the field of IS was not without shortcomings either. The field's historical preoccupation with technology acceptance models (TAM) means that, to date, the research questions posed by IS researchers interested in studying biometrics have been limited in scope, mainly focusing on end-user acceptance. This literature aims at better understanding what impedes users from accepting biometrics so that these impediments may be overcome and biometric technology more widely adopted.

As discussed, there is a potent normativity to these studies, in which adoption is viewed as a good thing and resistance something that can be designed out or regulated. While certain exceptions to this trend in the literature do exist (e.g., Scott et al. 2005; Zviran & Erlich 2006; Davis & Hufnagel 2007), the information systems field has largely been fixated on acceptance concepts and has underestimated and understudied other social dynamics.

Such restrictions to the research questions posed by information systems researchers naturally influence their selection of methodology. To take a particularly egregious example, a study of perceptions and user acceptance of fingerprint technology describes its research design and methodology and as follows:

> A laptop PC was equipped with a Microsoft Fingerprint Reader (Model DG2-00002). *The participants were informed that their fingerprint data was not being captured, but that they should role-play as if it was*. The fingerprint reader lit up when it was used. *The participants were told that this simulated data capture*, and they could then press the 'submit' button on their screen to complete their transaction. (Heckle et al. 2007, p.1, emphasis added)

It is the artificial makeup of such studies, where role-play and simulation are used as substitutes for a realistic engagement with the technologies, which detracts from their academic value. These types of study share some of the limitations of the experimental research projects discussed above in that, by design, they are removed from real-world contexts of use – and, as I will discuss later, it is these contexts that make the difference.

Likewise, most studies of user perceptions of biometrics seek to understand attitudes toward the technology without taking into account how such views are formed *in situ* and are influenced by changing applications and shifting contexts (cf. Sasse 2007). It is one thing to have a general opinion about fingerprinting, considering that most people view it as something that only criminals undergo. However, such opinions are likely to change when everyone is obliged to forfeit their fingerprints to some authority, perhaps with minimal personal benefit in return.

These IS studies regularly black-box biometrics, viewing them as a settled issue, whose stability and meaning is unproblematic. However, many biometric technologies are still in their infancy, especially in terms of large-scale roll-outs for everyday use, and thus measurements of perceptions or attitudes toward biometrics, when devoid of context and an appreciation of the ongoing uncertainties around the technologies, suffer real limitations.

Therefore, from an IS perspective we must ask whether the concept of 'acceptance' is sufficiently meaningful or even helpful in the current research context. This requires that we first ask *who* would have been accepting the biometrics in this case. This is not so straightforward. Was it the policy-makers and politicians responsible for establishing the NIS? The civil servants responsible for making it a reality? The government departments and other organizations (e.g., banks or employers) that were expected to incorporate the identity system into their customer or employee identification and authentication processes? The citizens and foreign nationals who were expected to enroll in the system and use it? Or some other set of actors? This initial consideration of actors suddenly complicates the question of acceptance, showing that in practice it is many different actors who could potentially accept the technology, in very different ways, and based on varying motivations.

Additionally, in a context where the collection and use of biometrics was legislated as part of a larger national identity system that, at some point, could have become mandatory, we must ask whether ‘acceptance’ is an appropriate analytical term. The focus on biometric acceptance is somewhat misleading and unhelpful in the current case for it is not clear that acceptance was a real option for certain actors (such as those non-EEA foreign nationals whose data was collected or the airport workers who were ‘encouraged’ by management to apply for identity cards). Can we speak frankly of biometric acceptance, which assumes a measure of choice both in the enrollment stage and in the subsequent use of biometrics, when the uptake by these users was more akin to compulsion than adoption?

The cases of US-VISIT and the United Arab Emirates’ iris recognition border-crossing system (both of which are compulsory for certain nationalities and must be used if one wants to enter the United States or the UAE, respectively) involve similar issues. Related proposals for national identity systems in countries such as India and Mexico, where the respective governments are currently pursuing policies for the mandatory collection and use of multiple biometrics including iris recognition technology, add to the increasingly international character of these debates in which it is common to hear that, by and large, the public “accepts” these technologies – whatever that means.

There is also the ongoing situation in which the ‘acceptance’ of biometrics is facilitated through their inclusion in new electronic passports, resulting from policy decisions that are made at a transnational level by policy actors who circumvent traditional deliberative channels (Hosein 2004). As before, the concept of acceptance does not fit well here. It suffices to say that it is a problematic term.

Yet the issue of acceptance is not totally absent. The concept might have some meaning and utility in this case insofar as it motivated people’s choices about whether to enroll in the Scheme when it was first launched in targeted geographical areas, or to the extent to which it helps to explain the ongoing resistance to the former proposals. Or, by exploring certain *discourses on acceptance*, among others, we might be able to understand the role that talk about the public played in the failed roll-out of the Scheme.

What I am suggesting is that in contexts such as these it may be more interesting and more fruitful to study how public discourses on the proposed biometric technologies developed over time within a particular socio-political reality. In other words, if we shift the analytical focus from the instrumental studies of user acceptance to which mainstream IS research has grown accustomed, to the discursive unfolding of biometrics in early 21st century Britain, then we may better understand how such technological innovations enter the public consciousness and come to life (or fade) before questions surrounding acceptance begin to make sense.

This raises a more fundamental question, motivated by the qualitative information systems research tradition (cf. Myers 1997) and inspired by developments within science and technology studies (e.g., Sismondo 2009), of *what* is being accepted by these actors? In other words, if we place the technological artifact front and center and explore what goes into giving it meaning and shaping our understandings of it, then we can study the technology’s trajectory through the various discourses that shape it and within the policy debates that provide its impetus at a particular point in recent political history.

# Chapter 3: Theoretical framework

## 3.1 Introduction

Recall that a recurring theme from the literature review was the lack of empirical research undertaken in the socio-political contexts in which biometrics are being deployed, especially when they are proposed for use on a national scale and on a potentially mandatory basis, as was the case in the UK. The National Identity Scheme (NIS) thus provided an occasion to study biometrics ‘in the wild’. Considering the timing of the study and the ultimate demise of the Scheme, this research focuses not on the technologies in use, but rather on the discourses that accompanied their planned widespread diffusion, before it was terminated following the change of government resulting from the UK general election of 2010. This requires theory that helps us to understand the role of discourse, and in particular future-oriented discourse, about new technology and its relationship with organizations that were expected to build and operate the systems, as well as the citizens who were expected to use them. The theory adopted must also appreciate the significance of changes in these discourses.

The goal of this chapter[8] is to develop the theoretical framework required for such a study, which draws on ideas from the social science literature on framing, the qualitative study of information systems (IS) (namely organizing visions theory), and science and technology studies (STS) (including the sociology of expectations and research on the public understanding of science). In the next chapter I spell out the research methods needed for collecting and analyzing data in accordance with this framework.

As an entry point into this theoretical discussion, I begin by introducing Gregor's (2006) ideas on the nature of theory in IS research. This theoretical reflection lays the groundwork for the choice of concepts that will comprise my theoretical framework.

Gregor starts by noting that there are important domain questions regarding what phenomena, problems, and topics are considered worthy of study by IS researchers (p.611). These debates over the domain's identity have been around for decades. Orlikowski and Iacono (2001) confront these debates by calling for increased analytical attention to what they term the 'IT artifact' in IS research.

[8] Portions of this chapter were previously presented as a conference paper entitled "Adapting theory for researching future expectations in information systems innovations: the case of the United Kingdom's national biometric identity scheme" (Martin 2008), at the Society for Social Studies of Science (4S) meeting in Rotterdam.

What is an IT artifact? There are varying definitions. For Monteiro and Hanseth (1996), it is the outcome of discourses that negotiate the development, adoption, and use of a new technology.  Lee (2001) sees artifacts as emerging when technological systems and social systems interact (p.iii). For Orlikowski and Iacono (2001), IT artifacts are “those bundles of material and cultural properties packaged in some socially recognizable form such as hardware and/or software” (p.121). Benbasat and Zmud (2003) argue that it is “the application of IT to enable or support some tasks embedded within a structures that itself is embedded within a context” (p.186). Agarwal and Lucas (2005) want to expand Benbasat and Zmud’s definition by “specify[ing] IT as the integration of the processing logic found in computers with the massive stores of databases and the connectivity of communications networks. The IT artifact includes IT infrastructure, innovations with technology, and especially the Internet” (p.394).

Orlikowski and Iacono admit that such theorizing about IT artifacts might take many different forms (2001, p.131). Nonetheless, they offer five premises from which they believe theorizing should happen.

- IT artifacts are never natural, neutral, universal, or given; they are necessarily contingent. “Because they are designed, constructed, and used by people, they are shaped by the interests, values, and assumptions of a wide variety of communities” (p.131)

- IT artifacts are always embedded in a context (understood as time, place, discourse, and community)
- The artifacts themselves are actually an array of different, interconnected components. We often talk about technology as a unified and stable thing, such as “the Internet” or in this case study “biometrics”, but in reality technologies are never as integrated as our language might lead us to believe
- Rather than being fixed and independent, IT artifacts *emerge* as a result of varying social practices
- IT artifacts are dynamic; any stability they might display is conditional

These points on theorizing the IT artifact condition my selection of theoretical concepts and, following from that, my research approach.

Besides the diverging views on domain identity, Gregor notes three other classes of theoretical concerns facing the IS discipline: ontological questions; epistemological questions; and socio-political questions. Ontological questions interrogate the nature and composition of IS theory and the types of claims that can be made by IS scholars. Epistemological questions inquire about theory construction and testing, how knowledge is considered scientific, and research methodologies. Socio-political questions consider the relationship between the knowledge generated by IS research and those who produce and use it.

Having acknowledged these general debates, Gregor explains that within the field there are multiple perspectives on the role of theory in IS research. Each perspective comes with its own set of assumptions regarding the different goals of the research enterprise, including: analysis, explanation, prediction, and prescription. She proposes a taxonomy to help to classify different IS theories based on how they address these goals (see Table 3.1).

| Theory type | Distinguishing attributes |
|---|---|
| I. Analysis | Says what is. The theory does not extend beyond analysis and description. No causal relationships among phenomena are specified and no predictions are made. |
| II. Explanation | Says what is, how, why, when, and where. The theory provides explanations but does not aim to predict with any precision. There are no testable propositions. |
| III. Prediction | Says what is and what will be. The theory provides predictions and has testable propositions but does not have well-developed justificatory casual explanations. |
| IV. Explanation and prediction | Says what is, how, why, when, where, and what will be. Provides predictions and has both testable propositions and causal explanations. |
| V. Design and action | Says how to do something. The theory gives explicit prescriptions (e.g., methods, techniques, principles of form and function) for constructing an artifact. |

Table 3.1: Gregor's taxonomy of theory types in IS research

Gregor argues that theory can do different things. There are theories for analyzing, describing, understanding, explaining, predicting, and explaining *and* predicting; and for design sciences such as architecture or IS, theories for designing and acting. While each theory type has its own distinguishing attributes, the different types are interrelated, with some well-established bodies of theory including parts from the different types.

To suit my purposes, in this chapter I want to focus mainly on theories that fall under type I and partly under theory type II. The research project seeks to identify, integrate, and strengthen theory to analyze and describe the discursive development of biometrics in the current case, with the hope that this theory can be applied to similar technologies and research contexts. Where explanation does occur, it is not an attempt at causal explanation, but rather about constructing “classificatory, compositional, or associative” relationships (Gregor 2006, p.623). Furthermore, as this is qualitative research, I am not especially interested in devising testable propositions for predicting the future outcomes of technology use (type IV); nor is this project about prescribing design methods (type V).

Theories for analysis focus on describing and making sense of “what is” rather than trying to explain causality or test propositions. Fawcett and Downs call these theories “the most basic type of theory” (1986, p.4), which can be used to describe or categorize the characteristics of the object of study, including phenomena such as new technology. “Descriptive theories are needed when nothing or very little is known about the phenomenon in question” (Fawcett & Downs 1986, p.4). Such is the state of affairs in this study, with the knowledge void that exists around real-world deployments of biometrics.  A contribution to theory within this type would attempt to provide a credible description of “what is”, perhaps structured analytically by a classificatory schema.

While descriptive analysis is a very important component of qualitative IS research, there is also a role for theory that explains *how* and *why* phenomena occur (Gregor 2006, p.624). Gregor notes that this class of theory could perhaps more accurately be labeled “theory for understanding”, which highlights how these theories can open up new ways of viewing phenomena, and de-emphasizes concerns about causal explanation and the formulation of testable propositions. In this sense, explanatory theory can be understood as a “sensitizing device” (Klein & Myers 1999, p.75).

Theories for analysis or explanation also lend themselves to case study research, whereby in-depth explanations can be given about the process by which some real-world event happened, as well as the factors that brought about such an outcome. Thus, a contribution to knowledge within this type of theory should resemble concepts that help to explain how and why something happened the way it did in this case, which was previously poorly understood. Gregor argues that contributions from case study research must be more than simply a story about what happened; for contributions to be considered “theoretical” they must offer “conclusions with some generality” (2006, p.625). As with contributions to theory type I (analysis and description), contributions must be plausible, credible, and consistent.

What academic fields and disciplines can be drawn upon in erecting a theoretical framework which allows us to understand more clearly the dynamics around discourses on biometrics in the context first identified in the introduction and then elaborated in chapter 2? Are there concepts that researchers can use to study similar information technology (IT) innovations as they emerge in a given socio-political context? If so, what are their strengths and weaknesses, and further, what might I be able to contribute back in terms of theory?

My objective in the following sections, therefore, is to marry sets of concepts from different fields to better understand the discursive development of IT innovation. This conceptual marriage lays the groundwork for the in-depth, qualitative study of biometrics that follows. Throughout, I place emphasis on theory that helps to describe and explain the dynamics of public discourses about new technology and the public.

## 3.2 Frames and framing processes

The idea of ‘frames’ has been used extensively in social science research on social movements and collective action (Goffman 1974; Benford & Snow 2000). Members of social groups, including actors such as the politicians and civil servants that sponsor and execute new policy initiatives, are viewed as signifying agents that actively engage in meaning production and meaning maintenance around social issues (Snow & Benford 1988). They do so partly through discursive work. Framing is understood as an active and goal-oriented process. It is a contentious activity in the sense that it involves generating interpretive frames that both differ from existing ones and also challenge them. Framing is also a dynamic process that is both enabled and constrained by political, cultural, and audience-related factors. These frames may become more or less resonant due to political currents, and are supported by the "extant stock of meanings, beliefs, ideologies, practices, values, myths, narratives, and the like" (Benford & Snow 2000, p.629).

The resulting products of this process are referred to as 'collective action frames'. For Goffman, frames represent "schemata of interpretation" that allow us "to locate, perceive, identify, and label" events and organize our experiences (1974, p.21). Likewise, collective action frames help us to interpret and organize the world out there, but with the objective of mobilizing for action. These action frames are more than just cognitive constructs. They are also the outcome of meaning negotiations (Gamson 1992, p.111). The concept of frames can thus be seen as core to understanding the processes of collective social action and organizing IT innovation.

The social science research on the different *processes* of framing activities is particularly relevant to the present study. Understanding the discourses that comprise the case from a process prospective will help us achieve a richer longitudinal analysis by highlighting how frames developed over time and explaining the significance of the changes they underwent. Research on the processes of framing is therefore especially helpful, although as Davidson (2006) notes, there is a dearth of IS research on the framing processes around new technology.

Snow and Benford review the social science literature to identify several processes that constitute the development, generation, and elaboration of collective frames:

- Frame articulation – the discursive linking and alignment of otherwise separate events in a unified and convincing manner
- Frame punctuation – highlighting some issues as being more salient or relevant than others
- Frame alignment, which is inclusive of:
  - Frame bridging – linking two or more "ideologically congruent but structurally unconnected" frames around an issue or problem area (p.624). Bridging can occur both within and across groups
  - Frame amplification – embellishing or clarifying a frame so that it resonates with existing cultural values
  - Frame extension – drawing out a frame beyond its primary focus to include other issues; however, doing so may destabilize the frame
  - Frame transformation (or frame switching) – changing frames or generating new ones in light of new evidence

- Counter-framing – when another group challenges, undermines or neutralizes another group's interpretive framework, which may subsequently lead to re-framing (Benford 1987, p.75). These processes are referred to as 'framing contests' (Ryan 1991). The media, in particular, play an important role in these contests

Beyond frame generation and development, another set of processes surrounds the *diffusion* of frames. How do frames move from one movement or context to another? Frames are said to diffuse either through strategic frame selection and strategic frame fitting (Benford & Snow 2000, p.628). When frames are strategically selected, they are actively borrowed or imported from another cultural domain. Strategic fitting involves strategically promoting and tailoring a frame from another context.

These different framing activities provide a dynamic and process-oriented perspective to apply to the core theoretical concepts in this thesis. It will be important to focus on how the frames that underlie discourses at work in the government's vision for biometrics developed and, more importantly, how and why they changed during the course of the proposals.

## 3.3 Organizing visions in information systems innovations

The core stream of IS literature that motivates this research project focuses on the processes of interpretation, legitimation, and mobilization in IT innovation (Swanson & Ramiller 1997; Swanson 2003). In particular, the notion of an ‘organizing vision’ provides a useful concept to help understand and explain the discursive emergence and development of an innovation such as the UK government’s pursuit of multiple biometrics in a national identity scheme.

In their seminal paper, Swanson and Ramiller aim to understand the institutional processes that facilitate the adoption and use of new technology in organizations. In contrast to the view that the early decision to adopt a given innovation is the result of local, rational organizational processes, which are subsequently institutionalized with the increased uptake of the technology (Tolbert & Zucker 1983), they argue that IS innovation can be better explained by viewing the phenomenon as a collective process of creating and propagating an organizing vision that co-ordinates decisions and actions related to the technology’s materialization and diffusion. The organizing vision can, thus, be understood as a sense-making device (Weick 1995). They state that, “in so making sense of the innovation, the community in effect also defines it and creates it” (Swanson & Ramiller 1997, p.459). I make use of such a constructivist conceptualization of innovation in the present study.

Organizations are frequently confronted with novel technologies which they perceive as demanding their attention. “New technology often arrives on the marketplace in an immature state, puzzling as to its benefits, future prospects, and long-term form" (Swanson & Ramiller 1997, p.459). Defined as "a focal community idea for the application of information technology in organizations" (1997, p. 460), an organizing vision is therefore intended to reduce, in broad strokes, the uncertainty that accompanies these new technologies. The organizing vision permits simplified understandings about these novel and, as yet unsettled, technologies.

Swanson and Ramiller identify three main functions of an organizing vision:

- **Interpretation**: When a new technology arrives on the scene its meaning and implications are not well-understood by organizational actors. It is in this context that organizing visions are generated to give some interpretive coherence to the innovation. They provide a focus for the innovation's interpretation (Swanson & Ramiller 2004, p.556).
- **Legitimation**: These visions also give organizations reasons and justifications for pursing an innovation. They provide an answer to the question, 'why do it?'. This legitimation process is facilitated through the reputations and authority of those promulgating the vision. To adapt an example from Swanson and Ramiller's paper to fit the case at hand, this process might be initiated as follows: "Why aren't we doing [biometrics] yet?" the [Home Secretary] might ask his or her [civil servant], having just read about it (and all the good things that come to leading [countries] doing it) for the first time in Business Week (1997, p.461).
- **Mobilization**: The organizing vision is a "creative force" that sparks and energizes market interest and activity to support the realization of the innovation. "Would be adopters look to the market for needed resources, including hardware, software, and skills, following clues and guidelines embedded in the organizing vision" (Swanson & Ramiller 1997, p.461).

Organizing visions are produced and sustained *discursively*, by a community with a common interest, who may agree or disagree about the content of the vision (Swanson & Ramiller 1997, p.462). "An organizing vision is a construction *in discourse*" (Swanson & Ramiller 2004, p.556, emphasis added). The potential for disagreement means that there is an ongoing contest of interpretation over the meaning of the technology. It may be the case that, in some instances, these contests consist of counter-framing processes that are motivated by hostility to the vision as a whole rather than mere disagreement about its content.

For Swanson and Ramiller, the depiction of the vision as an appropriate response to a certain problematic will determine its currency and perceived relevance. The vision's perceived distinctiveness, intelligibility, informativeness, plausibility, and practical value will determine how compelling it is to other stakeholders and its eventual success (or failure) (Swanson & Ramiller 1997, p.469). Importantly, there must be some new or emerging technology accompanying the vision that can be exploited by, but which also constrains, the vision. Often buzzwords (such as 'customer relationship management' (Firth 2001) or 'enterprise resource planning' (Wang 2009), or as in this present case, 'biometrics') play an important discursive role in signaling and strengthening the vision. However, there are risks to the overuse and overextension of such terms.

The notion of an organizing vision provides us with a main concept to study the role of imaginative discourse in information systems innovations. It explicitly recognizes that the content of visions may originate in contexts outside a single business organization and provides a means to understand the influence that other participants and actors (including technology vendors, consultants, academics, the trade press, etc.) play in IT innovation processes. Second, it provides a conceptual footing for the role of buzzwords and marketing hype in perpetuating IT fads. Third, its emphasis on the early stages of discursive development, when understandings and outcomes about new technology are most uncertain, makes it particularly useful to this case study.

Elsewhere, Swanson and Ramiller build on their organizing vision concept to explore the differences between ‘mindful’ and ‘mindless’ organizational innovation (2004). Mindless innovation is best illustrated by organizations that purse new technology because others are doing so – the well-known ‘me too’ phenomenon. In contrast, an organization that innovates mindfully does so “with reasoning grounded in its own organizational facts and specifics”

(Swanson & Ramiller 2004, p.559). Noting that mindfulness is a kind of ideal type, the authors identify five attributes of mindful innovation:

1. Healthy preoccupation with failure – rather than celebrating successes, mindful organizations obsess over failure and learn from close calls.
2. Reluctance to oversimplify interpretations of new technology – mindfulness “calls for the organization to eschew stock or formulaic interpretations of IT innovations” and “entails a resistance to the simplified image of the innovation that is encoded in the organizing vision” (Swanson & Ramiller 2004, p.660).
3. Sensitivity to operations – mindful organizations attend to minor and seemingly insignificant details.
4. Commitment to resilience – mindful organizations are resilient and flexible. They improvise rather than over-plan, adapt instead of following routine, and aim for effectiveness over efficiency.
5. Mindful organizations defer to experts over formal authority – such expertise is typically heterogeneous and dispersed throughout the organization.

Swanson and Ramiller note that future research in this area should explore the larger community terrain over which organizing visions reign (1997, p.471). While they do explicitly acknowledge the role that external actors play in developing and energizing visions for new technology, their original empirical focus was on institutions. There is therefore an opportunity to explore innovation processes beyond the boundaries of formal organizations, as Wang and others have recently done (Wang & Swanson 2008; Ramiller & Wang 2009; Wang 2009; Wang 2010). Wang argues that researchers studying IT innovation must peer beyond organizational boundaries to explore the collective discursive environment in which adopters, technology vendors, IT consultants, investors, journalists, analysts, academics, and others develop ideas about how to develop and use new technology (Wang 2009, p.4). These understandings represent what a technology is, why organizations should strive to adopt it, and how to go about doing so. Wang focuses on discourse arenas such as advertisements, books on new technology, magazine articles, conference and exposition speeches, training materials, brochures, interview scripts, roundtable discussions, and blogs to analyze the popularity and prevalence of ideas about new technology. For example, he and Swanson study advertisements for customer relationship management (CRM) systems in *Business Week* to show how ads provided fresh meanings to the technology's organizing vision (Wang & Swanson 2008).

Wang's approach to studying innovation processes through extra-institutional discourses on new technology supplements the organizing vision concept by focusing our attention on other arenas where innovation 'happens'.

## 3.4 Technology and expectations

Closely related to organizing visions theory is a growing body of concepts and empirical findings on *future expectations* in new science and technology emerging from the science and technology studies (STS) literature (van Lente 1993; van Lente & Rip 1998; Borup et al. 2006). This 'sociology of expectations' is concerned with the role and significance of prospective, speculative, imaginative, and futuristic discourse and imagery in science and technology ventures, exploring whether and to what extent these discourses mobilize and co-ordinate actors and shape organizational change. Expectations are seen as a constitutive or performative force of innovation; enabling some scientific and technological possibilities while disabling others. As the discourses that comprise the case are rife with expectations about what biometrics can achieve, I want to introduce these theoretical ideas on the relationship between technology and expectations. These ideas provide new insights that will sharpen the analytical lens we apply to the data by expanding our understanding of the function and agency of expectation-based discourses.

The sociology of expectations seeks to theorize how those with vested interests in a scientific or technological endeavor go about giving life to that which does not yet exist in material form. Through the careful development and management of future expectations, imaginings, and visions for technology, actors hope to guide activities, provide structure and legitimacy, attract interest and resources, and frame discourses on issues of seeming relevance (Borup et al. 2006, pp.285-286). Previous studies have investigated the role of expectations in biotechnology (Brown & Michael 2003; Väliverronen 2004), genetic technology (Horst 2007; Sung & Hopkins 2006), and nanotechnology (Lösch 2006), among others. In his analysis of the visionary depictions of nanotechnology, for example, Lösch (2006) showed how futuristic visual imagery serves as a means of expectation exchange and meaning production between the domains of science, economy, and mass media.

In their review of work from the sociology of expectations, Borup et al. (2006) appraise four major functions of expectations: expectations as a constitutive force of change, expectations as temporal variability, expectations as socio-spatial variability, and expectations as bridging the imagination and materiality. I summarize each in turn and explain their applicability to the current research.

## Expectations as constitutive force

In this function, expectations are seen as agents that broker relationships between different actors and groups involved in a scientific or technological pursuit. It is difficult to imagine technological development and innovation without a shared, yet flexible set of guiding expectations. This is especially the case during the periods of high uncertainty encountered in early moments of technological change, in which shared expectations are required to enroll a broad range of stakeholders and improve the likelihood of success (Borup et al. 2006, p.289). Van Lente and Rip (1998) view expectations as *prospective* social structures, which can be filled in, modified, or reconfigured. Within these dynamics, it is the *content* of expectations that matters. This content pulls actors together and shapes further action. These ideas about the potential agency of expectations resonate with Swanson and Ramiller's points on organizing visions, outlined above.[9]

## Expectations as temporal variability

Most scientific and technological undertakings experience cycles of hype and disappointment. This phenomenon of early promise and subsequent disappointment reveals how an early surge in hype might be necessary to get a hearing (Borup et al. 2006, p.290). In this sense disappointment may be viewed as being built into scientific and technological ventures. Early hope is almost never proportionate to the eventual results of a project. At the same time, past failures are often written off as unusual or atypical (Borup et al. 2006, p.290).

These are interesting ideas that need to be accounted for in the analysis. In particular, the temporal variability of expectations for biometrics will be examined. Moreover, the fact that the program was initiated and sponsored by the UK government, which is often criticized for its poor track record on completing large-scale IT projects (cf. Public Affairs Committee 2011), could

[9] However, explicit mention of the organizing vision perspective is missing from virtually all the work on the sociology of expectations, including the contributions to the 2006 *Technology Analysis and Strategic Management* special issue on expectations. Only recently have scholars begun to connect these theoretical dots (see Pollock & Williams 2010).

mean that expectations of failure were prominent from the outset, at least among certain groups.

## Expectations and socio-spatial variability

Expectations and future uncertainty vary not only over time, but also among different groups of actors involved in a project. As a result, people will attach different levels of trust to technological expectations. Borup et al. remark: “Expectations have the appearance of greater authority for those who see themselves as having little influence over the outcome of a promise (publics, for example). This easily translates into a normative framing of expectations: ‘it’s going to happen so you might as well get used to it!’” (2006, p.292).

These points align with arguments by MacKenzie – illustrated by his ‘certainty trough’ (see Figure 3.2) –, which depicts the relationship between a group’s proximity to a technological development and the degree of uncertainty they posses about the technology. It illustrates how those who are removed from the relevant decision-making processes tend to exhibit the highest levels of uncertainty about new technology. However, it also shows how those who are intimately connected with knowledge production are also often less sure about their knowledge claims than those with indirect knowledge.

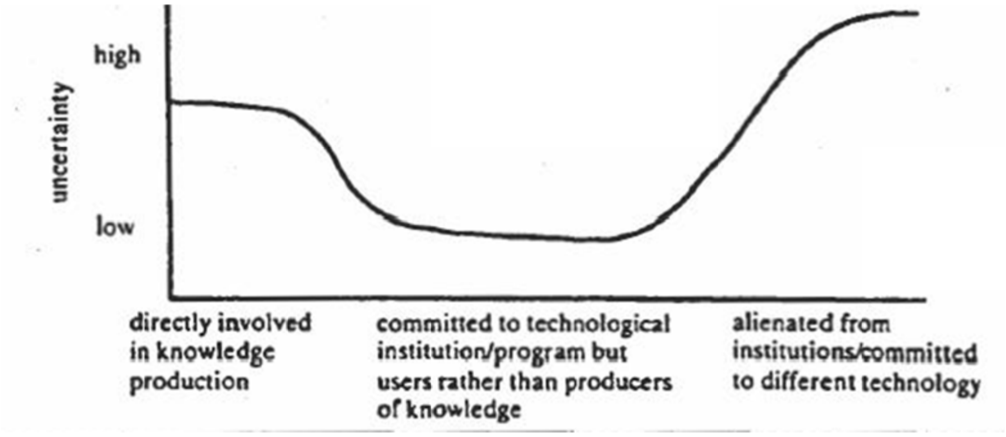


Figure 3.2: Certainty trough (MacKenzie 1993)

Applying MacKenzie's observations to the case, we will need to consider how expectations potentially differ across stakeholders and social groups involved in the government's program for identity cards, and reflect on how each group responds to degrees of uncertainty around the concept of biometrics. As we are primarily interested in the discourses of government officials involved in the National Identity Scheme (i.e., actors who are committed to the technological program but as users rather than producers of knowledge about biometrics), we will want to pay particular attention to how their vantage point vis-à-vis the Scheme affects the kinds of expectations they generate and the degree of uncertainty exhibited by those expectations.

## Imagination, materiality, and embodiment

Finally, to what extent are expectations simply discourse or rhetoric? Can we begin to understand expectations as being ‘inscribed’ in materiality? If so, then what are the ‘routes of transmission’ between imagination, embodiment, and materiality? While these questions are interesting, they are less relevant to this study, which focuses centrally on discourses rather than the material artifact. However, there were important moments in the development of the Scheme when expectations were ‘made material’, such as during biometric technology pilots and a “biometrics roadshow” across the UK. The discourses that emerge around these moments provide channels to analyze the dialectic relationship between the conceptual and material.

Finally, a recent critique and elaboration of these ideas in the sociology of expectations comes from Pollock and Williams (2010), who take issue with many studies of expectations that neglect the what they describe as the “business” of technological expectations; that is, the *promissory* intermediaries which produce, commodify, and sell future-oriented knowledge to organizations interested in adopting new technology. They argue that, by ignoring these middlemen and the attendant dynamics of knowledge production, scholars risk misunderstanding the effects of expectations – how expectations influence innovation in different ways. In particular, they take issue with the notion of expectation as ‘self-fulfilling prophecy’, which they claim oversimplifies the performativity of future-oriented discourse. These intermediaries where present in the case of the NIS. They will need to be accounted for in the analysis, along with the influence of their discourses.

## 3.5 The publics of technological innovation

### Public understanding of science and technology

I now move to review final set of ideas in order to draw out a concept to explain the ‘publics’ of innovation. Research on the public understanding of science and technology (abbreviated as PUS) has traditionally focused on the public’s perception, opinion, and acceptance of scientific innovations such as nuclear power (Gamson & Modigliani 1989), biotechnology (Gaskell & Bauer 2001), and nanotechnology (Gaskell et al. 2005), to name a few popular examples. Studies on the public’s perceptions and understandings of surveillance and security technologies are just now beginning to emerge (see, for example, Pavone & Degli Esposti 2010).

Bauer et al. (2007) identify and trace three main PUS research paradigms: 1) science literacy, 2) public understanding of science, and 3) the science and society critique. They argue that each paradigm approaches the problem of public understanding in a different way and poses distinguishing questions and solutions to the ‘problems’ of PUS (2007, p.79).

Originally, PUS research was mostly concerned with identifying and correcting knowledge and attitudinal deficits. This approach was castigated as being a patronizing ‘deficit model’ and has since been displaced by so-called critical approaches. In the next sections, I briefly outline each paradigm, noting their respective strengths and weaknesses. The output of this review is a concept to apply to *discourses* about *publics* and their *understandings* of new technology.

## Science and technology literacy

Historically, the science literacy paradigm has sought to measure textbook knowledge of scientific facts, the scientific method, and the history of scientific and technological ‘progress’. It has also aimed at helping the public reject unscientific superstitions such as astrology and numerology (Bauer 2009). The literacy paradigm often attributes a knowledge deficit to the public so that it may be corrected. By demonstrating that the public is ignorant about a certain scientific or technological issue, a case can be made for increased education. Calling the public ignorant in matters of science and technology also permits the rise of an expert class for scientific and technical decision-making. As Bauer et al. remark, the deficit model “plays into the hands of technocratic attitudes among decision-makers: a de facto ignorant public is disqualified from participating in science policy decisions” (2007, p.80).

This paradigm has been critiqued extensively over the years due to its inherently negative attitudes towards the public (Wynne 1995). Critics further argue that researchers in this domain rarely critically reflect on what is exactly meant by ‘science’, ‘understanding’, ‘technology’ or the ‘public’ (Wynne 1995, p.362; Jasanoff 2000, p.41). Horst notes that the idea of the ‘public’ as “a national unity of laypeople characterized by greater or lesser degrees of scientific literacy” is especially conceptually problematic (2007, p.152).

Critics have also taken issue with the literacy paradigm’s over-reliance on survey methods, as well as the tendency for governments, businesses, and scientific institutions to sponsor such survey research (Bauer et al. 2007, p.79). This tendency has been interpreted and criticized as pursuing agenda-based research, with the claim being that surveys can always be designed to discover some sort of knowledge deficit in respondents. However, Bauer et al. are careful to point out that the automatic equation of a particular political agenda with a particular research method is a fallacy (2007, pp.79-80). While it might be the case that past research into scientific and technology literacy has relied heavily on survey methods, it does not necessarily follow that public surveying is simply about identifying and correcting supposed public deficits. Nor does it mean that agenda-based research cannot adopt other research methods (e.g., focus groups).

As the first major research paradigm within PUS, the science literacy approach is historically important. Indeed, many policy discourses still reflect its biases. However, this paradigm does not provide any analytical tools for the present research study. Its focus on testing textbook knowledge of science and technology is incongruent with the stated aims of my research as it fails to appreciate the ongoing uncertainties and contingencies around biometrics.

## Public understanding of science: attitudinal deficits

In the late 1980s concerns about knowledge deficits among the public made way for alarm in scientific and policy-making communities about increasingly “poor” attitudes towards science and technology (Bauer et al. 2007, p.82). A public unsupportive of science was deemed bad for society. During this period, research shifted away from measuring literacy and towards assessing knowledge and attitudes. The correlation between knowledge and public attitudes therefore became the focal point of PUS research (Bauer 2009, p.224).

Within this research paradigm it is possible to locate two agendas: ‘normative-rationality’ and ‘realist-empiricism’ (Bauer et al. 2007, p.83). For the former, increased knowledge of science and technology is said to result in improved attitudes – ‘the more you know about science and technology, the more you love it’. A lack of knowledge is associated with biased risk perception. It is argued that an informed public is also more inclined to agree with experts, who know best.

For the ‘realist-empiricist agenda’, attitudes are said to be loaded with values, with important relations with the social world. These “values and emotions are a fact of life and the battle is a battle for hearts of a lifestyle public” (Bauer et al. 2007, p.83). Within this agenda, the public are seen as consumers of science and technology, and accordingly fall into different market segments: confident believers, technophiles, supporters, concerned, the ‘undecided’, and the ‘not for me’ (Office of Science and Technology 2000). It is said that scientific evidence and technical know-how need to be made ‘sexy’ so that consumers are seduced (Bauer 2009, p.225).

## Science and society

In the context of this second debate, the science and society paradigm seeks to move beyond the traditional deficit model by reversing it and attributing a deficit to scientific institutions and technical experts. Its critique of earlier paradigms centers on a perceived crisis of trust among the public with respect to science and technology and the expertise employed to communicate issues deemed relevant to public attention (Bauer et al. 2007, p.85).

It is believed that once public trust in science and technology is lost it is virtually impossible to regain, and therefore there is a perceived need for increased public deliberation and participation in scientific matters. Proponents argue that efforts of public engagement should occur ‘upstream’, meaning in the early stages of new scientific and technological developments, “to enable front-end input and not only post-hoc reactions to already established facts” (Bauer et al. 2007, p.85).

One stream of research within the science and society critique to public understanding considers the extent to which members of the public are consulted and involved in decision-making processes, particularly during the early phases of planning, designing, and developing science and technology projects. Michael describes this model as a movement aiming to capture and circulate “the voice of publics” vis-à-vis scientific and technological controversies (2009, p.621).

Such deliberative models rely on citizen juries, public hearings, consensus conferencing, scoping exercises, science festivals, and so forth (Einsiedel 2001; Bauer 2009). These different engagement formats share the same basic elements: the participation of the lay citizenry in considering some scientific and technological problem; an extensive learning process and exploration of what is known amongst the public about a given issue; considering the different values underlying these viewpoints; examining what is known, unknown, or unsure on the evidence base; facilitating deliberation between citizens and representatives of various technical perspectives; and developing policies based on these deliberations (Einsiedel 2001, p.95). These formats for assessing public understanding were prevalent in the case of the National Identity Scheme and offer a special set of discourses about the public on which to draw.

Despite its promise, there are several problems with this approach. Bauer (2009) argues that engagement research runs the risk of becoming advocacy, for, in many ways, it is action research in which analysis is not always separated from intervention. Worse, academics can end up as political consultants who are tasked with rebuilding public trust. And as public engagement requires ‘event making’ where engagement and deliberation can ‘happen’, resources and know-how (i.e., expertise) are required to run the show. Furthermore, policy-makers feel the need to evaluate these public deliberations (i.e., were they effective and good value for money?) and thus the ethos of traditional PUS research ironically creeps back in.

## Theorizing publics

Instead of assessing or correcting presumed knowledge or attitude deficits in the public, critical approaches to PUS research explore the range and diversity of local or contextualized understandings with respect to new science and technology. In doing so researchers try to explain what these understandings represent in terms of science-society or technology-society relationships. In particular, some scholars try to discern the different ‘publics-in-particular’ (Michael 2009) or ‘ethno-epistemic assemblages’ in respect of a given innovation. These publics are described as coalitions or hybrid groups characterized by heterogeneity and fluidity in their understandings of and dispositions toward new science and technology (Irwin & Michael 2003; Horst 2007). They are manifestations that are always being constructed, deconstructed, negotiated, and reconfigured as part of the meaning production taking place during a technology’s development.

This conceptual reformulation is in opposition to previous notions of the ‘public-in-general’, which are perhaps most evident in the national surveys of PUS informed by traditional deficit models. Critics charge that these instruments actually construct the public (or publics) whose knowledge they aim to measure. When these publics appear in policy discourses on science and technology they may have further normative and performative effects.

The concept of an ‘ethno-epistemic assemblage’ on the other hand provides a alternative by highlighting how any discussion of the public, be it in a research instrument, a political speech, or media report, simultaneously functions to ‘make’ and perform publics. It allows us to theorize the publics of biometrics in an innovative way – as constructions that emerge through the research instruments used to measure their acceptance, opinions, and knowledge, the policy discourses that depict them and their relationship with the government's proposals, and the media coverage that captures these events.

## 3.6 Integrating the framework

Having reviewed the theoretical literature that informs this study, in this section I present a summary of the conceptual framework for the study of discourses about biometrics in the case of the NIS (see Table 3.3).

| Concept | Empirical application | Comments | Key questions |
|---|---|---|---|
| Organizing vision | Government discourses on biometrics | This serves as the core concept in this study. It will be applied to the government's discourses to explore how officials made sense of biometrics and the extent to which their discourses were able to mobilize efforts | What was the government's vision for biometrics? Was it distinctive? Intelligible? Informative? Plausible? Of practical value? How did it change over time? What difficulties did the vision encounter and how were they resolved? |
| Technological expectations | Public discourses on biometrics (including policy and media discourses) | Enriches our understandings of the agency and function of future-oriented discourses | What types of technological expectations were active in public discourses on biometrics? What function did these expectations play? |
| Technological publics (ethno-epistemic assemblages) | Discourses about the public with respect to biometrics | Provides a radical view of the publics of new technology | How did the publics of biometrics emerge in government discourses? What problematic publics emerged? |

Table 3.3: Concepts for analyzing discourses about biometrics and their publics

How do these concepts interconnect? First, the organizing vision concept serves as the core theoretical construct in this study. The objective in using the concept is to understand how a vision for biometrics emerged in the case and the extent to which it was sustained. Whether or not a vision organizes is a separate issue. This is an open question that must be empirically determined. Answering this question involves exploring the vision's capacity to interpret, legitimize, and mobilize actors to innovate (i.e., to satisfy the three functions of an organizing vision).

Studying visions in this manner means studying discourses. I understand a vision for new technology to emerge *through* discourse. It is an *outcome* of a discursive process involving proponents and challengers. These discourses also function to sustain the vision if and when it emerges. A significant subset of these discourses can be characterized as expectations insofar as they attempt to describe or predict a future state of affairs. Technological expectations may perform different functions, including being a constitutive force of change, providing temporal and socio-spatial variation, and bridging the gap between imagination and materiality. Another subset of these discourses will pertain to the publics of new technology. I conceptualize these discourses in terms of the ethno-epistemic assemblage. That is, I will allow the publics of biometrics to emerge through the discourses that describe and try to resolve them.

All of the discourses that comprise the vision for new technology provide a *medium* for the framing processes that underlie the production and maintenance of meaning. Of particular interest are the changes that frames undergo over the course of the case study. Figure 3.4 visually depicts how these concepts fit into a high-level framework.

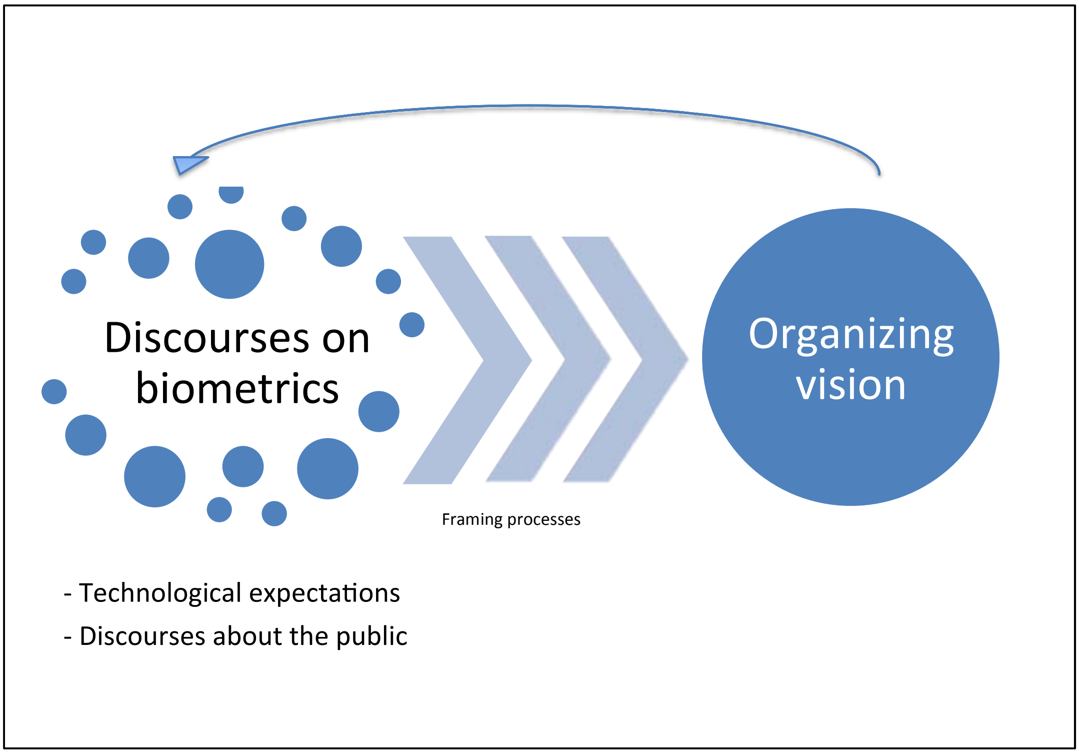


Figure 3.4: Working theoretical framework

## 3.7 Research questions

Finally, the preceding theoretical discussion gives rise to a set of core research questions:

1. How did government spokespeople portray a vision for biometrics in the National Identity Scheme, and to what extent did this vision organize efforts and mobilize actors to innovate?

2. How did policy debates and attendant media reportage discursively capture biometrics, and what were the limitations of these discourses in revealing the complexities and perplexities of the technologies?
3. How were the ‘publics’ of biometrics portrayed in these discourses?

I now move to devise my research methods for answering these questions.

# Chapter 4: Research methods

## 4.1 Case study research

I elected to adopt a case study research strategy to investigate the discursive trajectory of biometrics within the National Identity Scheme (NIS) in the UK because, as Yin (2003) points out, case studies permit the investigation of phenomena in their 'natural' environments (that is, in real-life contexts rather than as part of artificial experiments).

But what is a case? It is a question for which conclusive answers are hard to come by. Indeed, there are entire volumes dedicated to pondering this question (e.g., Ragin & Becker 1992). It is an issue that has forever plagued social science. Ragin argues that there are four possible ways to answer the question:

- Cases are found – implies that cases are "empirically real and bounded, but specific". Researchers identify and establish cases during the process of doing research (Ragin 1992, p.9).
- Cases are objects – also treats cases as having an empirical reality and being bounded, but these can be *unspecific*. That is, researchers feel no need to designate boundaries around the case.
- Cases are made – cases are "*specific* theoretical constructs which coalesce in the course of research" (Ragin 1992, p.10, emphasis added).
- Cases are conventions – cases are *general* theoretical constructs which are the product of the collective work of scholars.

Importantly, these distinctions are not absolute and overlap is to be expected. Myers (2008) reiterates these points when he notes that, “In case study research, it is in fact very difficult to separate the phenomenon of interest from the context, because the context itself is part and parcel of the story” (p.75). As discussed earlier, the context in which the NIS proposals took place was tightly interwoven with the discourses themselves, as well as other, related government programs and technological discourses. During the research my venture to ‘find’ the specific case ran into various stumbling blocks, which were partly the result of a lack of specificity around the object of study. As a result, I treated the case as a real but relatively unspecific object, existing through the various and occasionally contradictory discourses under analysis. And by studying this case, I undoubtedly simultaneously constructed it.

Ragin and Becker call for researchers to ask themselves “what is this a case *of*?” throughout the course of their research project. Heeding this call, mine is a study of the case of biometrics in the UK government’s proposals for a national identity program. The case study strategy to social research involves an extended, longitudinal examination of the phenomenon. Mine is idiographic in nature as it tries to understand the discursive dynamics around a (supposedly) single phenomenon (namely biometrics) within a particular time and place (early 21st century Britain) (Benbasat et al. 1987, p.369). Such a strategy is also particularly useful when the data sources are multiple (Yin 2003, pp.13-14), as, indeed, was the case in this research project.

This research project covers the time period spanning from July 2002, when the original *Entitlement Cards and Identity Fraud* consultation document was launched, until December 2008, when the Home Office began issuing identity cards for foreign nationals and the Identity and Passport Service (IPS) moved to create a market for biometric enrollment through its release of a *Front Office Services Prospectus.* This provides roughly 6 years of data from which to tell a tentative and incomplete story of biometrics.

There were two major empirical research phases in this project: a data collection phase and an extended analysis phase. The data collection phase included exploratory focus group interviews as well as the systematic gathering of government communications about biometrics and relevant media coverage. The decision to collect data from these spheres was motivated by Bauer's (2002) triangular model of the public sphere of science and technology, which encourages the analysis of data from the arenas of policy, media, and public opinion. The data analysis proceeded from this first phase, and was based on techniques of critical discourse analysis.

## 4.2 Methods for data collection and analysis

### Data collection

From the beginning of the research project (Autumn 2006) I reviewed the wide array of documents relating to the NIS that were regularly issued by the sponsor actors in the case (namely, certain members of the Labour Party, the Home Office, and its newly created sub-department: the IPS), the transcripts of interviews that the leaders of these organizations as well as political figures such as the Prime Minister occasionally gave, and the records of parliamentary statements (found in Hansard) regarding the Scheme and the role of biometrics. These sponsor actors were an amalgamation of those individuals and organizations who had privileged access to information about the Scheme and who made policy decisions about its introduction and ongoing implementation.

During this time I also reviewed the historical documentation that had been issued since 2002 (prior to the commencement of my PhD research), which had been archived by the LSE Identity Project (with whom I was fortunate to work closely). The LSE Identity Project team has amassed what is probably the most comprehensive archive of documentation related to proposals for identity cards in the UK (Whitley & Hosein 2010, p.xviii). Alongside these documents, I also monitored the mainstream press coverage of the NIS, familiarizing myself with how issues were framed and their lifecycles. This early reading of documents and the monitoring of media coverage were intended to inform me of the major currents and themes of interest and was not initially systematic. The systematic documentary data collection and analysis would take place later. These early efforts, combined with the subsequent systematic analysis, contributed to an important hermeneutical component to my study (Myers 2008, chap.14).

## Exploratory focus group interviews

Following my PhD upgrade I undertook a series of focus group interviews with certain members of the public. These interviews were intended as an opportunity for “relevant social groups” (Pinch & Bijker 1984) to voice their understandings of and concerns about the topic of biometrics, and for me to begin exploring the meanings that these technologies elicit when people are given an opportunity to reflect on them. The focus group interview format was chosen because it is a staple of public understanding of science and technology research (the more qualitative version of the research approach lends itself quite well to focus group methods), but also because I was interested in ascertaining collective views on the topic of biometrics and group interviews are conducive to generating these shared meanings.

In the first instance I drafted an interview guide, which was tested in a pilot session and reworked for subsequent interviews. One of my first findings in the initial pilot interview was that I assumed that the interviewees would know what the term “biometrics” meant. A surprising number of them did not recognize the term, but were familiar with the different types of biometrics once they were put forward. By naming examples of types of biometrics (fingerprints, iris scanning, and facial recognition) in the opening questions, I was able to facilitate a better discussion.

The finalized interview guide is available in Appendix 1. The questions included in the guide were theoretically-informed, generated from a detailed reading of the academic literature on biometrics, and modeled after focus group guides from previous research on biotechnology (Gaskell & Bauer 2001) and information and communication technologies and trust (Lachoee et al. 2006). The interviews were scheduled to run for a full hour, but occasionally ran over.

I used video stimuli in the focus group interviews. Two video clips were originally appropriated for the pilot. The first video was produced by the IPS and served as a general introduction to the Scheme and how it was envisioned to work. It also introduced the concept of biometrics to viewers. In order to balance the perspective put forth by this government-sponsored video, I contacted Mr. Phil Booth, the national coordinator of the anti-ID card civil society group No2ID, to have him record a video response in which he provided another set of opinions and perspectives on the biometric technologies in the Scheme. In the end I chose to replace the No2ID video with two shorter clips originating from Germany, which highlighted the perceived risks with their new biometric passports (i.e., that the fingerprint technology might not be totally secure and is spoofable). Combined, the IPS video and the two videos on the German biometric passport ran for 10 minutes. Screen shots from each of the videos (including the replaced No2ID clip) are presented below.

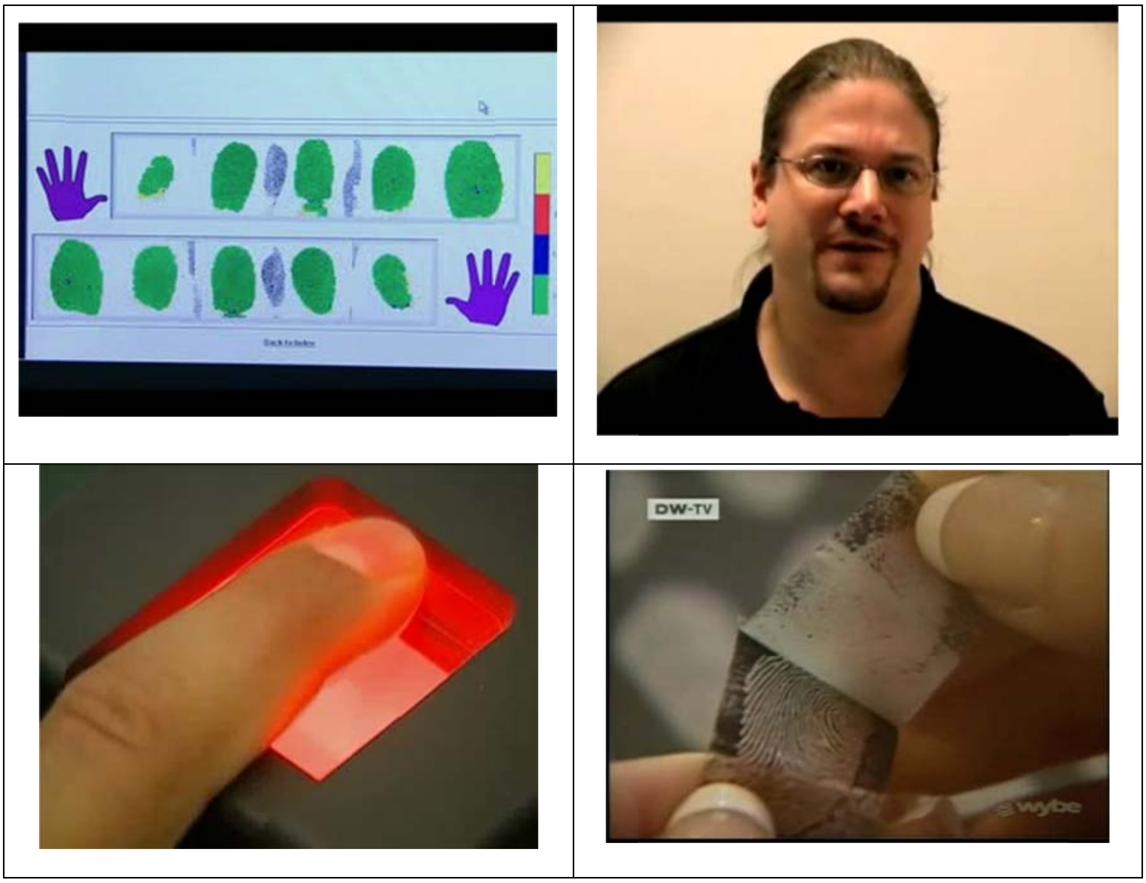


Figure 4.1: Screen shots from stimuli videos (from left to right): IPS video entitled *Identity Cards Scheme: A summary*; No2ID video response (which, in the end, was not used); News report explaining biometric passports in Germany; Second news report on insecurities in the German biometric passport

My original intention was to hold focus groups with a wide range of relevant social groups who were identified by the Home Office and other authorities as being required to enroll early in the NIS. That way, the sampling rationale would be pre-decide. Table 4.2 lists these groups and why they were originally selected to participate in the focus group interviews.

| Social group | Reason for inclusion |
|---|---|
| **Airport workers** | Targeted by government in its *Delivery Plan* (IPS 2008c) |
| **Foreign nationals** – particularly non-EEA students; those on discretionary leave; those in marriages or civil and common law partnerships; children of parents already settled in the UK; and those with work permits | Targeted by the Home Office and Border and Immigration Agency (BIA 2008) |
| **Young people** (i.e., students) | Targeted by government in its *Delivery Plan* (IPS 2008c) |
| **People renewing the passports** | Eventually, those renewing their passports were to be automatically enrolled on the NIR |
| Those in **positions of trust** who require a criminal background (Criminal Records Bureau (CRB)) check, including certain public sector workers, and possibly those working with vulnerable children | Mentioned in a leaked government document, entitled *National Identity Scheme Options Analysis – Outcome* (IPS 2007a) |

Table 4.2: Original social groups deemed of interest to the research project

However, as I began approaching representatives from these groups, particularly airport workers, I encountered some recruitment challenges. Initially, the union representatives for the airport workers (affiliated with the *Unite* union) showed interest in participating in group interviews, and even offered for me to come to Heathrow airport and use their facilities, but their interest waned shortly thereafter.[10]

I also sought to interview refugees in Belfast because of their unique status in the country and because asylum seekers are already required to hold a

[10] Coincidentally, this was around the time that Terminal 5 opened at Heathrow and the resulting chaos around lost baggage and cancelled flights (BBC News 2008) spoiled my chances of meeting with the airport workers there.

biometric identity document (known as the Application Registration Card (ARC)). Having arranged an interview in Belfast through the Northern Ireland Community for Refugees and Asylum Seekers (NICRAS) in March 2008, no one showed up at the meeting. Likewise, I faced problems identifying people in the process of renewing their passports and so they were also dropped from my interview schedule, as were those in the process of undergoing CRB checks, as it was revealed that the proposed policy requiring them to be one of the first groups to enroll in the Scheme was not certain. Other planned interviews (with students in the Sheffield area, for example) also failed to materialize.[11]

In the end I was able to complete 10 focus group interviews (including the initial pilot). Table 4.3 lists the pertinent information about these interviews.

[11] One of the lessons learned from the process of trying to arrange focus group meetings is that doing so without adequate financial resources and incentives for potential attendees can be a frustrating and unfruitful process.

| ID | Group type | Number of participants | Date | Venue |
|---|---|---|---|---|
| Pilot1 | Foreign national students at the LSE | 9 | 6 February 2008 | LSE |
| ForNat2 | Foreign national students at the LSE | 5 | 22 April 2008 | LSE |
| ForNat3 | Foreign nationals (IT professionals) | 7 | 28 April 2008 | LSE |
| ForNat4 | Summer school students on e-business course (foreign nationals) | 5 | 12 August 2008 | LSE |
| Stud5 | IS143[12] students | 12 | 12 December 2008 | LSE |
| Stud6 | IS143 students | 13 | 12 December 2008 | LSE |
| Stud7 | IS143 students | 12 | 12 December 2008 | LSE |
| Stud8 | IS143 students | 12 | 12 December 2008 | LSE |
| Stud9 | IS143 students | 13 | 14 December 2008 | LSE |
| Stud10 | IS143 students | 13 | 14 December 2008 | LSE |

Table 4.3: Focus group interviews

Many of the students were recruited from classes in which I was a teacher.

Others (such as those in ForNat3) were recruited through personal channels

[12] IS143 is a first-year undergraduate course at the London School of Economics and Political Science. The course, named ‘Information Technology and Society’, explores social and political aspects of information and communication technology.

at the university. Thus, these were very much convenience (non-probability) sampling methods.

Each of these interviews was audio recorded and later analyzed by the author. Notes were taken throughout the discussions and entered into a journal. I also adapted a technique known as ‘interviewing the moderator’, which is an ancillary method to focus group interviewing (Traulsen et al. 2004). Immediately following each focus group I would interview the moderator (that is, myself[13]), asking a number of prepared questions about the group dynamic during the interview, the composition of the group, how they reacted to the questions, issues relating to surveillance, privacy, or the government (as the sponsor actor), and anything that might have been said off the record (that is, after the recorder had been switched off). This technique provided me with immediate feedback on the data and furnished additional data for later consideration. It also introduced an important degree of reflexivity in the interviewing process. (See Appendix 2 for the ‘interviewing the moderating’ guide used.)

As part of that reflexive process, I came to realize that these conversations were lacking a certain level of depth. It is not that they were not interesting or insightful. Rather, the interviewees often seemed reluctant to engage the topic

[13] Typically, team members on the research project conduct these interviews, but as this is a PhD project, these interviews were, in practice, me completing a pre-written questionnaire.

and at times were concerned about providing the ‘right’ answer to my open-ended questions. Part of this, I believe, is related to the fact that many of these conversations were with students who viewed me as an instructor (in many cases I was their class teacher) and not an equal peer in the discussion, despite my initial pleas that I was not there to teach them. I expected this sort of dynamic to emerge and had even thought through how to manage it, but sometimes this did not always work as planned, plausibly partly due to my inexperience.

An arguably more important methodological insight from these interviews was that many people were simply unsure about the topic. Biometrics are, still, a very new thing and to expect people to ‘get their heads’ around the main ideas and ‘generate data’ in an hour long group interview might have been simply too much to ask. It was upon this reflection that I decided that I needed to begin focusing more closely on public discourses around biometrics. That is not to say that the focus groups were all for naught – quite the opposite. These discussions provided me with a renewed perspective on the issues, coming from the very people who soon were supposed to be using these technologies, with which to return to the stock of public knowledge found in policy documents and begin a process of systematic analysis.

## Data collection methods for government communications on biometrics

Following the exploratory phase of my project, I began an exhaustive collection of relevant government communications around the Scheme. The already sizeable archive obtained from the LSE Identity Project was supplemented with various other texts that I had collected since starting my research project. These were documents published through the IPS's web site, along with other communications about the Scheme. The final corpus included every known public government document relating to the NIS, published within the specified research time frame (July 2002-December 2008). In total, there were 129 documents in this corpus, including:

- Legislative or parliamentary publications (such as the *Identity Cards Bill* or parliamentary committee reports)
- Research publications (including feasibility studies and tracking research)
- Corporate publications (such as business plans, delivery plans, and contracts)
- Speeches (with written transcripts)
- PowerPoint presentations by civil servants and ministers
- Interviews and interactive web chats
- Monthly newsletters (published by the IPS)
- Leaked government documents (which were made available to No2ID and subsequently published on-line)
- Publicly-available responses to Freedom of Information requests

These documents are listed in Appendix 3.

The use of such documents is well-established in social research (Prior 2003). To cope with the “attractive nuisance” of qualitative data (Miles 1979), this corpus was then indexed in its entirety in the ATLAS.ti software for analysis (version 6, with native PDF support). (Below I explain my coding techniques, rationale, and analysis methods.)

My familiarity with the historical development of the case and the larger political context in which the NIS took place, along with the formal coding of government documents, then allowed me to identify a number of “critical incidents” (Miles & Huberman 1994),“moments of interest” (Hosein 2002), or “watershed events” (Bauer 2002, p.146) within and around the Scheme’s development. These were moments when there was increased activity around or public interest in the Scheme, which spurred public discourse and deliberation about the program and, in particular, the role of biometrics. These included:

| Critical event | Date | Period for which data is collected |
|---|---|---|
| The re-introduction of the *Identity Cards Bill* to Parliament following the general election of 2005, which coincided with the publication of a report by the consultancy, Atos Origin, with the findings from a trial of biometrics | 25 May 2005 | 25 May 2005 – 25 June 2005 |
| The day the *Identity Cards Bill* received Royal Assent, thus becoming the *Identity Cards Act 2006* | 30 March 2006 | 30 March 2006 – 6 April 2006 |
| The period in which iris biometrics began to be downplayed in policy communications | December 2006 - January 2007 | December 2006 - January 2007 |
| The publication of the *National Identity Scheme Strategic Supplier Framework* | 9 August 2007 | 9-17 August 2007 |
| The period following the HMRC data breach | 20 November 2007 | 20-28 November 2007 |
| The launch of the foreign national ID card, which coincided with the move to the market for biometric enrollment through the publication of the Front Office Services Prospectus document by the IPS | November 2008 – December 2008 | November 2008 – December 2008 |

Table 4.4: Critical moments for biometrics in the NIS

In chapter 5 I explain in-depth the rationale behind selecting each of these critical moments and why they are important to the case study. In this section, I describe the data that were collected around these moments. These data included both parliamentary debates about biometrics, captured in Hansard, and mainstream media (i.e., newspaper) coverage about the Scheme. Whereas the first corpus of government publications included all the available data published about the identity cards program, these two data sets were much more selective and focused around the six events listed above.

## Hansard

One of the interesting methodological aspects of studying a high-profile, national e-government system such as the NIS in the UK is the existence of Hansard and the historical record it provides to researchers. Hansard is the official transcript of parliamentary debates in the Westminster system of government and is a rich source of political discourse. As Bayley notes, “parliaments are institutions dedicated to talk; members of parliament debate legislative proposals and scrutinize the work of governments through questioning” (2004, p.1). These debates can be lively affairs and they offer an opportunity for parliamentarians to engage in relatively spontaneous discussion about issues. While much of the agenda is prepared in advance, when compared to the official published reports on the same matters, which are reviewed many times over and carefully edited before their release, parliamentary debate is somewhat freer and more dialogic.

I chose to include these parliamentary discourses about biometrics in the NIS as a second dataset. To do so, I searched the archives for the Commons Hansard Debates, Commons Written Answers, Lords Hansard Debates, and Lords Written Answers around the six periods listed above. Along with the transcripts of parliamentary debates, Hansard also publishes written answers given by ministers in response to questions formally posed by members. These data were usually collected the week following the event, but occasionally longer if the event itself was an extended affair (such as when officials first started downplaying iris biometrics in their official communications). My search terms in the Hansard archives were:

- biometric*
- finger*
- iris
- retina
- facial
- face
- DNA

The search results were filtered for relevance (to ensure they were about the NIS, which defined the case), indexed as a separate hermeneutical unit in ATLAS.ti, and then coded and analyzed. Appendix 4 lists information on the Hansard debates analyzed in this thesis.

## Data collection methods for media coverage on biometrics

Writing about public political discourse, Bayley argues that “the arena for political debate has shifted in the last fifty years from Parliament to the mass media, which have arguably become the principal organ for the communication of political ideas” (2004, p.11). Therefore, in addition to capturing the parliamentary discourses on biometrics around the moments of special interest, I also explored mainstream newspaper reports about biometrics within the NIS. Research within the public understanding of science has championed the analysis of press coverage in studying how new science and technology enter public discourse (Gregory & Miller 2000; Bauer 2000), as has recent IS research on IT innovation (e.g., Wang 2009). There is even some emerging surveillance studies and privacy research that focuses on media representations (Hoofnagle 2009; Finn & McCahill 2010).

To gather the media stories I logged onto the Nexis on-line archive service and performed an initial search of major UK newspapers, including the following broadsheets and tabloids:

1. The Guardian
2. The Independent
3. The Daily Telegraph
4. Daily Mail
5. The Mail on Sunday
6. The Times
7. The Mirror
8. The Sunday Mirror

9. The Sun
10. News of the World
11. The Express
12. The Observer
13. The Sunday Times
14. Independent on Sunday
15. Sunday Telegraph
16. The Sunday Express

As the Financial Times is not indexed by Nexis, I paid for a subscription in order to access its archive and download the relevant articles.[14]

17. Financial Times

I downloaded all the articles published in these outlets from 25 May 2005 until the end of December 2008 that included any of the following terms:

- "ID card"
- "identity card"
- "national identity scheme"
- "national identity register"

These articles were then indexed in ATLAS.ti and filtered for relevance. For example, any report including the term "identity card" which was not about the UK's identity card program was ignored. In total, there were 354 newspaper reports within the final sample. These reports were subsequently coded and analyzed, with an emphasis on discourses about and portrayals of biometrics. In the same fashion as the Hansard data, I targeted the data analysis around

[14] My aim in including such a wide variety of newspapers in my search was to capture the widest possible range of media discourses about the NIS and biometrics. These selections span the UK political spectrum and include both left-leaning and right-leaning newspapers, as well as those of the tabloid and business variety.

the six moments of interest to see whether and how these events were represented in the media. Figure 4.5 represents the frequency of UK media reports with references to identity cards or the National Identity Scheme, spanning 25 May 2005 to the end of 2008, and inclusive of all 17 newspapers listed above. The red areas depict the periods for which I conducted the extensive critical discourse analysis, focusing on discourses on biometrics present in the newspaper coverage.

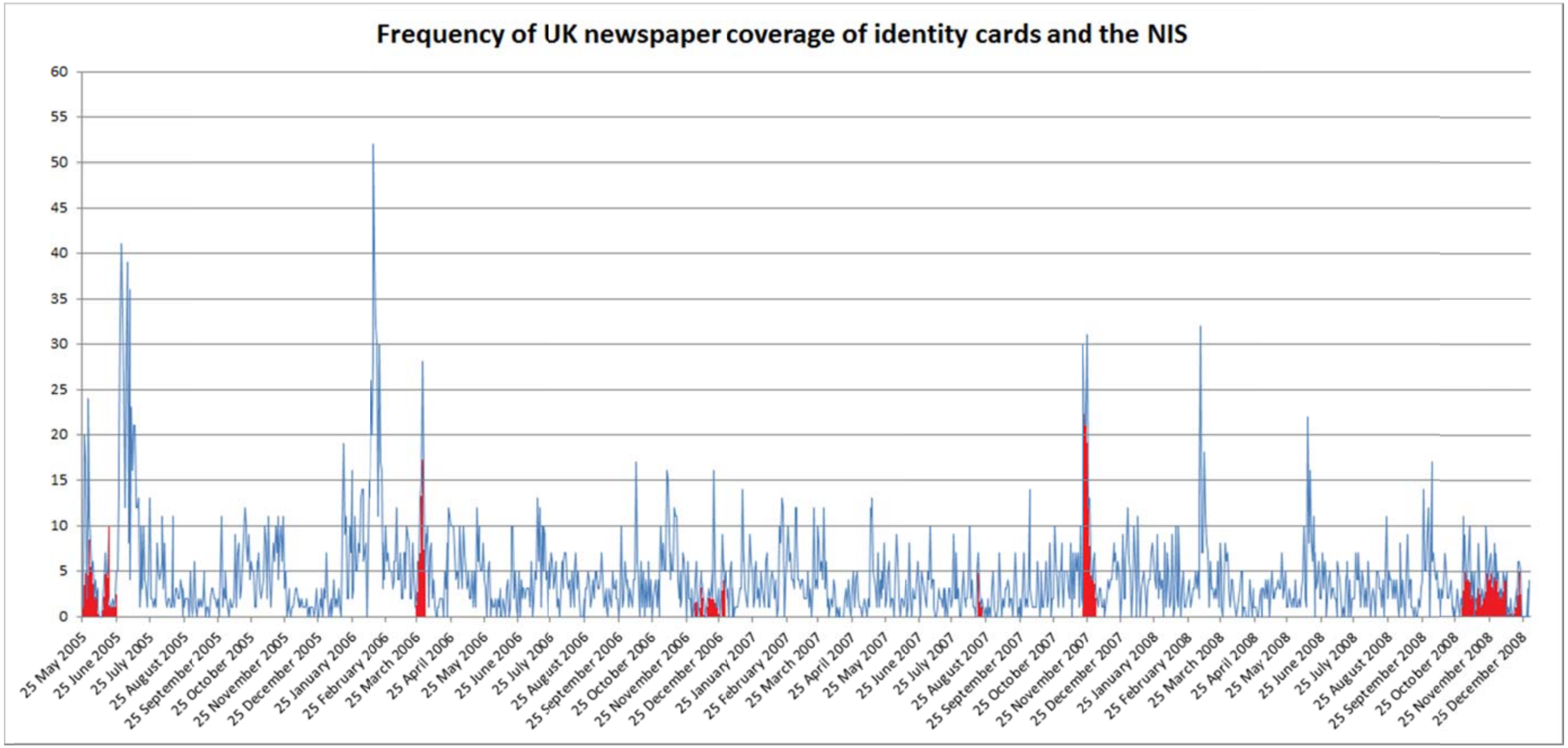


Table 4.5: Frequency of UK newspaper coverage on the topics of identity cards and the National Identity Scheme (the areas shaded in red represent the periods for which I performed the critical discourse analysis on the topic of biometrics)

As with my multiple and hermeneutical readings of the policy communications, my iterative and redundant readings of the media reports on biometrics over time granted my analysis an inestimable hermeneutical component. It provided me with a much broader understanding of the various happenings throughout the case and how they interrelated. It also helped to ensure that my research was rigorous by forcing repetitive readings of events from multiple perspectives.

## Data analysis

The distinction between data collection and data analysis is especially problematic for qualitative research. During the collection phase, researchers almost always informally ‘analyze’ as they order and categorize their data. Such is the nature of qualitative data that these decisions made in the early stages of data collection have analytical effects. For example, deciding to focus on certain ‘critical’ moments as a means to make the data more manageable and revealing can be considered a type of analysis. The point being, interpretation of data begins well before any formal analysis commences.

Yet, a formal and systemic analysis is critical to any serious research project. In this section I explain and justify my analytical approach and choice of analytical technique: critical discourse analysis.

## 4.3 Critical discourse analysis

Once each of the datasets was loaded into ATLAS.ti, I coded them according to principles and techniques from critical discourse analysis, starting with the main corpus of government publications on the NIS, then moving on to the media reportage and finally the data originating from Hansard.

According to Fairclough (2010), critical discourse analysis consists of three main properties. First, it is a relational form of research. This means that its focus is not entirely on entities or people, but rather social relations, which can be complex and layered (p.3). Discourse is relational in both an internal sense (i.e., discourse is a complex network of communicative relations between people and texts), as well as in an external sense (i.e., discourse is also often about objects in the world, which are interconnected via social activity). Fairclough is keen to stress that discourse is not some simple, discrete thing that can be defined independently. It is arrived at by analyzing social relations. And by studying discourse we better understand meaning and the processes of meaning-making.

Second, discourse is said to be dialectical in that these relations are between things which are different from one another yet not totally discrete. Fairclough's favorite illustration of this dialectical nature of discourse is the relationship between power and discourse. Power is, in part, discursive (insofar as power depends on discourse to sustain legitimacy), but power is not totally discursive (as it can also rely on physical force or resort to violence). Power is partly discursive and discourse is partly power – they 'flow into' one other, as he puts it. "The complex realities of power relations are 'condensed' and simplified in discourse" (Fairclough 2010, p.4).

Third, when we study discourse, we are not studying it in and of itself. Instead, we are studying the dialectal relations between discourse and other phenomena. Critical discourse analysis is therefore *trans*disciplinary, for analyzing discourse and the relations it renders involves cutting across disciplines such as linguistics, politics, sociology, information systems, etc. (Fairclough 2010, p.4).

Fairclough describes his approach to studying discourse as a form of critical realism, which acknowledges that there is a real world which exists irrespective of our knowledge and understanding of it. Within this worldview he believes there is a social world, which is separate from the natural world, and depends on human activity for its existence. The social world is a construct made possible *through* discourse.

Parker (1992) identifies twenty steps to analyzing discourse critically.

1) Discourse is realized in texts, which are the primary objects of study.

2) The connotations in these texts must be explored through methods of free association. Johnstone (2002, p.8) builds on this point by suggesting that “the basic questions a discourse analyst must ask are: Why is this text the way it is? Why is it not another way? Why these particular words in this particular order?”

3) As discourse is about objects, the analyst must ask what objects are being referred to and describe them in detail.

4) This involves talking about the text “as if it were an object”.

5) Discourse contains subjects, so analysts should specify what *types* of person or thing about spoken about.

6) The analyst must also speculate about what these subjects are capable of saying in the discourse.

7) As a system of meaning, a discourse maps a picture of the world.

8) It is incumbent upon the analyst to understand how texts use discourse to deal with meanings that run counter to their own; i.e., counter-discourses.

9) Discourse refers to other discourses, so contrasting these discourses is a valuable means of understanding.

10) Identify where discourses overlap and talk about similar objects in different ways.

11) Explore how discourses address different audiences.

12) Reflect on how those speakers label their own talk.

13) As discourses are historically located, examine how and where they emerge.

14) Describe how they change.

15) As discourses support institutions, the analyst must discover which institutions benefit from a given discourse.

16) And those institutions that suffer from discourses.

17) Identify which persons benefit from a discourse.

18) Who would promote such discourses and who would rather avoid them?

19) Demonstrate the extent to which a discourse connects with other, oppressive discourses.

20) Show how discourse allows dominant groups to subjugate less powerful groups.

Reflecting on these steps, a critical discourse analysis naturally involves the study of texts and therefore requires some form of linguistic analysis. In particular, the micro-analysis of texts is a form of coding which is designed to break open textual data so that the analyst considers all the possible meanings of a term or phrase (Corbin & Strauss 2008, p.59). Micro-analysis focuses on the minute details of language use – “it is like using a high-powered microscope to examine each piece of data close up” (Corbin & Strauss 2008, p.59). Micro-analysis involves meticulously coding around a concept. Importantly, any micro-analysis of a text must also link to a social analysis of the practices, organizations, and institutions which produced the text (Fairclough 2010, p.7). I employed such a micro-analysis technique in my coding. (See Appendix 5 for a screen shot of what this micro-analysis technique looked like in practice.)

Elsewhere, Fairclough (1995) explores the analysis of media discourse and what is special about these texts. His aim is to show how a critical analysis of media language can be recognized as an important element within research on contemporary processes of social and cultural change. He describes the ‘conversationalization’ of the public language of science and technology (p.9). Conversational language is realized through the use of linguistic features such as colloquial vocabulary and idioms. Conversationalization helps to democratize science and technology, making it more accessible by raising the status of the language and experience of ordinary life by recasting science in lay terms and rejecting the perceived elitism of science (pp.13-14).

One objection to discourse analysis of media texts comes from scholars of media receptions, who disagree with the analytical focus on meaning and ideological effects, without taking into account how texts are actually received by audiences. They argue that texts do not have unitary meanings and can be interpreted in various ways by different audiences and individual audience members. This is a fair point, but while interpretations may vary, any reading of a text is a product of an interface between the properties of the text and the interpretative resources and practices which the interpreter brings to bear upon the text (Fairclough 1995, p.16). The range of potential interpretations is always constrained by and delimited according to the nature of the text in question. Textual analysis remains a central element of media analysis, though it should be complemented by analysis of text reception, where possible, as well as by analyses of the production of media texts.

Texts can also be seen as a set of options: selections among available forms of language, in which one word was chosen rather than another, or where one grammatical structure was used instead of another. These formal choices constitute choices of meaning. Such a view of texts encourages the analyst to be sensitive to absences from a text – to explore the choices which were not made but which might have been made. That is to ask, how else might this phrase or utterance have been put? (Fairclough 1995, p.18).

What is *critical* about critical discourse analysis? Fairclough argues that it requires a degree of normativity in the analysis, focusing on social, organizational, and institutional wrongs and how the researcher can right them. This implies that the analysis is rooted in a set of values – views about what constitutes 'the good' – with which to evaluate a state of affairs. While these values are always specific to a particular society and culture, Fairclough's main argument is that the researcher is in a special position to understand what exists, how it could be otherwise, and how things should be based on some coherent set of norms and values (Fairclough 2010, p.7).

## 4.4 Coding discourses about new technology

To guide and structure the critical discourse analysis, I opted to code the data on government discourses around the seven high-level dimensions related to new IT offered by Orlikowski and Gash (1992). These dimensions are as follows:

| Dimension | Definition | Components |
|---|---|---|
| 1. Philosophy towards technology | Beliefs and assumptions about technology and information technology in general, as held by self and perceptions of organizations' philosophy | Personal philosophy<br>Organizational philosophy |
| 2. Issues around initiation | Knowledge and experiences of the initiation stage of a specific technology, including background, participants, feasibility assessments, and perceptions of the technology's objectives, utility, and importance | Rationale/history<br>Costs/benefits<br>Decision process<br>Managerial support |
| 3. Issues around implementation | Knowledge and experience of the implementation process of a specific technology, including background, participants, stages, design issues, support from users, managers, technologists, and others | Involvement<br>Barriers/facilitators<br>Cost/scope/time frame<br>Training<br>Managerial support |
| 4. Issues around | Knowledge and experiences of the use of a | Customization |

| Dimension | Definition | Components |
|---|---|---|
| use | specific technology, including frequency and discretion of use, level of customization, satisfaction, technical support, maintenance requirements, and expectations and experiences about the technology's criticality, ease of use, usefulness, quality, reliability, integrity, and availability | Maintenance<br>Technology attributes |
| 5. Criteria of success | Beliefs about how the success of a specific technology is being or should be assessed, and which particular criteria and measures are or should be used. Assessment of how a specific technology is meeting these criteria | Criteria<br>Measures<br>Experiences |
| 6. Impact | Expectations or experiences about the impact of a specific technology on the strategy, structure, culture, and way of doing business, as well as how a specific technology should or has/will change jobs, tasks, autonomy, control mechanisms, skills/knowledge, responsibility, social relations, status, workload and stress | Organization-wide effects<br>Task-level effects<br>Individual effects |
| 7. Relations with other players in the computing social world | Expectations and experiences about the frequency and extent of interaction with other  players about IT, the nature of the interaction including the role played in this relationship, and perceptions of attitude towards and understanding of technology | Managers (senior, middle)<br>Technologists<br>Users<br>Third parties |

Table 4.6: Dimensions, definitions, and components of technological change (Orlikowski & Gash 1992)

These dimensions span general philosophical orientations toward technology; personal perceptions about how technology is to be initiated, implemented, and used within an organization; perspectives on how to measure and determine success; expectations of the technology's impact on the organization; and how the technology implicates others in the organization (and beyond).

Orlikowski and Gash’s objective is to track the shifts in the technological frames of managers, technologists, and users over time to understand better technology-motivated organizational change. By comparing frames across groups longitudinally, they believe the researcher can better understand the sources of conflict that arise from the introduction of new technology, the barriers to change, and both the intended and unintended outcomes (1992, p.9).

These dimensions provide the overall structure for the presentation of the first part of the analysis (in chapter 6).

# Chapter 5: Introducing the case study

## 5.1 Identifying the actors

Due to the intended scope of the proposals, the case of the National Identity Scheme (NIS) involved many different actors.[15] Therefore, before beginning the in-depth analysis of biometrics within these proposals, the immediate aim is to identify the main players and their interrelationships. This will help to situate and clarify the analysis of the contest of discourses about biometrics. These various actors spoke for biometrics in varying capacities and through assorted media (including policy documents, conference presentations, newspaper interviews, and on-line forums) over the course of the Scheme's existence.

In particular, when I speak of 'officials' or 'the government' throughout the analysis, I am using these terms as a form of short-hand to capture those politicians and decision-makers within certain governmental agencies, who were responsible for, or provided policy assistance to, the NIS under the Labour government. These actors ranged widely and changed frequently as

[15] These actors are an elaboration of the resistance framework first presented in a published paper: "Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework" by Martin et al. (2009).

political careers ended and new blood was nominated, or through internal promotions and career changes in the civil service. Thus, the first major actor in this study ('the government') is actually a multitude of related, but distinct actors, including different government departments (and the civil servants therein) and various Labour party politicians.

- Government departments and their sub-departments
    - Home Office
        - Identity and Passport Service (IPS) (formerly known as the Passport Service and before that the Passport Agency)
        - Occasionally, the Borders Agency
    - Cabinet Office
        - Office of Government Commerce

- Labour politicians
    - Prime Ministers (Tony Blair and Gordon Brown)
    - Home Secretaries (David Blunkett, Charles Clarke, John Reid, Jacqui Smith)
    - Junior Ministers (Andy Burnham, Joan Ryan, Liam Byrne, Meg Hillier)

It is these official voices that are present in the vast majority of the policy communications analyzed in the first part of the analysis. Where possible and relevant, I assign specific individual-level attribution to quotations originating from these actors, although occasionally authorship is difficult to discern (as in reports from the Home Office).

There are also the branches of Parliament that played an important role in the Scheme's development though their oversight of the proposals and publication of regular reports related to the government's plans for identity cards. These include:

- Branches of Parliament
    - Home Affairs Select Committee (House of Commons)
    - Select Committee on the Constitution (House of Lords)
    - Joint Committee on Human Rights (including members of both Houses)

The Parliamentary record of the extended debates on the identity cards program, captured by Hansard, also gives voice to those members of the Labour party who did not support their leaders' proposals, as well as members of opposition parties such as the Conservatives and the Liberal Democrats. These actors had the capacity to speak for themselves in Parliament, and also in other settings such as at party conferences and at public events.

At times, local governmental bodies proved an interesting point of resistance to the Scheme, with certain councils such as those in Sheffield and Liverpool City vowing not to co-operate with the IPS during the roll-out of identity cards (Council of the City of Sheffield 2009; Anonymous 2009).

Other actors, such as the International Civil Aviation Organization (ICAO) and the EU are spoken *for* in the debates in relation to specifications and requirements for travel documents, for example.

- Other Parliamentary actors
    - Members of the Labour party who disagreed with the proposals
    - Opposition parties (Conservatives, Liberal Democrats) who disagreed with the proposals
    - Members of the Conservative and Liberal Democrats who were in favor of the proposals
- Local government organizations (such as councils)
- External actors (ICAO, the United States, the EU)

There are non-governmental actors as well, which are equally important to the story of biometrics, originating in civil society, the scientific community, and academia. Sometimes they are spoken for; other times they speak for themselves. These actors emerge in different ways, depending on the occasion and the medium. For example, in some policy-related communications such as the consultation documents, the views of the police, unions, activists, experts, and academics emerge. On other occasions, these actors manifest themselves in parliamentary debates, when for example parliamentarians pose questions to ministers about an expert report on biometrics or the view of activists regarding the efficacy of biometrics in preventing identity fraud.

- Civil society groups (including No2ID and Privacy International, among others)
- Experts (Biometrics Expert Groups, Biometrics Assurance Group, Independent Scheme Assurance Panel)
- Academics (such as the LSE Identity Project and the Foundation for Information Policy Research)

Certain of the commercial documents published by the IPS gave rise to commercial actors and other potential business partners, including those that eventually bid for contracts, those that did not, and those that withdrew from the commercial process. Some of these actors re-emerge in the media reports about the Scheme, especially in the more business-oriented Financial Times.

- Commercial actors and potential business partners (e.g., Accenture, BAE Systems, CSC, EDS, Fujitsu, IBM, Steria, Thales, the Post Office, etc.)

The media played a special role in reporting developments around the NIS – arguably one of the most highly publicized e-government programs in recent history in the UK – by framing the issues and regularly refreshing the meanings and significance of the proposals for identity cards. Social science research has established that the media play an important role in the general social psychology and the formation of public opinion about social issues (e.g., Gamson & Modigliani 1989). Indeed, studies of the public's understanding of scientific and technological controversies take this media content and treat it as a cultural indicator of public perception (Bauer 2000).

- Media (newspapers and on-line media (such as blogs and the specialist information technology magazines))

And, of course, the ‘public’ make regular appearances in these debates, represented by those who participated in various ‘customer experience’ studies, the survey respondents whose opinions are analyzed in various government-commissioned reports, and the participants on the *mylifemyid* web site (an on-line space created by the Home Office where young people were asked to share their opinions about the government’s plans), among many other outlets. The public is also frequently spoken for by politicians who reiterate how strongly the public supported the government’s proposals, for example; or by activists who present counterarguments about how the public actually detested plans for identity cards. Indeed, the public is continually constructed in these discourses by those seeking to enroll them in their rhetoric, either positively or negatively, about the NIS. This discursive construction of ‘publics’ and their relationship with the identity cards program and biometrics will be discussed further in the analysis and discussion chapters.

Naturally, there are countless other actors that I have not listed here. The point is not to enumerate each and every actor in the relatively short history of the NIS, but rather to highlight the main players in this case study, and particularly those relevant to an exploration of public discourses about biometrics.

## 5.2 A brief history of biometrics in the National Identity Scheme

The history of biometrics in the NIS is, in a way, rather ambiguous and irregular. Recall that biometrics were only one small part of a much larger set of plans for a national identity program in the UK, which was to include other technologies such as 'smart' cards and new databases for storing citizen's identity-related information. Non-technological components included new legal powers for enrolling people into the program and data-sharing mechanisms, and even a new government sub-department (i.e., the IPS) to house and administer the program.[16] There was thus a lot more to the Scheme than just the introduction of biometrics.

In many of the documents that I analyzed, biometrics received very little attention, and if they were mentioned at all it was in passing. More often than not the focus was on outlining why identity cards were necessary or on cost-related matters, which became an issue of top priority following the publication of the LSE Identity Project's report on the Scheme, which questioned the government's costing of the program (among other issues). In those

[16] For an extensive history of the National Identity Scheme, see Whitley & Hosein (2010, chap.3-4)

documents in which biometrics were not the focus, there was very little substance on which to build an analysis. However, in other documents the topic of biometrics was treated much more considerably and extensively. It is from these documents that we can ascertain the history of proposals for biometrics within the government's plans for identity cards. A review of this history will allow us to identify the most important moments relating to, or implicating biometrics, and from there we can proceed to the main discourse analysis.

First and foremost, the government's plans for biometrics as part of the Scheme were never fully explicit or certain. For example, when entitlement cards were first proposed by the Labour government in 2002 in a consultation paper, the use of biometrics was considered simply an "option" within a much larger proposal for an entitlement cards scheme. The inclusion of biometrics was said to be ultimately dependent on the feasibility, cost-effectiveness, and, importantly, public acceptance of the Home Office's proposals.

> Another *option* which the Government would like to explore is the recording of biometric information as part of a card scheme. This would take the form of recording a fingerprint scan or the image of a person's iris (the coloured ring around the eye) as well as a digital photograph which is already taken for passports and driving licences. There would be strict controls on how this information was used. If it proved feasible and cost-effective, recording this information would greatly reduce the ability of fraudsters to create multiple false identities and provide a powerful way for people to prevent their own identities from being stolen. However it is also important that the introduction of this technology should be acceptable to the general public and the Government would

> like to use this consultation exercise to seek people's views. This means whether it would be acceptable in principle for this information to be recorded and also whether it would be acceptable in practice as people would need to go somewhere where the appropriate recording equipment was installed when they applied for a card. (Home Office 2002, p.2, emphasis added)

Eventually this “option” for biometrics became a requirement, enshrined in the *Identity Cards Act 2006*, although the specifics around biometrics in the Scheme would remain fuzzy throughout the life of the proposals. For example, the decision about which biometrics the government would use to identify citizens was never firm. It was deliberately technology-neutral. While facial photographs were always considered the most viable and practicable option, they were not always spoken about as “biometric” and instead were sometimes treated differently. (I explore this categorical tension in-depth in the next chapter).

Fingerprints, the most publicly recognizable biometric, were also subject to uncertainty in the government’s plans. For example, the original thinking was to collect only four fingerprints from citizens.

> Modern fingerprinting systems no longer require fingers to be inked and then rolled onto paper. Electronic scanners are now used but these still require well trained staff to ensure that fingerprints are properly scanned. The Government envisages a much simpler scanning system than that used by the police or the Immigration Service, *which would probably involve just the scanning of four fingers.* (Home Office 2002, p.105, emphasis added)

However, the number of fingerprints to be scanned soon increased to ten – a policy decision that seemed as certain as any in the NIS until a leaked government document, made public by the activist group No2ID (2007b), revealed that the apparently settled policy for everyone to enroll ten fingerprints was not necessarily set in stone. In a bullet point in the "Options Analysis" document, unnamed decision-makers conceded that the "nature of the group(s) selected drives the requirement for the [biometrics] infrastructure (especially face vs. fingerprints)" (IPS 2007a, p.2). No2ID interpreted this disclosure as an "indication that dropping fingerprints is being considered for some groups. This blows apart the government's whole case for the ID scheme, which rests on 'biometrically securing' personal information and preventing multiple/fraudulent applications through biometric cross-checking" (No2ID's annotations in IPS 2007a, p.2).

Iris biometrics, on the other hand, were regularly described as a future option and were never a guarantee in the NIS. This was despite many bold claims made by government officials about what the program was supposed to achieve – claims which many experts agreed were impossible without incorporating robust and scalable technology such as iris biometrics from the outset. For example, claims about effective one-to-many biometric searches using fingerprint records in a fully populated NIS were deemed far-fetched by experts, who argued that only iris biometrics were capable of performing on this scale.

In 2004, the (then) UK Passport Service commissioned Atos Origin, a consultancy, to conduct a biometrics enrollment trial to “help inform the Government’s plans to introduce biometrics to support improved identity authentication and help prevent identity fraud” (Atos Origin 2005, p.3). The trial included more than 10,000 participants from across the UK, who had their face, fingerprint, and iris biometrics recorded and subsequently verified. The trial was not a success in terms of demonstrating technological reliability, with many of the biometrics performing quite poorly (e.g., 39% of 750 disabled participants were unable to enroll their iris biometrics). These results led critics to question the reliability of biometrics and their proposed use in a national identity system. However, the final report on the trial stressed that its objective was *not* to test biometric technology, but rather to “test the processes and record customer experience and attitude” (Atos Origin 2005, p.3). That is, to test the system’s user friendliness, but not the technology’s reliability. For some, this distinction was disingenuous and simply a way to cover up bad results (see, for example, Moss 2009).

Then in 2005, the UK Passport Service held a “biometrics roadshow” at different locations across the country, where the public was invited to try out biometrics in order to raise awareness about the technology. Members of the public were able to have their irises and fingerprints recorded. At the time, then-Home Office minister Andy Burnham said: “This roadshow is very much a hands-on experience and people will be able to see for themselves how biometrics work and what advantages they can bring in safeguarding our identities” (Burnham, as quoted in McCue 2005).

The role of expertise and expert oversight is another notable, if not curious, theme in the history of biometrics in the Scheme. In 2004, the Home Affairs Committee recommended that the government’s Chief Scientific Officer oversee the development of biometrics in the Scheme (p.59), but this apparently never happened. Instead, a Biometrics Assurance Group was eventually formed, which comprised of experts in biometrics who were expected to review the biometric components of the Scheme. This group released two reports, in 2007 and 2008, but was disbanded thereafter for reasons that remain unclear.  It is also uncertain what influence their policy guidance and recommendations had on the plans for biometrics in the Scheme.

Another major biometrics-related policy change was the decision for the Home Office not to enroll biometrics in-house, but rather to look to the market for ways of outsourcing this function. This decision, publicized in 2008, was an apparent attempt to reduce the cost to the Home Office of recording people's biometrics, with the idea being that people would pay out-of-pocket to enroll their own biometrics at a high street location such as the Post Office or pharmacy. While this move to the market never reached fruition (as the Scheme was scrapped before the contracting processes were complete), the desire to offload this aspect of the Scheme onto third parties represents an important event in the history of the NIS.

## 5.3 Critical moments for biometrics

As already noted, the second half of the analysis is focused around six different events related to biometrics that occurred as part of, or alongside, developments in the NIS. These are presented again in summary form in Table 5.1, with an explanation for their inclusion following.

| Critical event | Date | Period for which data is collected |
|---|---|---|
| The re-introduction of the *Identity Cards Bill* to Parliament following the general election of 2005, which coincided with the publication of a report by the consultancy, Atos Origin, with the findings from a trial of biometrics | 25 May 2005 | 25 May 2005 – 25 June 2005 |
| The day the *Identity Cards Bill* received Royal Assent, thus becoming the *Identity Cards Act 2006* | 30 March 2006 | 30 March 2006 – 6 April 2006 |
| The period in which iris biometrics began to be downplayed in policy communications | December 2006 - January 2007 | December 2006 - January 2007 |
| The publication of the *National Identity Scheme Strategic Supplier Framework* | 9 August 2007 | 9-17 August 2007 |
| The period following the HMRC data breach | 20 November 2007 | 20-28 November 2007 |
| The launch of the foreign national ID card, which coincided with the move to the market for biometric enrollment through the publication of the Front Office Services Prospectus document by the IPS | November 2008 – December 2008 | November 2008 – December 2008 |

Table 5.1: Critical moments for biometrics in the NIS

1. **The Identity Cards Bill:** The re-introduction of the *Identity Cards Bill* to Parliament after the general election of 2005 clearly marks an important

moment in the history of the Scheme. It followed nearly three years of consultations, impact assessments, and debates about the merits and drawbacks of a national identity card, as well as an unsuccessful attempt at passing the legislation during the previous Parliament. It also re-energized both Members of Parliament and activists, who further scrutinized the government's plans, including its proposals for biometrics. This event initiated a series of new battles within Parliament about certain controversial aspects of the proposed Scheme, a tug-of-war between the House of Commons and House of Lords regarding the bill's appropriateness, and a vocal public debate that played out in the popular press.

Coincidentally, the very same day as the re-introduction of the Bill, the government released research findings from the Atos Origin trial of biometrics enrollment. Certain of the findings from the trial also made their way into critical news reporting on the Scheme.

2. **The Bill becomes an Act:** This event signifies a political victory for the Labour government: the legislation of the Scheme, which was one of the party's election manifesto commitments. It follows almost a year of vitriolic political debate, including numerous amendments to the Bill's original text.

3. **Iris biometrics become even less certain:** Whereas hitherto iris biometrics were almost always listed as an option in the NIS, sometime in late 2006 they started disappearing or being downplayed in government discourses on the Scheme. This marks an important moment in the Scheme's history because it is widely accepted in the scientific and technological community that relying on fingerprints alone to 'uniquely identify' everyone in a national population of around 60 million people (the current size of the UK's population) is highly problematic. Yet, this unannounced policy shift did not noticeably affect the government's ambitions for biometrics in the Scheme.

To demonstrate this gradual policy shift: Iris biometrics were explicitly mentioned in the *Identity Cards Act 2006* ("biometric information is data about [an individual's] external characteristics, including, in particular, the features of an iris or of any other part of the eye"). The December 2006 *Strategic Action Plan* downplayed the role of irises, noting that "When you enrol into the Scheme, your fingerprint biometrics (all 10 fingerprints) will be recorded and stored in the National Identity Register…The introduction of iris biometrics also remains an option" (2006, p.16). Then the *Delivery Plan*, published in 2008, made no mention of iris technologies.

4. **Strategic Supplier Framework:** The publication of this document marked the beginning of the Home Office's procurement for the Scheme. It was intended

for commercial parties interested in bidding for work to help the government deliver its system. The document acknowledges that the government did not have the expertise, skills, and capacity to deliver the Scheme on its own. The government thus hoped for these bidders to become “long-term partners” of the IPS.

At the time, the document also represented the official current thinking of the IPS on the design of the Scheme, which went through various iterations during its existence.

5. **Her Majesty’s Revenue and Customs breaches data security and the public’s trust:** While this event was not directly related to the NIS, it had major consequences on official discourses about the government’s ability to secure citizens’ personal data and the role of biometrics in data security. A series of parliamentary debates and frenetic media reportage followed (then) Chancellor Alistair Darling’s announcement to Parliament that HRMC had lost two compact discs with the records of 25 million people. Among other things, these debates and media reports focused on whether the inclusion of biometrics would have prevented or lessened the impact of the breach. Certain statements in Parliament by members of the government regarding the capacity of biometrics to prevent lost data such as those in the HMRC dataset from being misused led a group of experts to openly criticize these

assertions as “a fairy tale view” of what biometrics are about (Anderson et al. 2007). This was an unusual and unexpected moment in which numerous parliamentarians opined openly and at length about biometrics.

6. **Launch of the foreign national ‘identity card’ and a move to the market for biometric enrollment services:** In November 2008 the Home Office began issuing the first biometric immigration documents to foreign nationals, regularly referring to them as ‘identity cards’. While technically not identity cards in the sense that they did not fall under the legal remit of *Identity Cards Act 2006*, they were publicized as such by government officials keen to show that the Scheme was on track and, indeed, a ‘reality’. As with the soon-to-be-issued UK national identity cards, these documents involved the collection of fingerprint biometrics and digital facial photographs from enrollees.

On the same day, the Home Office issued a prospectus in which it reached out to the market for help in providing a “biometric enrollment service”, with the idea being that companies would compete to collect citizens’ biometrics for the government in exchange for a fee. In selling this idea to potential service providers, the government also noted that further benefits to companies would include a new revenue stream, increased footfall, access to new customer segments, an association with a respected and trusted brand,

and goodwill generated by providing a valuable public service (IPS 2008f, p.5).

These events represent important moments for biometrics (and the organizations involved in trying to innovate them as part of the NIS). We will return to them again in chapter 7, where we analyze media reportage and parliamentary debates concerning the Scheme. In the next chapter, we focus on the government’s policy discourses regarding biometrics.

# Chapter 6: Analysis (I)

The security and reliability of biometrics are at the heart of the Government's case for their proposals [for a national ID card program]. We note that no comparable system of this size has been introduced anywhere in the world. *The system proposed would therefore be breaking new ground*. - House of Commons Home Affairs Committee (2004, p.4, emphasis added)

You're walking into Tesco for a tin of baked beans: "Hang on, I only want baked beans. What do you want my iris for?" - Focus group interviewee (cited from Cragg Ross Dawson 2004b, p.18)

As for the biometric technology, we have invaluable experience in managing biometric systems to draw on which will reduce our delivery risk. *People who suggest that this is novel, untried technology seem to forget that there are many operational successful biometric systems within government* - for example, we have over 6 million sets of fingerprints on police systems and hundreds of thousands of fingerprints taken for immigration purposes. - Joan Ryan, former Parliamentary Under Secretary of State for nationality, citizenship, and immigration at the Home Office (2006, p.3, emphasis added)

Biometric technologies will gather momentum over the coming years and we can expect improvements in technology and a deeper understanding of the management and operation of biometric systems. - Independent Scheme Assurance Panel (2008, p.15)

In fact, I don't actually think most of the general public think that the use of biometrics is in itself wrong, either for private transactions or for passports or whatever. – Former Prime Minister Gordon Brown (as cited in Watt 2008)

## 6.1 Introduction

This chapter opens with five quotations concerning the potential future use of biometrics in the National Identity Scheme (NIS). Each quotation depicts and frames the issues of biometrics in a different way.

In the first quotation, we are told by the Home Affairs Committee that the government's proposals for biometrics were groundbreaking – an innovation even – with questions about the security and reliability of biometrics at their core. The second quotation is from a member of the public, who was asked his opinion of the government's proposals. (He uses humor to emphasize valid concerns regarding the principle and proportionality of biometric checks.) Third is a short quotation from the Independent Scheme Assurance Panel, an independent advisory group tasked with overseeing the Scheme's development, which reflects a technologically deterministic view of biometrics. The fourth quotation re-frames the debate by stressing the government's important experience in operating and managing large-scale biometric systems – experience which would serve them well in the future, we are told. Last is a quotation from former Prime Minister Gordon Brown, who discursively frames a public that is willing to accept biometrics into their lives.

Each of these quotations speaks to important themes and issues around biometrics that will be explored in this chapter. Rarely does society face a proposal of such magnitude, complexity, and divisiveness – one which engenders such a wide range of reactions to and interpretations of a new technology. The UK's proposals for biometrics provide us with an opportunity to explore the diverse and shifting discourses that surrounded the attempted diffusion of a politically charged and controversial technological innovation.

As previously explained, the first part of the critical discourse analysis (this chapter) is structured around Orlikowski and Gash's (1992) seven dimensions of new technology (to reiterate, these are: philosophy towards technology, issues around initiation, issues around implementation, issues around use, criteria of success, impact, and relations with other players in the social computing world). The second part of the analysis (in the next chapter) is presented around the six moments of interest in the Scheme's history and analyzes the Hansard debates and media coverage around these moments.

To provide a flavor of the type of analysis I undertake in this chapter and the next, recall the following extended quotation, which first appeared in the previous chapter, regarding the "option" of using biometrics within the Scheme (which at the time was still being referred to by government as an entitlement card scheme).

> Another *option* which the Government would like to explore is the *recording of biometric information* as part of a card scheme. This would take the form of recording a fingerprint scan or the image of a person's iris (the coloured ring around the eye) as well as a digital photograph

> which is already taken for passports and driving licences. There would be strict controls on how this information was used. If it proved *feasible* and *cost-effective*, recording this information would greatly reduce the ability of fraudsters to create multiple false identities and provide a powerful way for people to prevent their own identities from being stolen. However it is also important that the introduction of this technology should be *acceptable to the general public* and the Government would like to use this consultation exercise to seek people's views. This means whether it would be acceptable in principle for this information to be recorded and also whether it would be acceptable in practice as people would need to go somewhere where the appropriate recording equipment was installed when they applied for a card. (Home Office 2002, p.2, emphasis added)

From the perspective of a critical discourse analysis, there is a lot to unpack in this passage from the government's initial proposal for biometrics. For one, note how biometrics are understood as "information" and how examples of biometrics are provided to elucidate the concept, along with short descriptions of each method. We are reminded that digital photographs are already a reality in other identity documents. The passage also speaks of "recording" and "scanning" biometrics – two very specific, technical processes. Certain problem frames immediately emerge in this passage as well, including how biometrics could help to prevent the use of fraudulent identities as well as secure our own identities from external threats. These are rhetorical trends that persisted over time as the government communicated its plans for the Scheme.

Second, note how the public is already brought into the fold, with the government promising public consultation and an assessment of public acceptance. In particular, the Home Office is keen to acknowledge the practical matter of requiring everyone to travel to some location to enroll their biometrics. This point draws on a frame of convenience.

In this first instance of proposing biometrics, the Home Office (under then-Home Secretary David Blunkett) was already expressing an interest in recording multiple biometrics (in this passage, a digital photograph, fingerprints, and irises). These three types of biometrics feature extensively throughout government discourses, although as discussed earlier, doubts around the use of irises (as well as fingerprints) did arise, bringing important rhetorical and practical consequences. For now it suffices to appreciate the immensity and complexity of such an undertaking such – one which aims to build a national identity system from scratch and collect multiple biometrics from an entire national population and certain foreign visitors.

For some, this early proposal for a national entitlement scheme (soon thereafter rebranded as a “National Identity Scheme”, and then again a “National Identity Service”) might be unproblematic. The extract appears to be a basic introduction to biometrics and some of the surrounding problems, such as identity fraud. However, from a critical discourse analysis perspective, one can make a number of important observations and insights. First, biometrics are described as “information”, which perhaps appears a natural way to describe them.

But another description of biometrics from the very same 2002 consultation document on entitlement cards states that they are:

> Things which you ‘are’ i.e. your biometric identity. These are *attributes* which are *unique to an individual* and include fingerprints, iris patterns (the coloured part of the eye around the pupil), *and DNA profile*. *Physical appearance can also be regarded as a form of biometric identity provided the method of checking it (e.g. computer analysis of physical features) is sophisticated enough to allow for changes e.g. growing a beard, ageing or minor cosmetic surgery.* (Home Office 2002, p.100, emphasis added)

Here biometrics are described as “attributes” rather than “information”. The authors at the Home Office list both fingerprints and iris patterns as examples of biometrics, along with DNA profiling. Considering the very different set of ethical, technical, and operational aspects that DNA engenders, it is a curious biometric to include as an example in a document on entitlement cards. But this is not the only occasion on which it is mentioned.

This second passage also states that physical appearance could be considered “a form of biometric identity”, assuming it satisfies certain technical requirements. This question of when a bodily feature is actually ‘biometric’ persists throughout the documents and discussions on the NIS, serving a key rhetorical function. We will return to this theme, for it is an important one in the case. Finally, here we also see another prominent theme emerge – that biometrics are ‘unique’ to an individual. This supposed advantage of biometrics is by far the most discussed benefit in the official discourses, and so the question of uniqueness is also something that will be explored in this chapter.

## 6.2 The essence of biometrics

Starting with Orlikowski and Gash’s first dimension relating to philosophical aspects of technology, in this section I want to explore the contested ontology of biometrics in government discourses. This involves reviewing the wide range of descriptive frames that the government used in policy documents and public statements to explain what biometrics ‘are’ (see Table 6.1). Thus far we have read that biometrics are ‘information’ but that they are also ‘attributes’. Perhaps this particular duality can be reconciled by describing biometrics as ‘information about attributes’, but other documents tell a different story about the potential ontology of biometrics. The descriptive frames that appear in government discourses on biometrics range from the literal and technical (e.g., biometrics as “data” or “technology”) through to the figurative (e.g., biometrics as a “safeguard” or a “gold standard”), and include the use of simile (e.g., biometrics as a “lock” on identity). Altogether, they reveal an ongoing process of sense-making around biometrics in government policy discourses.

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| **Markers** | “The concept of a biometric *marker* on key documents used as evidence of identity has attractions.” (Cabinet Office 2002) | This term has potentially negative connotations (i.e., “mark of the beast”). It was soon disused |
| **Attributes** | “Biometric identity: *attributes* that are unique to an individual, i.e. fingerprints, voice, retina, facial structure, DNA profile, and geometry, heat radiation, etc.” (House of Commons 2004) | Attributes are typically understood as properties that define an entity – this definition emphasizes those physical attributes that are “unique” to individuals |
| **Digital records** | “The Home Office described a biometric as ‘a *digital record* of a particular physical characteristic that is unique to each individual, such as fingerprints or the shape of a person’s face’.” (House of Commons Home Affairs Committee 2004) | Not just a record, but a digital one; like some of the others, this definition stresses the physical-ness and uniqueness of biometrics |
| A **concept** | “Initial responses to the use of biometrics depended largely on familiarity with the *concept*.” (Home Office 2004a) | A more philosophical understanding of biometrics |
| Part of the **gold standard** of identity | “The rigour of the application process and the uniqueness of the biometric will mean that, in time, the identity card will become the gold standard way of proving identity throughout the UK.” (Home Office 2004b) | In this analogy, biometrics are to identity as the gold standard is to the monetary system; that is, a stable and recognizable reference |

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| A **technology** | “Recent events have brought home how, in today's rapidly changing world, the need for trust and confidence actually require us to move beyond this and take the opportunity of new biometric *technology* which allows for a completely new level of verifying identity.” (Home Office 2004c) | Is this a single technology, or many? If the latter, what important issues are obscured by reference to a singular biometric technology? |
| **Information** | “Recording biometric *information* will take place at local and regional, convenient access points and will help to ensure that an identity record is associated with information unique to that person.” (Home Office 2004c) | Recordable information |
| A **use** | “Biometrics, the *use* of eyes, the *use* of fingerprints is now a certainty in a way that never was before so therefore identification either whether it be on border controls or whether we have to deal with stop and search in the street, anti-terrorism kind of activity or even along the normal way that police officers work would give a certainty we need.” (Home Office 2004d) | Here biometrics are explained, not in terms of information, data, or technology, but as a use of particular parts of the body; where is IT in this conceptualization? Furthermore, biometrics are spoken of as a certainty – as something that *will* happen |
| **Characteristics** | “A biometric is a unique personal physical *characteristic* such as a fingerprint or iris pattern.” (Atos Origin 2005) | As with attributes, characteristics are supposed to be distinctive |

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| A **procedure** or process | “There were few objections to biometric *procedures* among the able-bodied, but those with special issues expressed anxieties about the physical *process* and how it might cause them difficulties.  Muslim women also had worries about aspects of enrolment, particularly to do with possible physical contact and removal of hijab or burkha.” (Home Office 2005b) | This quotation picks up on the physical nature of the processes of biometric enrollment. It captures how biometrics can be seen as more than simply data or information, but rather as part of a larger set of processes and experiences |
| A **capability** | “In the future, foreign nationals will have to invest their time to travel to an enrolment centre for their biometrics to be recorded and pay an additional price for *biometric capability* of a product.” (Home Office 2005f) | This speaks to the understanding of biometrics as a facility or potentiality, rather than an actuality |
| **Images** | “The chip will hold data in line with International Civil Aviation Organization (ICAO) recommendations, including a biometric *image* of the bearer's face.” (IPS 2006a) | By this definition, a biometric can exist in the form of an image; it is thus a *reproduction* of *something* |
| **Data** | “The biometric *data* held by the Scheme has the potential to make the work of the police in detecting crime a lot easier.” (IPS 2006a) | See the debates about the ontological differences between data and information (Boland et al. 1987; Buckland 1991) |
| **Traits** | “A measurable, physical characteristic or personal behavioural *trait* used to recognise the identity or verify the claimed identity.” (IPS 2006b) | Biometrics are not just any trait, but those that are *measurable*; this begs the question of what we mean by measurement |

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| **Features** | “Documentation issued to non-British citizens will also include all the biometric *features* of the ID card and holders will be entered onto the National Identity Register, enabling them to prove their identity to the same standard as a British citizen.” (IPS 2006b) | As with attributes and characteristics, features are usually considered distinct properties of something; thus, the distinctiveness of biometrics re-emerges as a frame |
| A **step change** | “The real *step change* in the National Identity Scheme is that biometrics, such as fingerprints, will be recorded and linked to a single, confirmed biographical record (covering name, address, etc.)” (IPS 2006c) | This point connotes the perception that biometrics in this case are an innovation – a major change in identity assurance |
| Part of a **vision** | “Our *vision* is a universal identit y management scheme with identity information securely linked to individuals through biometrics.” (Ryan 2006) | I explore the role of biometrics in the government’s vision for identity management in this chapter |
| **Measures** | “Clients will demonstrate their right to that credential through the use of, in the case of digital certificates, a private key and using a password or biometric *measure*.” (Cabinet Office 2006a) | This again raises the question of what is being measured, and how |
| **Records** | “The increasing number of biometric *records* will also make it easier to detect illegal working.” (Home Office 2006) | Full of interpretations (administrative, bureaucratic, technical) |
| **Link** | “Biometric technology now means that we can *link* people to a unique identity.” (Home Office 2006) | It seems to be assumed that such links are strong ones; could there be weak links? |

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| Group of **technologies** | “The term refers to a *group of technologies* used for fully automated recognition of a person based on physiological (e.g. face, iris, fingerprints) or behavioural (e.g. signature dynamics, voice) characteristics.” (NAO 2007) | Not just a single technology, but a family of them; note how biometrics are said to be fully automated, involving not just the physiology, but also behaviors |
| **Electronic records** | “The identity card will lock together your basic identifying details with a combination of your unique personal features – *electronic records* of your face and fingerprints – because these are very hard to forge, steal, forget or lose.” (IPS 2008a) | Biometrics are understood here as electronic records (rather than digital ones), which form an odd relationship with an identity card and one’s “identifying details”. Where is the person in this relationship? |
| A **safeguard** | “The major new *safeguard* included when you enrol for either a passport or an identity card will be an image of your fingerprints.” (IPS 2008a) | If biometrics such as fingerprints are a safeguard, against what are they a precautionary measure? |
| A **fix** | “By recording a person’s fingerprints, we can now *fix* a person to a single identity making it simpler to check whether someone is who they say they are.” (UK Borders Agency 2008b) | This terms engenders multiple meanings, including the stabilization of identity, but also its mending |

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| A **service** | For biometric information, we will initially use existing biometric systems used for asylum seekers and biometric visas to meet our short-term needs, moving to new biometric services when the NIR is fully operational." (IPS 2008c) | This understanding of biometrics as a function or service to be provided by government (or a contracted third party) reflects a business logic; in treating biometrics as a service, do citizens therefore become customers? |
| A **tie** | "Biometrics will *tie* an individual securely to a single unique identity." (IPS 2008c) | Figurative language used to describe the processes of linking, fastening, and securing identity |
| A **bind**(ing) | "It will be reliable because it will use physical evidence – photograph and fingerprints – to *bind* personal information to its owner." (IPS 2008d) | Connotes the securing of identity through "physical evidence"; also note the reference to ownership |
| **Evidence** | "It will be reliable because it will use physical *evidence* – photograph and fingerprints – to bind personal information to its owner." (IPS 2008d) | Here biometrics are given an evidentiary status, using physical information as a "bind" |
| **Identifiers** | "Each person's identity will be secured by the registering of a number of biometric *identifiers*, such as fingerprints and facial images. The recording of iris biometrics is also an option." (IPS 2008e) | An identifier is something that identifies and, thus, this definition is somewhat tautological |
| **Details** | "For customers who apply in person, rather than online, this service will help them through the application process, recording both their biographic and *biometric details*." (IPS 2008f) | Conceiving biometrics as "details" takes them as something that can be treated granularly, such as a name or phone number |

| What are biometrics? | Illustrative quotation | Comments |
|---|---|---|
| Lock | "The person is then *locked* into the identity using biometrics – photograph and in future fingerprints." (Hillier 2008a) | This conceptualizes biometrics as both strong and durable |
| Something | "…*something* you are (e.g. a picture or other biometric such as fingerprints)." (Crosby 2008) | This bypasses the representational aspect to explain biometrics as *what we are* |

Table 6.1: Descriptive frames for biometrics in analyzed government communications (presented chronologically and with emphases added)

One might argue that this review of frames is nothing more than petty semantic hair splitting – that a certain degree of flexibility or looseness in terminology is to be expected and should not matter in the grand scheme of a project such as the NIS. Indeed, the organizing vision concept accepts that language about new technology will be incoherent and ambiguous, which is viewed as potentially a positive thing as it provides the vision “a capacity to grow, undergo refinement, and benefit from experiments-in-practice” (Swanson & Ramiller 1997, p.463). This may be so, but such looseness can also be detrimental in the long-term, especially in the technology policy arena in which the language used to describe and communicate ideas about technology has special import. I elaborate on these points later on. For now, what is important is to recognize that biometrics cannot be viewed as a single, unproblematic, unified thing – they are technologically multiple and ontologically ambiguous.

Biometrics can be understood in many different ways, depending on who is speaking and the context in which s/he is communicating. Even these basic descriptive frames are rife with variation. More than simply varying, these understandings are also occasionally potentially contradictory; e.g., are biometrics something that we are, information (or data) about parts of our body, or the use of that information (or data)? It is these controversies about the nature and state of biometrics which provide an opening to interrogate the contest of discourses and construction of meaning around the biometric artifact in this case study (cf. Venturini 2009).

## Problematic epistemologies

The very initial proposal for biometrics in the first consultation document included explicit mention of three different biometric methods (i.e., fingerprint, iris, and face). The second passage made reference to fingerprints, iris patterns, and DNA profiles, as well as one's physical appearance.

In the many documents that I analyzed, the use of the term 'biometrics' is very often accompanied by particular examples of biometrics (primarily fingerprints, with the 'other' biometrics including digital photography and iris, and very infrequently more 'traditional' biometrics such as signatures). What is it about the concept of biometrics that, when it is communicated as part of the proposals for a national identity scheme, it must consistently be exemplified in this manner?

In contrast, in the same policy documents other technological concepts such as 'identity cards', 'passports', and 'databases' do not require the same sort of explanation and exemplification. One might argue that this is due to the fact that identity cards, passports, and databases are 'old' technologies, and that biometrics are somehow newer and thus require more careful explanation.

Perhaps, but this distinction between new and old technology is dubious. The practice of biometrics has been around for centuries as part of traditional forensic techniques. On the other hand, national identity cards have an irregular history in the UK and are in some respects ‘newer’ in this context. Electronic databases are likewise a relatively recent invention. We therefore need to dig deeper to understand these discourses.

I want to suggest that the concept of biometrics is vague, awkward, and even alien. It can be perplexing and its dictionary definition is largely unhelpful. It is not always entirely clear what is meant when people use the term, including government officials in the case at hand. Perhaps suspicious of this, during the consultation period for ‘entitlement cards’ and again during a subsequent consultation on ‘identity cards’, the government commissioned a series of studies on public perceptions in order to explore these very issues.

One of the important findings from the first of these studies was that the “term ‘biometrics’ was rarely known” by interview respondents (Cragg Ross Dawson 2004c, p.59). In the Home Office’s summary of findings from the consultation on identity cards they noted that: “Awareness of the term ‘biometric information’ was low - at least 70% amongst each sample had not heard of the term before” (2004a, p.86).

As plans for identity cards progressed, these findings were echoed in Tracking Research surveys conducted by the Central Office of Information (COI) on behalf of the Identity and Passport Service (IPS), in which it was repeatedly found that less than half of the respondents were aware of the term 'biometrics' (Central Office of Information 2007a; Central Office of Information 2007b). I also observed this lack of awareness in my focus group interviews, in which my first mention of the term usually brought blank stares, so I can confirm these findings.

This then raises a number of questions about the use of the term. If study after study concluded that the term 'biometrics' was confusing and alienating, why then did policy-makers continue using it in policy documents, speeches, and so forth? Why not revert to speaking specifically about the particular biometrics under consideration, such as fingerprints or irises? What can explain the term's currency?

I recall attending a public speech on ID cards at the Social Market Foundation in 2010 given by the (then) Under-Secretary of State at the Home Office, Meg Hiller, who momentarily went off-script to openly confess that she "hated" the term 'biometrics'. Even so, she continued using the term that day as she promoted identity cards for the disempowered. Biometrics were obviously an important component of her vision for an inclusive national identity system, even if the term itself was unsatisfactory. Why was such a frustrating term so convenient for the government sponsors of the NIS?

In seeking answers we can look to the literature on technology and policy. Whitley and Hosein (2010, chap.7) have described a similar phenomenon as “intentional ambiguity” about technology, whereby members of the UK government appeared to intentionally obfuscate the issue of the voluntariness of the Scheme (that is, whether people would have a choice to enroll their data in the identity card program). Their point was that members of the government were intentionally equivocal in their public statements about the legal compulsion to apply for an ID card due to the political sensitivity around the issue.

It is not clear if the routine use of the term ‘biometrics’ in this case qualifies as an instance of intentional ambiguity or if it represents another discursive dynamic. While it appears to have been a strategic discursive move – that is, part of a larger rhetorical plan to sell the merits of identity cards – in some ways it seems to have been a form of *unintentional* ambiguity. That is, uncertainty and ambiguity about a relatively unfamiliar concept – something which most people, including the politicians in this case, would probably know very little about and with which they would have had little or no prior experience using. In other words, if it was repeatedly discovered in the Home

Office's research that people remained unaware of biometrics, then perhaps it is not too far of a stretch to think that policy-makers and political leaders were also inclined to misunderstanding, miscommunication, and ambiguity in their discourses. To take a particularly egregious example, in a House of Commons research paper from 2004 'ethnicity' is said to be a "biometric detail" (2004, pp.37-38) (which, by nearly every expert account, it is not).

On the other hand, one could argue that the term 'biometrics' served as a strategic discursive catch-all, which was used by officials in a way that made it difficult to question or take issue with certain aspects of proposals for the NIS without getting into the technicalities of biometrics. By speaking of 'biometrics' in general, they did not have to engage with the important differences among the various biometric modes (including error rates and the required infrastructures), while being able to convey a sense of progress and innovation in their proposals.[17]

If the term 'biometrics' is difficult to comprehend, then perhaps talking specifically about the various biometric technologies that are of interest in a given project would help to alleviate some of this confusion. This is essentially the 'exemplification strategy' discussed above. However, this too brings with it certain problems, as these different technologies are also relatively novel and

[17] Indeed, in some of the documents I analyzed, 'biometrics' is a term that is used excessively – at times, it appears, as often as possible, even when the term adds very little to the meaning of a remark.

unfamiliar to many, particularly as part of a proposal for a national identity system (as opposed to the practice of fingerprinting in police work, for example).

From the analysis of six years of policy discourses emerged a list of different terms that were used to describe the three ‘main’ biometrics proposed within the Scheme (see Table 6.2).

| Fingerprints | Iris (or eye) biometrics | Face biometrics |
|---|---|---|
| Fingerprints (276) | Iris patterns (32) | Facial image (48) |
| Digital fingerprints (39) | Iris biometric(s) (29) | Digital photograph (39) |
| Fingerprint biometrics (35) | Iris image (16) | Photo biometric (29) |
| Fingerprint scan (8) | Iris recognition (9) | Facial recognition (26) |
| Fingerprint images (8) | Iris photograph (8) | Facial biometrics (21) |
| Biometric fingerprints (6) | Iris scanning (8) | Face biometrics (16) |
| Fingerprint data (5) | Irises (6) | Photograph biometrics (11) |
| Fingerprint checks (3) | Eye biometrics ("any other part of the eye") (5) | Facial photograph (7) |
| Fingerprint identifiers (2) | Iris scans (4) | Facial recognition technology (4) |
| Fingerprint pattern (2) | Eye, the use of (4) | Face recognition (3) |
| Fingerprint recognition (1) | Iris features (3) | Digital facial image (3) |
| Fingerprint technology (1) | Retina (3) | Photograph of his head and shoulders (3) |
| Fingerprint templates (1) | Eye scans (2) | Facial data (2) |
| Fingers (1) | Iris digital photograph (1) | Facial digital photograph (2) |
|  | Iris imaging (1) | Facial measurements (2) |
|  | Iris picture (1) | Facial recognition image biometric (2) |
|  | Iris recognition data (1) | Facial structure (2) |
|  | Iris scan data (1) | Digitalized photograph (2) |
|  | A third biometric (iris) (1) | Digitized facial image (2) |
|  | Retinal patterns (1) | Digitized photograph (2) |
|  |  | Photograph (2) |
|  |  | Physical appearance (1) |
|  |  | Picture (1) |
|  |  | Face (1) |
|  |  | Facial characteristics (1) |

Table 6.2: Terms used to describe fingerprint, iris, and face biometrics in government policy communications (the # in parenthesis beside each term denotes the frequency with which it appeared in the analyzed data)

While some of these distinctions might be understandable from a technical point of view (e.g., when distinguishing between a fingerprint template and a fingerprint image (see Chapter 2)), one could argue that the rest are simply different ways of describing the same general idea about a given biometric.

However, these different understandings have import. What is of immediate interest is not the 'correct' interpretation of biometrics, but rather the different ways in which a new and uncertain technology is described and conceptualized in this policy context. For example, the uncertainty around the specifics of using the eye as a biometric identifier is common, so it is not surprising to see generic references to "eye scans" and the occasional reference to using retinas in government policy statements. In fact, this distinction between iris and retina biometrics became a major point of contention in public debates between politicians and experts involved in evaluating the Scheme, with strong accusations of technical incompetence charged at academics who attempted to engage the government concerning its proposals. In its interim report on the government's proposals for identity cards, the LSE Identity Project mistakenly used the term 'retina' instead of 'iris'. Cambridge computer scientist John Daugman, then a government expert advising the Home Office on the biometrics component of the Scheme, picked up on these mistakes, calling them "persistent errors of fact" and using the incident as evidence that the research team at LSE was determined to kill the Scheme no matter what (LSE Identity Project 2006).

Another notable observation from the categories listed in Table 6.2 is the very different ways in which face biometrics are described. What explains this categorical uncertainty? Is a face biometric simply a picture? A picture of what? A picture of the face, or of the head and the shoulders? How important is the process of digitization to a picture becoming ‘biometric’? And when does the ‘recognition’ element of face biometrics come into play? That is, in what circumstances does a face ‘biometric’ lend itself to facial ‘recognition’?

This takes us back to the second passage from the original consultation document on entitlement cards, about the circumstances in which a face biometric should indeed be considered biometric. From a technical perspective, a photo of a person’s face is said to be ‘biometric’ when it satisfies internationally agreed standards that dictate the arrangements of the environment where the image is captured, how features of the face such as the ears and eyes are presented, image resolution, and the data format requirements which permit it to be read by computers.

Unsurprisingly, such technical specificity is lost in the vast majority of the policy documents that I analyzed pertaining to the case, in which there is a enduring degree of uncertainty over the issue of if and when an image of the face is biometric or not. For example, in the *Identity Cards Act 2006* – the legislation which enacted the Scheme – photographs of the face are listed separately from fingerprints and 'other' biometrics.

> The things that an individual may be required to do under subsection (4) are—
>
> (a) to attend at an agreed place and time or (in the absence of agreement) at a specified place and time;
> *(b) to allow his fingerprints, and other biometric information about himself, to be taken and recorded;*
> *(c) to allow himself to be photographed;*
> (d) otherwise to provide such information as may be required by the
> Secretary of State (2006, p.5, emphasis added)

These are distinct discourses on biometrics and their relationship to photography that distinguish the former from the latter.

Later in the Act, biometrics are defined as follows:

> "Biometric information", in relation to an individual, means data about his external characteristics, including, *in particular, the features of an iris or of any other part of the eye* (2006, p.38, emphasis added)

Here biometrics are understood in terms of both information *and* data, and are about one's "external characteristics". Specifying biometrics as "external" characteristics is significant for at least two reasons. First, by definition it precludes internal characteristics from being considered biometric, so for example hand vein pattern recognition systems (a set of emerging technologies that are said to have great potential) would not qualify according to this legal prescription. Second, it is debatable whether irises, or even fingerprint biometrics are, in fact, external to the body. Irises reside *within* our eyes. Likewise, there are new fingerprinting techniques (including multispectral imaging), which read the information below the epidermis (as it is more stable than the information on the fingerprint ridges). In both cases, the external/internal distinction complicates such matters.

In the same document, a photograph is specified as

> a photograph of his head and shoulders (showing the features of the face); (2006, p.42)

This seems a clear enough legal description of a photo. However, in the various drafts of the *Identity Cards Bill* that circulated through the Parliament before the legislation was finally enacted, a photograph was described slightly differently. For example, in the first version of the Bill that was amended in Committee, a photograph is said to be

> a photograph of his head and shoulders; (2005, p.40)

That is, not specifying that it need to highlight certain facial features. Whereas in related legislation known as the *UK Borders Act 2007* – which, among other things, made way for the issuance of biometric identity documents to certain segments of foreign nationals – explicit mention of face biometrics is missing altogether.

> (b) "biometric information" means information about external physical characteristics,
>
> (c) "external physical characteristics" includes, in particular—
>
> (i) fingerprints, and
>
> (ii) features of the iris or any other part of the eye (2007, p.10)

Here we read that biometrics are again about "external" characteristics, and more specifically "physical" ones, but only fingerprints and "features" of the iris (or the eye) are explicitly listed. These shifting definitions of biometrics, which appear not just in any text, but in formal legislation that established the legal bases for two major government identity programs (national identity cards and biometric identity documents for foreign nationals, respectively), reflect the unsettled and uncertain organizational knowledge around biometrics in both the Home Office and Parliament.

## Signatures: the forgotten biometric

Complicating this situation even further is the fact that signature biometrics – arguably the oldest form of recorded biometric – are absent in the first draft of the *Identity Cards Bill*, and only appear in later versions of the Bill. When they do appear, they do so not as a 'biometric' per se. Rather, they stand alone (like facial photographs). They are missing altogether in the *UK Borders Act 2007*.

This repeated omission is interesting because, as with photography (of the face), signature biometrics are arguably a less 'sexy' biometric and often overlooked in popular discussions. Compared to fingerprints, which are easily the most spoken about biometrics in the policy discourses on the NIS that I analyzed (see Appendix 6), signatures very rarely get mentioned. This is notable considering the special historical and legal status of signature biometrics – they convey intentionality in ways that other biometrics do not –, as well as the ease with which they can be forged and misused. In many ways, signatures are the 'forgotten' biometric in the story of the Scheme.

However, this is not absolute. As I write this section of my thesis, the new coalition government is in the process of nullifying the *Identity Cards Act 2006* and as part of that process a new piece of legislation (known as the *Identity Documents Bill*) is passing through the various committee stages. During the first sitting for the new Bill, former Under-Secretary of State Meg Hiller was keen to stress "biometrics include signatures" in response to a remark from a witness regarding the appropriateness of using biometrics in certain social contexts (Hillier 2010, col.3). Hillier's point was to show that biometrics are mundane and resorted to the signature example to illustrate this point.

Yet the question remains regarding whether and in what circumstances face images or signatures, or any use of the body for that matter, are 'biometric'. It is becoming clear that there is no conclusive answer in the data. It seems to depend, in part, on who is speaking and what they aim to achieve in their rhetoric.

To explore this point further, let us review the wording of a survey conducted on behalf of the Home Office in the early days of the proposals for a national identity system, which again describes the different biometric modes in very particular terms and arguably in a way that helps to familiarize respondents to biometrics while demystifying them to an extent.

> To what extent are you in favour of or against providing the following biometric details?
>
> - Fingerprint (collected by pressing your fingers against a glass reader – *no ink is involved*)
> - Digital photograph of your face (*like going into a photo booth*)
> - Digital photograph of your iris (*like going into a photo booth*) (Home Office 2004a, p.84, emphasis added)

Participants were told that providing face and iris biometrics to the Home Office is more or less the same as having a simple photograph taken. Note how the process of fingerprinting is depicted in terms that emphasize cleanliness, as opposed to, say, privacy or data security concerns.

A similar conceptual tension arises in a 2005 briefing document on identity cards.

> We will record biometric information when the person applies. Biometric information - such as fingerprints and iris patterns - is unique to each individual. Recording this information takes just a few minutes and is *just like having your photograph taken.* Recording biometric information will mean that the scheme will be able to detect people who try to establish

> more than one identity and who use multiple identities to hide criminal activities. (Home Office 2005c, p.6, emphasis added)

As before, biometrics are described in terms of examples (i.e., fingerprint and iris biometrics this time around). The benefit frame of ‘uniqueness’ is present and the problem frame of ‘multiple identities’ likewise emerges. But more important to the current discussion is how biometrics are described as “just like” having one’s photo taken, resembling the previous description. These discourses convey that biometrics are “just like” older forms of photography. Note as well how facial photos are missing in this excerpt on biometrics.

Elsewhere Baroness Scotland, former Attorney General under the Labour government, remarks that

> I'm afraid that I do not accept the argument that this legislation will change radically the relationship between the state and the individual. The relationship between the state and the individual did not change in 1837 when it was made compulsory for every birth in England and Wales to be registered and recorded nationally, nor when similar provisions were introduced in Scotland in 1855 and in Ireland in 1864. *The information to be held on the National Identity Register will not include highly sensitive personal information* such as financial, medical or tax records*. It will include biometric information to identify an individual (much as a photograph is used currently in a passport)* as well as basic identity information such as an individual's name, address date of birth etc.--most of this information will already be known to government, for example in the existing records held by the UK Passport Service which already covers around 80% of the British population. (House of Lords Select Committee on the Constitution 2005, p.18, emphasis added)

Two points stand out here. The first, pertinent to this ongoing tension between photography and biometrics, is that biometrics are understood in this passage in terms of photography. Indeed, Baroness Scotland seems to be arguing that biometrics are, in fact, nothing special – they are something that have been included in passports for many years. Second, this rhetorical move of describing biometrics in terms of (facial) photographs allows her to argue that biometrics are *not* sensitive information, thereby nullifying a oft-repeated counter-frame used to contest the introduction of biometric systems. I return to this point about data sensitivity in a moment.[18]

In official discourses on biometrics, therefore, face biometrics served as an important gateway for familiarizing debates and discussions. However, this rhetoric was neither neutral nor apolitical. Spokespeople could argue that, as a relatively established technology with which most people are familiar, facial photos would not introduce major cost concerns or present any real threat to privacy or data security, respectively. Accepting that biometrics (in the form of digital face photos) were already a reality in passports and other identification documents, it could then be argued that it is desirable to pursue more of them so as to enhance the security of identification systems. As David Blunkett

[18] Similar rhetoric has emerged in debates about the New York Police Department's use of iris scanning technology. Civil society groups have argued that these measures are excessive, whereas proponents argue that they are nothing new. As Police Commissioner Raymond Kelly remarked, "We are authorized to take pictures. This is just a picture of your iris. ... We're matching that iris to see if you're the same individual. Our lawyers say we don't need any mandate to do it." (as quoted in Snow 2010)

remarked in 2004, “If we want, and we've already agreed as a nation that we do want, secure passports, the only way to get them is to use biometrics. So the question is do we use 1, 2 or 3? We think that we should endeavour to use 3 biometric identifiers as a safeguard for all of us.” Speaking to and on behalf of the nation, Blunkett was calling for multiple biometrics as the logical next step in pursuing digital photo-based electronic passports. However, this logic would be questioned.

The discussion to this point has focused on revealing the conceptual uncertainty around biometrics in government discourses. This uncertainty did not result in the government dropping its plans. Official spokespeople were able to leverage the concept in the government’s pursuit of the proposals. In the following sections I move away from this conceptual deconstruction to explore how the black-box of ‘biometrics’ was discursively deployed along the other six dimensions offered by Orlikowski and Gash, focusing first on the reasons for pursuing biometric technologies in the ID card scheme.

## 6.3 Initiating biometrics

The analysis now moves to explore issues relating to the motivations for and initiation of the use of biometrics in the Scheme (i.e., dimension 2 in Orlikowski and Gash’s guiding framework). This dimension concerns the knowledge, expectations, and experiences that individuals and organizations have about a technology’s initiation. As such, it dovetails nicely with the legitimizing function of an organizing vision. In this section I want to explore three main areas: government discourses on the ‘international obligations’ for biometrics, the government’s desire for the United Kingdom to become an international leader in biometrics, and the government’s discursive reasoning regarding what policy problems biometrics were supposed to help to address.

## Obligations for biometrics?

Government talk about duties and obligations for biometrics was common throughout the course of the Scheme. At one point during the roll-out, the government argued that it would be a “dereliction of duty” in the “modern age” for it not to “protect the public” using biometrics (Ryan 2006, p.6). In framing the issues in this way, biometrics were made out to be a part of good governance – something all governments should be doing for their citizens. This rhetoric of obligation often transcended the domain of national governance, however, to include international obligations.

By far, the most persistent justification regarding the decision to collect biometrics as part of the NIS revolved around supposed international obligations to incorporate them into passports. These ‘requirements’ were said to be imposed on the UK government by different external bodies, including the International Civil Aviation Organization (ICAO), the United States, and the European Union. In its most basic form the argument was that, because the

UK was obliged to collect biometrics for passports anyway, it might as well use them in its new national identity card program. There are several problems with this argument, including what exactly these obligations required in terms of the type and number of biometrics and whether the UK was, indeed, obliged to follow them.

Concerning the ICAO requirements for ‘biometric passports’, the government stated in 2004 that:

> Since the terrorist attacks of 2001 the International Civil Aviation Organisation (ICAO) has been pressing for travel documents to be standardised worldwide and to incorporate a "biometric". A biometric is a unique identifying physical characteristic such as facial recognition, iris pattern or fingerprints. The ICAO has nominated facial recognition as the primary biometric for travel documents, with iris pattern and fingerprint as secondary but not mandatory. In line with these recommendations, the UK Passport Service is planning to implement a facial recognition image biometric in the British passport book from late 2005/early 2006. The biometric can be derived from a passport photograph and will be in accordance with ICAO standards. (House of Commons 2004, pp.24-25)

Note that the only requirement that the ICAO imposes on governments is for a digital face biometric, to be included on a chip in the passport document. Other biometrics, such as fingerprints or irises, were (and as of 2011 still are) strictly optional. This facial biometric requirement involves the digital capture of facial photographs, which must be taken in accordance with certain standards. Importantly, this digitization process can be applied to images that are taken and submitted by applicants, thus building on well-established application processes. The collection of fingerprints or irises is not possible in the same way, as these require special equipment and expertise.

Related to this ICAO requirement for face biometrics in electronic passports is the visa waiver program in the United States, which UK passport holders are eligible to participate in. The visa waiver program requires citizens of certain countries to hold a 'biometric passport' (with only a facial image, following to the ICAO standard) in order to remain eligible for visa-free travel to the US.

A second biometrics-related travel program in the US is the US-VISIT system, which mandates the collection of face and fingerprint biometrics from all foreign travelers as they enter the United States through certain ports of entry. This includes British citizens. Thus, British travelers to the US are required to hold ICAO-compliant facial biometric passports, and will also have their fingerprints collected as they enter the country, although these are distinct programs.

Yet these two programs were often described as international developments which *necessitated* the collection of multiple biometrics from UK citizens by the UK government, but it is not the case that the US government expected or required the UK to take fingerprints from its own passport holders. Moreover, these two programs were occasionally confused in government discourses about the need for biometrics. For example:

> The US has already imposed a fingerprint requirement on all visitors to the US who have historically not required a visa ('the visa waiver scheme'). This includes British citizens. (Home Office 2005a, p.4)

To be clear, the visa waiver program does not (as yet) include a fingerprint requirement. The biometric requirement is simply for digital face biometrics to be stored in the passport document – in other words, the ICAO requirement. Fingerprints are collected under a separate program, by US border officials as travelers enter the country.

The third and final 'international obligation' repeatedly referred to by government officers was that EU requirements somehow mandated the UK government to collect biometrics from its citizens. In fact, this requirement only applies to members of the Schengen travel area, which the UK opted out of. Then-Junior Minister Andy Burnham made such an obfuscated argument in 2006 in a letter to Labour MPs in advance of a vote on the *Identity Cards Bill*.

> Irrespective of the Identity Cards Bill, people will have to register fingerprint biometric information when applying for a passport from 2008/09 to keep us in line with standards being adopted in the rest of the EU. (Burnham 2006, p.2)

Or as was later stated in an IPS policy document:

> *Why do I have to record my fingerprints?*

> The identity card will lock together your basic identifying details with a combination of your unique personal features – electronic records of your face and fingerprints – because these are very hard to forge, steal, forget or lose.
>
> *The UK is also committed to following new EU standards which are designed to make EU passports the most secure in the world and require all passports to include fingerprints on their electronic chip from 2012. So even if you don't want or need an identity card, you will still need to record your fingerprints as part of your passport application.* (IPS 2008a, p.14, emphasis added)

The UK's "commitment" to collect fingerprints from its citizens according to EU standards was, in reality, strictly voluntary. It was not a legal requirement imposed by European authorities, but rather an opportunity for the UK government to pursue a policy that it had mooted for years. In fact, the government even brought a legal challenge to the European Court of Justice to be allowed to participate in the regulation of biometric passports, from which it had been excluded because it is not signee of the Schengen Agreement. Ultimately, it lost its case and conceded to pursue fingerprint biometrics in passports voluntarily, fearing that otherwise the British passport would be seen as "second class" (Hillier 2008b).

Throughout these discourses on 'international obligations', the term 'biometrics' was regularly used by authorities to obscure the actual requirements for the inclusion of digitized facial images in passports with both optional extras such as the collection of fingerprints or other biometrics (ICAO secondary options) or standards that were inapplicable to the UK (Schengen).

These discourses permitted government actors to speak of obligations for ‘biometrics’ while obscuring the legal and technical specifics of these requirements.

## International leadership

This brings us onto a second factor which motivated the government’s pursuit of biometrics. If, indeed, there was no real legal requirement for the collection of biometrics on the scale proposed in the NIS (that is, collecting multiple biometrics such as face, fingerprint, and potentially iris from not just passport holders but all citizens), then perhaps we can look elsewhere for explanations. We catch a glimpse of such motives in a series of statements about the Scheme and the opportunity it provided the UK to lead the world in the development of biometrics. As Joan Ryan remarked to attendees at a biometrics conference in London:

> And the last thought I want to leave you with is that the UK is ahead of many others in setting out its plans for a secure biometric identity card. With your help we can be at the forefront of these technologies and have the opportunity to be a centre of excellence for identity management and biometrics. (Ryan 2006, p.8)

Or as the Home Office wrote the same year:

> The UK will continue to take a leading role in developing the use of biometrics and information technology to secure our borders, working with other governments to increase security around the world. (Home Office 2006, p.10)

And as Jacqui Smith argued in 2008:

> *Britain leads the world in successfully delivering biometric visas*, with all those coming to the UK on a visa now required to provide a fingerprint. So far, more than one million biometric visas have been issued, to travellers from 135 countries around the globe. (Smith 2008b, p.7, emphasis added)

These discourses on international leadership in the domain of biometrics reveal the UK's desire to be a global champion of the technology. Far from being forced to pursue biometrics by external forces such as the US and Europe, it seems these were policies and technologies that the UK government wanted to engage and lead on.

One could argue that the original discourses on international obligations provided an opening for the Home Office to initiate its pursuit of biometrics in various security and immigration-related programs. Following this, then, it was able to begin championing the continued development and use of biometrics on the basis of not being outdone by other international players, for biometrics were (and still are) seen as a major business opportunity for those with the expertise and know-how to undertake and implement them.

## Biometrics: a panacea for our ills

We can also explore the government's motivations by analyzing the numerous policy discourses on biometrics. Across the many government policy documents that were analyzed, biometrics were said to be capable of solving or contributing to solutions in wide-ranging policy arenas, including identity, crime (of various types), public service delivery, commerce, immigration, and terrorism, among others. The common theme across these policy areas was a perceived limitation in existing means of identifying and authenticating people. The vast majority of these discourses were positive regarding what biometrics are capable of, although some dissenting discourses did emerge in the official policy communications.

The policy area of ‘identity’, broadly defined and understood, was by far the most frequently discussed ‘problem’ for which biometrics were said to be an ideal solution. In these discourses, the relationship between biometrics, identity, identification, and various identity-related artifacts is complex and multifaceted.

### *Biometrics and identity*

The various government documents related to the NIS articulated the relationship between biometrics and identity in several different ways. At different points in the history of the Scheme, biometrics were said to be about “securing”, “linking”, or “fixing” a person to a “single”, “core”, or “unique” identity. They were also described as a “guard” or “protector” of identity. Furthermore, it was claimed that biometrics were a “stronger” or the “best proof” of identity, as compared to other means such as passwords and PINs.

A quotation which nicely illustrates this rhetoric about biometrics and identity states that

> The Scheme will *secure identity* to the highest standards *by*, for example, *the use of fingerprint biometrics*. (IPS 2008c, p.16, emphasis added)

*Biometrics and identification processes*

Beyond the vague concept of 'identity', the *processes* of identification were also said to benefit from the government's plans for biometrics. For example, biometrics would improve the "integrity" of *enrollment* processes. They would also to make identity *checks* "faster", "easier", "stronger", and "more confident". Likewise, biometrics would "simplify" and "strengthen" *authentication* and *verification* procedures.

Towards the end of the Scheme's life, biometrics were also repeatedly said to provide citizens with a means to *prove* their identity with a "high degree of assurance".

> As part of a number of methods offered to verify a person's identity, *the introduction of biometrics will also enable individuals,* when appropriate, *to easily prove their identity to a high degree of assurance by providing a biometric for verification against the biometric recorded when the ID card was issued.* (IPS 2008b, p.13, emphasis added)

This rhetoric of identity assurance was part of a larger set of discourses surrounding so-called citizen-centric identification, popularized with the publication of the Crosby report (2008), which was about empowering citizens through digital identity systems. However, the sort of thinking reflected in the quotation above assumes that a very specific identity infrastructure is in place – one which would permit more or less real-time biometric checking against a record (stored either on a card or in a database elsewhere). These discourses thus served as a medium for framing expectations about how the proposals would work in the future – expectations that assumed a lot of the biometrics in the Scheme.

### *Biometrics in the identity ecosystem*

It was not just 'identity' or the generic processes of identification which biometrics were supposed to secure. They were also implicated in certain other relationships and configurations in the larger identity 'ecosystem'. Biometrics were variously said to be able to "secure" or "protect" not just our identity *information*, but also identity *records* as well as identity *tokens*. Within the identity ecosystem these are distinct artifacts, with, for example, identity information being stored as records on databases or on storage devices within the tokens themselves. Three quotations illustrate the range of these discourses:

> Our vision is a universal identity management scheme *with identity information securely linked to individuals through biometrics*. (Ryan 2006, p.7, emphasis added)

> *Registering the biometrics of people* who want to visit the UK lets us vet visa applicants for previous immigration or criminal history in the UK, and *create a secure record* on our databases. (Home Office 2006, p.8, emphasis added)

> Inserting a microchip containing *facial image data* into the passport book will improve *the security and integrity of the passport* by linking the passport holder to the passport book more tightly *via the biometric*. (UKPS 2006, pp.12-13, emphasis added)

In some of these discourses, it is not entirely obvious what it is that biometrics are supposed to secure. For example,

> The use of biometric information to link a person to a passport will enhance security. (UKPS, as cited in House of Commons 2005, p.30)

Sometimes it is the identity information, record, or token itself (e.g., the ID card or passport) which is made secure through their inclusion.

> Over the coming year we will complete the introduction of ePassports, where a facial biometric is stored on a chip in the passport; *this will enhance* both *the integrity of the document* and strengthen our authentication processes. (IPS 2006b, p.5, emphasis added)

But at other times it is the link or connection *between* these objects (such as the individual and his or her passport or record in the NIR), which is said to benefit from the introduction of the technology.

> The first generation of biometric passports will be issued from 2006. *The use of facial biometrics will make a more secure link between the passport and its holder*. (Home Office 2005c, p.6, emphasis added)

There were thus various configurations in the proposed identity ecosystem that were said to benefit from biometrics. Importantly, these different envisioned configurations assumed particular technological and organizational arrangements within the identity system. That is, different visions insinuate different information systems. We discuss these different visions for the eventual use of biometrics, and the architectures they assume, in later sections.

### *Biometrics and identity 'exploitation'*

> Managed correctly and to high standards of privacy, security and choice, it is clear to me that the use of *biometric cards and passports can be an important part of the scheme that allows us as citizens to easily assert and prove our identity, and that prevents our identity from being exploited or stolen by others.* (Smith 2008b, emphasis added)

Much of the government's discourse on biometrics resembles the passage above, which addresses the various risks to identity which biometrics would help to prevent. These risks include the fraudulent use of someone else's identity, identity "theft", and the enrollment and use of "duplicate" or "multiple" identities. More often than not, these risks to identity were accepted as real and unproblematic – not as social or media constructs (cf. Poster 2006, chap.5). In these discourses it was assumed that the category of 'identity crime' was obvious and self-evident.

The inclusion of biometrics in one's record on the NIR was said to be an obvious way to protect them from "identity fraud". Note again how the following discourse frames a certain pattern of practices around the NIS, which would require regular biometric checks to reduce the risks of identity fraud.

> Preventing identity fraud and other criminal activity
>
> *Because your name will be linked by your fingerprints to a unique entry on the National Identity Register (NIR), you will have much greater protection from identity fraud: to impersonate you, a fraudster will have to have and be able to mimic your biometrics*. At the moment, they may be able to forge an identity just by finding out your name and address and personal details. Benefit fraud based on false or multiple identities will be much easier to stop. (IPS 2008c, p.11, emphasis added)

Such discourses were especially prevalent in parliamentary debates and media coverage following the HMRC data breach, so we will return to this discussion in the second part of the analysis (chapter 7).

In addition, the belief that biometrics can prevent duplicate or multiple identities was also common in these discourses. The basic argument was that once you have enrolled your biometrics alongside an identity, it is impossible to re-enroll to obtain another identity because biometrics are unique. In practice, this would require one-to-many biometric matching.

> Each person's identity will be secured by the registering of a number of biometric identifiers, such as fingerprints and facial or iris images. *The biometric information will make it much easier to detect attempts to record duplicate identities.* It will also enable individuals, when necessary, to easily prove their identity to a high degree of assurance by providing a biometric for verification against the biometric recorded when the ID card was issued. (IPS 2006a, p.12)

From a sociological perspective, it is interesting how duplicate identities are treated as a something worthy of suspicion, particularly in an age in which technology allows us to reinvent ourselves and assume new identities such as in on-line environments. Notably, other countries that use biometrics in their national identity schemes are not as concerned with biometric 'de-duplication'. Moreover, there are important off-line scenarios in which people are expected to be able to hold multiple 'official' identities, such as for people in police protection (e.g., spouses who require protection from their abusive partners) or members of the security services who assume different identities as part of their work. These exceptions did not make their way into the government's discourses on the harms of duplicate identities.

Similarly, a lot was said about biometrics and their capacity to make it much more difficult for people to register so-described false identities.

> The National Identity Register will hold a small amount of personal biographic details separately from biometric fingerprints and photographs, *making it incredibly difficult for anyone to steal or exploit another's identity*. (Smith 2008b, emphasis added)
>
> By recording biometric data it will be much harder for people to register with the ID Cards Scheme under a false identity, and the scheme will make it far easier to detect people attempting to register more than once (as their biometrics would be detected), *so people who assume a false identity will be stuck with it*. This will help to curtail the illegal activity of terrorists and organised criminals. (IPS 2006a, p.6, emphasis added)

However as the second passage concedes, biometrics are incapable of preventing someone from registering under another's identity. It is just that, assuming the biometrics used are unique and individuating, he or she will be "stuck" with this other identity (at least until the identity's 'true' owner attempts to register the same details with different biometrics). Note also how it is argued that the prevention of 'false' identities will somehow prevent acts of terrorism or organized crime, without a clear explanation of the link between identity and these activities. This association was made frequently in the government's discourses.

A few dissenting voices did emerge in the policy communications, mostly in the consultation documents, which argued that biometrics may in fact increase the risks to identity, such as through malicious intent or human error. For example:

> People were concerned that when appointments were made there might be a possibility of information being misappropriated, and at the point when biometric information was provided, that it might be possible for this to be illicitly taken and used or forged. (Cragg Ross Dawson 2004a, p.56)

Or:

> Errors during data capture can lead to complications – e.g., biometrics of a person attached to another person's identity. (The Faith Community Consultation Consortium 2005, p.12)

### *Biometrics and public policy*

Moving from these discussions about identity to more specific applications, we find that biometrics were said to have a role to play in several different government policy areas.

### *Public service delivery*

In selling the idea of biometrics to the public, the government argued that biometrics would help to create efficiencies in public service delivery while also restricting access only to those eligible for services. As concerns the latter objective:

> Would Jean Hutchinson [a benefits fraudster] have been able to commit her crimes if she had been asked to give a photo and fingerprint as proof of her identity when she registered each new benefit claim?
>
> The answer is no. A simple check against the National Identity Register would have revealed the real person's face and fingerprints. (Smith 2008c)

Likewise, biometrics were said to be a part of the government’s strategy for “transformational government” (Cabinet Office 2006b, p.20).

### *Immigration*

In terms of immigration, biometrics were framed as being able to prevent illegal immigrants from defrauding the system while providing a means for legal immigrants to prove their entitlement.

> Foreign nationals come to the United Kingdom for a wide range of reasons such as to study or work. Using advances in biometric technology we can reinforce our business processes and cut illegal working, protect legal migrants, and identify those trying to evade our rules and laws. This will help strengthen border security and lay the foundation for the wider National Identity Scheme. By recording a person's fingerprints, we can now fix a person to a single identity making it simpler to check whether someone is who they say they are. The card will make provide [sic] reassurance and identity protection to the many here legally. (UK Borders Agency 2008b, p.4)

In this context, recall the earlier discussion about whether the use of biometrics would alter the relationship between the government and citizen. In contrast to arguments that this relationship would not change, discourses such as the one above seem to presume guilt or wrongdoing on the part of foreign nationals, who must prove, with biometrics, that they are who they say they are and entitled to be in the UK.

### *Personal finance*

Biometrics were also tied discursively to concerns about securing financial transactions and combating fraud.

> Financial security: The ID card will provide a more secure way for you to apply for financial products and perform financial transactions, whilst making it more difficult for someone else to try fraudulently to access your finances. It is more secure as your ID card is linked to your biometrics (e.g. fingerprint) which are unique to you and no one else can use it. (Home Office 2005f, p.23)

Again, these discourses assume that banks, for example, would have the capacity to scan fingerprints and perform biometric checks.

*International travel and trade*

As with the use of biometrics for public service delivery, in the context of international travel and trade they were ascribed a dual role – as a means of securing activities from 'bad' elements and as a way of facilitating 'legitimate' travel and commerce.

> Biometric documentation will be used to increase security and to facilitate the passage of legitimate passengers and trade. (UK Borders Agency 2008a, p.6)

*Borders*

Similarly, biometrics were seen as a way of 'off-shoring' borders such that individuals could be screened throughout their journey before arriving to the UK.

> Border control can no longer just be a fixed line on a map. *Using new technology, particularly biometrics,* and new approaches to managing risk and intelligence*, we must create a new offshore line of defence, checking individuals as far from the UK as possible and through each stage of their journey*. Our aim is to make legitimate travel easier, yet prevent those who might cause us harm from travelling here. (UK Borders Agency 2008a, p.6, emphasis added)

*Terrorism*

On certain occasions, the government tried to argue that biometrics would help to prevent acts of terrorism, claiming that false or multiple identities were a staple of rogue actors intent on doing wrong.

> Terrorists and criminals use false and multiple identities to avoid detection and enable them to 'launder' money. The Identity Cards Scheme will make it easier to detect people attempting to register more than once (as their biometrics would be detected) helping in the fight against terrorism and organised crime. (Home Office 2005c, p.21)

However, these discourses on terrorism were challenged by various actors, including civil society groups such as Privacy International and Liberty, who disputed the capacity of biometrics to prevent people from organizing and executing acts of terror. For example, as the Home Affairs Committee noted in 2004:

> There is little reason to believe that terrorism would be so undermined. Privacy International has supplied us with a list of a number of countries that have suffered most from terrorist attacks since 1986. Eighty percent of these have long-standing identity card systems, of which a third contain a biometric such as a fingerprint. (House of Commons Home Affairs Committee 2004, p.85)

In response, the government claimed that the important difference between the experiences of these countries and its own proposals was the role of the central database of biometrics within the NIS.

> When [the Home Affairs Committee] put this argument to the Minister of State for Citizenship and Immigration, he replied that other countries did not have the biometric database that was being proposed as part of this scheme, and that this, rather than the card, was the defence against the use of multiple identities. (House of Commons Home Affairs Committee 2004, p.29)

Here we see that it is not simply biometrics but rather a specific proposal for an information technology architecture and set of organizational practices and routines around biometrics which would supposedly impede terrorists' attempts to enroll multiple identities. However, this discourse still begs the question of how biometrics (and their supposed defense against multiple identities) would prevent terrorism, which is, to say the least, a very difficult political problem involving more than just the possession of multiple identities.

### *Crime detection*

The government mooted using biometrics, and in particular the fingerprints which were originally to be collected for the Scheme, to help to solve crime. Their plan was to cross-reference fingerprints stored in the identity card database against those collected from crime scenes.

> The ability for the police to compare their 900,000 outstanding crime scene marks with fingerprints held on the National Identity Register will provide a significant opportunity to increase detections. This is estimated to have a benefit of £40m pa by reducing the social and economic costs of crime. (Home Office 2005d, p.8)

In making such arguments, the government overlooked a wide range of important concerns about privacy (i.e., secondary usage of information and proportionality) and civil liberties. It also fuelled concerns that the NIS would result in ordinary citizens being treated as potential criminals.

### *Police administration*

Last, beyond potentially using fingerprints from the Scheme to investigate unsolved crimes, there were also proposals for the police to use biometrics routinely to identify members of the public. In a rather odd twist of logic, this was seen as being more “convenient” for the public.

> Allowing for more efficient use of police resources. *There is considerable scope for reducing the administrative burden on the police in dealing with the routine identification of individuals* with their consent e.g. motorists. The voluntary production of an ID card - *or a biometric ‘card not present' check* - *would save police administrative costs and be more convenient for the general public.* (Home Office 2005a, p.16, emphasis added)

## 6.4 Implementation

Having discussed the ‘why’ of biometrics in the NIS, we now move to issues surrounding implementation; that is, the ‘how’. This analysis follows from the third dimension of Orlikowski and Gash’s framework, encompassing issues to do with the knowledge, expectations, and experiences that individuals and organizations have about the design, development, and installation of a technology. In particular, this section focuses on two sets of concerns that emerged during the debates about identity cards in the UK: the costs related to ‘doing’ biometrics and how the Home Office and IPS would establish, run, and manage a nationwide network of equipment for recording and reading biometrics. Importantly, these concerns are rife with future expectations about an implementation that never happened.

## Costs

The monetary costs of their implementation in the NIS were by far the most regularly discussed issue related to biometrics. As already mentioned, this was partly due to a critical report released by the LSE Identity Project (2005), which questioned certain of the government's cost projections for the Scheme, including those costs related to nationwide biometric enrollment. There is, therefore, plenty of discourse in the data on which to build an analysis.

The costs of the Scheme were always said to depend on *whether* and *which* biometrics would be chosen, and importantly, *how* they would be collected and used in the future. For example, in its very initial consultation document, the Home Office conceded that:

> Photograph recognition could be less costly to implement than fingerprints or iris patterns as it would not require a regional network of devices to record applicants' information. (Home Office 2002, p.108)

Of course, this sort of discourse implied that photographs would be submitted by applicants to the Home Office, for example by post, and then digitized, rather than being taken in-person by a trained official. As an aside, it should be noted that this means of collecting face biometrics introduces various data integrity and security concerns (see, for example, Linder 2007).

By framing the pursuit of biometrics as an international obligation, as discussed, the government could also argue that (most of) the costs would be incurred anyway. For example:

> The US has already imposed a fingerprint requirement on all visitors to the US who have historically not required a visa ('the visa waiver scheme'). This includes British citizens. The EU will be mandating biometric passports for its citizens in the next few months. *The costs of recording biometric information and issuing more secure identity documents (in the form of biometric passports) is* [sic] *therefore unavoidable*. (Home Office 2004d, p.4, emphasis added)

Or as stated elsewhere:

> Given that we will be introducing biometric identifiers for the 80% of our citizens who are passport holders and also for foreign nationals, we believe we can - for slightly more investment - yield much wider benefits for individuals and society [in the form of a biometric national identity card]. (Home Office 2005c, p.4)

There were also concerns about which organizations or individuals would incur these costs associated with using biometrics. While some assumed the Home Office would be paying for the entire Scheme, including the start-up and maintenance costs across all public sector organizations using the system, it eventually emerged that it intended only to cover the capital costs to its organization. This meant that other organizations would need to cover their own costs of using the system (Burnham 2005b; Whitley & Hosein 2010, p.173). As was explained to the Home Affairs Committee:

> The Home Secretary told us that this figure does not include the costs of biometric readers and other equipment to be installed in other Departments, such as the Department for Work and Pensions, or the National Health Service. The overall costs of these would, in any case,

> be difficult to establish as there is little if any certainty about the numbers and types of readers required. (House of Commons Home Affairs Committee 2004, p.53)

Private sector organizations would presumably also pay to use the system, including equipment costs but also for every biometric check against the Register.

Growing concern and mounting pressure about escalating costs in the Scheme led the IPS to suspend the idea of pursuing iris biometrics, as mentioned, and later to initiate a process to outsource the collection of fingerprint biometrics from citizens. These were two major events for biometrics in the Scheme's history. Therefore, financial concerns (as opposed to, say, security or reliability motivations) were arguably the most important driver of policy decisions about the implementation of biometrics in the Scheme.

> We will look at new ways of recording fingerprints and photographs to make it easy and convenient for individuals. For example, we are looking to a future where the market would provide biometric enrolment services, giving citizens a choice of competing services which should maximise convenience and *drive down price.* (IPS 2008c, p.8, emphasis added)

This policy decision also meant that citizens would be responsible for paying to have their biometrics collected, thus shifting the cost obligation from government (funded by the taxpayer, of course) to the citizenry, who would pay directly out of pocket to have their biometrics recorded. By doing so, the government was able to claim cost savings in its regular reporting to Parliament.

Furthermore, the central database on which all the biometrics in the NIS were to be stored went through different re-configurations as a result of concerns about costs. Originally the Home Office intended to build a brand new database, which would segregate citizens' biometric and biographical data for security reasons. Eventually they opted instead to re-use existing biometric systems for asylum seekers and biometric visas, with the aim of moving to a new system once the Scheme was operational. These design changes were driven by short-term cost concerns (IPS 2006c, p.10) in an apparent attempt at showing that the Scheme could be made to work in an affordable way, particularly before the general election of 2010, after which the Scheme's future would be in even greater doubt.

Throughout these discourses on costs, much was uncertain about the 'true' costs of doing biometrics. Cost projections were loaded with assumptions about technological advancements, economies of scale, and the possibility of cheaper equipment being available in the future. For example, when it came to costing readers, the government noted that:

> We expect that the various reader technologies will have moved on by the time that the scheme rolls out. In particular one might expect better integration of these devices, for example a less fragmented face recognition market and better performance from low-cost sensors. This

> makes it dangerous to predict reader costs, although the scheme does take a view on all of these types of sensors. (IPS 2005, p.5)

This discussion on costs leads us into an analysis of the discourses on the government's changing strategy for implementing biometrics in the Scheme.

## Implementing infrastructures

Recall from the literature review that, in practice, doing biometrics involves two major steps: the initial enrollment of biometrics from a person and the subsequent comparison of his or her biometrics against the previously enrolled data, during either an identification or verification mode.

From the beginning of proposals for the NIS, the government paid considerable attention to how it might enroll the nation's biometrics. For example, noting the significant "learning curve" associated with implementing biometrics (Home Office 2002, p.64), it sought opinions on this issue during the very first consultation exercise.

> The Government would like to hear the views of potential partners on how a nation-wide network of easily accessible biometric recording devices could be established and operated, how people who are not mobile or who live in sparsely populated areas could be served and what other value added services potential partners might offer. (Home Office 2002, p.110)

Such discourses explained the importance of providing biometric enrollment facilities in locations across the UK, and where that proved impractical the use of mobile recording devices.

> As well as local centres there will also be mobile centres for sparsely populated areas. (Home Office 2005c, p.4)

However, much less attention was paid to how these enrolled biometrics would then be used in practice, particularly in ways that benefited the citizen whose data were being used. That is, the government's priority seemed to be figuring ways of collecting and storing everyone's biometrics in the first instance, and not how they would be subsequently used. Indeed, as a focus group interviewee from one of the early government's consultation exercises complained:

> "For [biometrics] to be beneficial all these places would have to have finger scanning and eye scanning facilities. Otherwise it's pointless." - Christian white male and female 31-50 London (Cragg Ross Dawson 2004a, p.55)

One could argue that the government was especially focused on enrolment because it is a necessary first step in doing biometrics and that other concerns would be addressed later on. Indeed, the government admitted in the beginning that, in the initial stages of Scheme, the use of biometrics would likely be limited, with the focus being on checking that people were not enrolling more than once.

> The use of any of the above types of biometric information (or a combination of these) would probably be limited in the early stages of an

> entitlement card scheme to ensuring that a person could not establish multiple, false identities. (Home Office 2002, p.105)

A further argument is that it was up to the organizations that would eventually use the NIS to decide when and how they would make use of biometrics. That is, that it was the government's job only to provide the basic infrastructure for an identity scheme and that the eventual use of biometrics by public and private sector organizations should be demand-led and not dictated by the government.

However, the government's marketing activities for biometrics in the Scheme never extended beyond enrollment issues, with various attempts at forging relationships with organizations capable of enrolling large volumes of biometrics, without a clear explanation of how these would be used afterward. This further fuelled speculation amongst critics that the Scheme was one massive government data collection exercise, with little eventual benefit to the citizen.

Another aspect of implementing biometrics has to do with the human resources required for such an undertaking, including both specialist training for facilitating and overseeing the enrollment process but also identifying and acquiring the expertise necessary for dealing with system errors and other anomalies as they emerge during biometric checking (cf. Davis & Hufnagel 2007).

A major concern in the government discourses was whether the public sector had suitable human resources to conduct large-scale biometric enrollment. At first, the need for trained specialists was downplayed by the Home Office.

> The Government envisages a much simpler scanning system than that used by the police or the Immigration Service, which would probably involve just the scanning of four fingers. The prints would not be scanned to a legal standard of proof of identity. *The staff taking the fingerprints therefore would not need to be as highly trained as those working for police forces of the Immigration Service and there would be no need for trained fingerprint officers to interpret the results of any potential matches detected by the computer.* (Home Office 2002, pp.115-116, emphasis added)

Government discourse shifted in later documents, with revised claims that while expertise was needed, there were sufficient human resources already in the civil service on which to found an expert base. For example in the *Strategic Action Plan* the government stated:

> We will put in place the skills and expertise to support large-scale use of biometric matching. Biometric technology identifies small percentages of what are known as 'false matches' or 'false non-matches'. These need expert human assessment to ensure that matches are being made correctly. For this, *we will build on resources which currently exist within government.* (IPS 2006c, p.15, emphasis added)

Soon thereafter the discourses about biometrics training and expertise began to change again, with an emphasis being placed on the need for support services. As was admitted in the *Strategic Supplier Framework Prospectus*:

> With the use of probabilistic biometric matching technologies, there may also be associated biometric support services within this package (i.e. those services requiring expert human intervention). (IPS 2007b, p.34)

The question, of course, was where this expertise would come from. While the government claimed that the UK Borders Agency (UKBA) (which was then actually two separate departments: the Border and Immigration Agency and the UKVisas) was developing the relevant human resources through its programs for collecting asylum seekers' biometrics and issuing biometric visas to foreigners, the size of these programs was dwarfed by the potential scale of a national identity program. Concurrently, the government began articulating the need for "biometric enrollment services" for the NIS, to be developed and provided by the market.

> The capacity to handle these enrolments – in terms of high street estates, personnel and technology – does not exist today. The Biometric Enrolment Service would need to deploy a nationwide capacity capable of handling five million+ enrolments a year, in a way that is convenient for customers, efficient and of high integrity. (IPS 2007b, p.39)

Yet again, the focus was on the human resources needed for the initial enrollment of biometrics for second generation (fingerprint) biometric passports as well as identity cards, rather than how these biometrics might be later used in various identification contexts and the potential human resources required for facilitating such activities. As noted earlier, a greater consideration of how to use biometrics and the attendant human resource implications might have emerged once the system had matured, with a significant number of people's biometrics having been enrolled, but this never came to fruition.

## 6.5 Biometrics in use, or expectations thereof?

We now move to focus on the fourth dimension of Orlikowski and Gash's framework, related to issues around use. They see this dimension encompassing knowledge and organizational experience of the use of a specific technology and perceptions of the technology's attributes, among other aspects (1992, p.6).  In an important sense, the discourses surrounding the use of biometrics in the Scheme were highly speculative and far removed from practical contexts. If we consider the events that make up the life and demise of the Scheme, the reasons for this become clear.

Depending on how you define the scope of the program, biometrics were rarely ever actually used in the NIS. There was the Atos Origin trial of face, fingerprint, and iris biometrics, but this was only a small trial, as well as the 'roadshow' for biometrics in the early stages of the Scheme. There are also those foreign nationals who were issued biometric immigration documents (which included face and fingerprint biometrics) starting in late 2008, but this program technically fell outside the scope of the NIS, despite certain government discourses which tried to blur the distinction between the two programs. In addition, there were the first generation 'biometric' passports (with digital facial images), but these were not a central part of the NIS (and, indeed, passport documents were not “designated” identity documents under the *Identity Cards Act 2006*). Therefore, most of the activity related to the use of biometrics in the short-lived program was actually discursive; that is, talk about their *potential future* use. Setting aside discourses about enrollment for the time being (as we already explored these in the previous section on implementing biometrics), we now explore what was said about the *use* of biometrics. Most of these discourses were framed in terms of when, where, why, and how to do biometric ‘checks’ at some undefined point in the Scheme’s future.

The original consultation document for an entitlement card system in the UK offered two scenarios for biometrics check: off-line and on-line checking (see Figures 6.3 and 6.4).

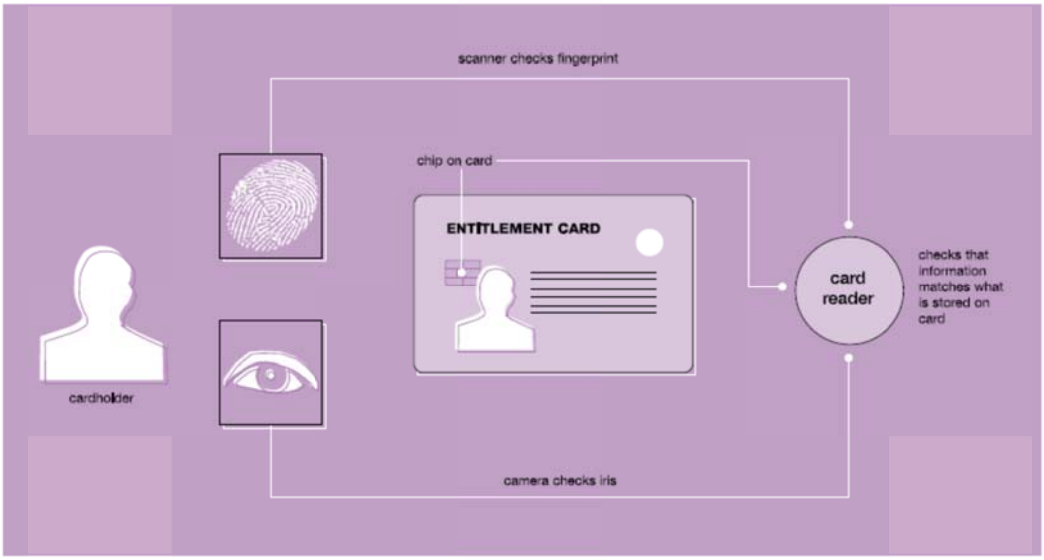

scanner checks fingerprint
chip on card
ENTITLEMENT CARD
card reader
checks that information matches what is stored on card
cardholder
camera checks iris

Figure 6.3: Off-line biometric check (Home Office 2002, p.59)

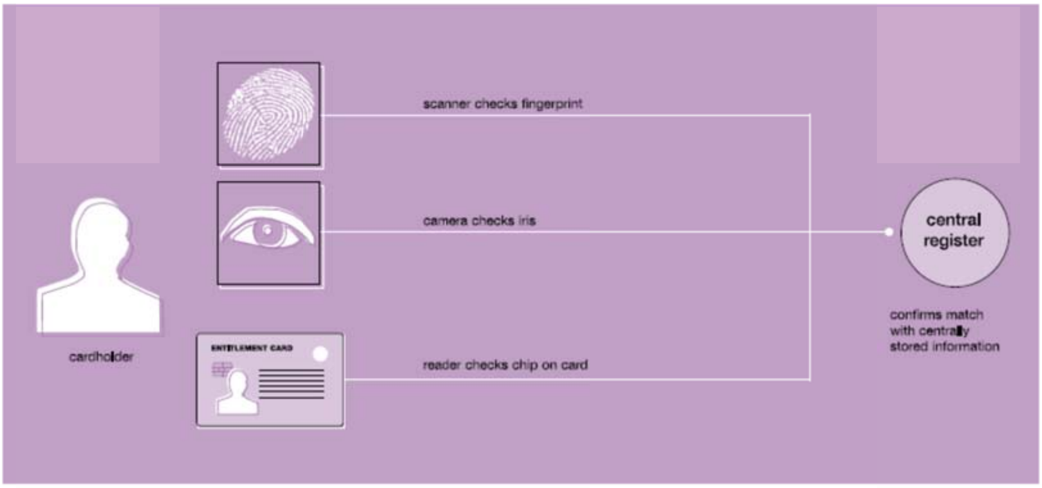

scanner checks fingerprint
camera checks iris
central register
confirms match with centrally stored information
cardholder
ENTITLEMENT CARD
reader checks chip on card

Figure 6.4: On-line biometric check (Home Office 2002, p.59)

Figure 6.3 depicts a scenario for checking biometrics in an off-line mode by comparing them against records stored on an identity card, listing both fingerprint and iris biometrics as possibilities. Figure 6.4 offers another scenario in which biometrics are compared in an on-line fashion, against records on a centralized register. Of course, both of these diagrams greatly simplify the technical and business processes at work during these checks, and are removed from any real-world context, but the important point is that the major distinction being made in the diagrams is between off-line and on-line checks. Interestingly, both of these scenarios for checking biometrics involve the use of information technology. Elsewhere, the role of technology in using biometrics is depicted otherwise.

In a subsequent consultation document (on identity cards, in 2004), the government provided some further detail on how biometrics could be used by certain organizations.

> Banks or building societies might check a person's biometric (using a card reader) and verify this against the National Identity Register before opening an account. (Home Office 2004c, p.28)

And there were even visions for 'card not present' biometric checks, especially for police use.

> The intention is that people will be able to have their biometrics checked against the Register even in the absence of a card on a voluntary basis in order to be able to demonstrate their identity if, for example, they are stopped by the police. (Home Office 2004c, p.34)

In 2004, the Home Affairs Committee commented that the government needed to provide more specific information regarding how biometrics would be used in practice.

> We note that at the moment there is very little clarity about the level and nature of checks that will be required and carried out*, even though this is fundamental to the whole scheme.* We recommend that the Government should provide estimates of the proportion of checks that would be

> biometric and therefore highest security. (House of Commons Home Affairs Committee 2004, p.72, emphasis added)

Subsequently, Home Office research found that respondents approved of biometric checks during “high risk, high value transactions” (Home Office 2005a, p.7) or situations involving an “application” (Home Office 2005e, p.8). Opening a bank account is an obvious example of a situation in which people complete an application to access services, where many would probably deem providing biometrics unproblematic. However, there are other services requiring applications for which providing biometrics might be considered unreasonable or disproportionate, such as joining a gym or frequent traveler program, or applying for a supermarket loyalty card. Hence, it is not immediately apparent what transactions or interactions would require biometric checks. This lack of clarity persisted throughout the course of the Scheme.

On other occasions, the government argued that public sector organizations could use biometrics to regulate claims to social benefits, but as already discussed this sort of cross-departmental co-operation was never achieved in the NIS.

> Benefit fraud will be easier to detect and prevent. Tighter identity requirements and better checking services will make it harder for people to abuse the system. Biometric ID can be checked against centrally held records, which will make it harder to use a false identity or make repeated claims successfully. Sharing data about identity between

> government services will make it easier to check eligibility and detect multiple applications and duplicated records. (Home Office 2006, p.9)

Such visions of real-time, on-line, on-the-spot biometric checks against a central store recurred often in the government's discourses; however the actual practice of identity checks turned out to be much more mundane. This was a necessity as the vast infrastructures required for biometric checks never came to be during the brief existence of the Scheme. During the roll-out of foreign national biometric identity documents in 2008, the government provided guidance to the organizations that would encounter the newly issued cards. Rather than elaborating the merits of electronic fingerprint checks against information held on the card or against the Register, the Home Office offered up another form of 'biometric' verification.

> As it is made entirely from polycarbonate, [the card] will have a distinctive sound when flicked, and the holder's image will always be in grey-scale. (UK Borders Agency 2008c, p.3)

These are a very low-tech means of assuring an identity. The second part of the comment describes a process of visually verifying an image on the card, as border officials currently do during traditional passport checks. The contrast between such a 'low-tech' process and the "satisfyingly hi-tech" biometric checks (as they were once described in Home Office public engagement documents (Cragg Ross Dawson 2004c, p.14)) is stark. Yet again, this exposes a tension in the potential meanings of 'biometrics'. Whereas in the original diagrams biometric checks were understood to require the use of technology in reading the body and settling identity claims, organizational realities dictated a different process.

## Characterizing the attributes of biometrics

As Orlikowski and Gash (1992) focus, in particular, on perceptions of technical attributes within this dimension of their framework, we now turn to review the frames that emerged from the government discourses on biometrics regarding their supposed traits and qualities. This review exposes other discursive trends. Beyond the ontological question of what biometrics are (e.g., a process, a technology, data, etc.), it is interesting to explore how the perceived characteristics of biometrics were portrayed and framed by government actors and the meanings that these frames provided the biometric concept.

The following frames emerged through the coding process (see Table 6.5). At various stages during the development of proposals for the NIS, biometrics were described as follows:

| Frame | Context |
|---|---|
| Personalized | "…proceeding towards more secure passports and driving licences based on biometric technology - with *personalised, specific* identifiers" (Home Office 2004c) |
| Specific | |
| Sensitive | "Secondly, it was argued that there would be a new requirement to register information, including *sensitive personal* biometric data, with the state. This is a significant new obligation on the individual citizen which will be *intrusive* in operation." (House of Commons Home Affairs Committee 2004) |
| Personal | |
| Intrusive | |
| Unique | "A biometric is a *unique identifying* physical characteristic such as facial |

| | |
|---|---|
| Identifying | recognition, iris pattern or fingerprints." (House of Commons 2005) |
| Reliable | "Biometrics are being developed around the world to improve the *security* and *reliability* of identity documents including fingerprint biometrics on visas and our own facial image biometric passport to be introduced next year." (Burnham 2005a) |
| Secure | "I would argue that in the modern age, failing to offer the ability for people to link their personal data to *secure* biometric information would be a derelicti on of our duty to protect the public." (Ryan 2006) |
| Measurable | "A *measurable*, physical characteristic or personal behavioural trait used to recognise the identity or verify the claimed identity." (IPS 2006b) |
| Singular | "Biometrics will tie an individual securely to a *single unique* identity." (IPS 2006c) |
| Unique | |
| Difficult to forge, steal, forget, forget or lose | "Why do I have to record my fingerprints? The identity card will lock together your basic identifying details with a combination of your unique personal features – electronic records of your face and fingerprints – because these are *very hard to forge, steal, forget or lose.*" (IPS 2008a) |

Table 6.5: Attribute frames assigned to biometrics in analyzed government communications (ordered chronologically)

As before, the review of terminology reveals more than semantic hair-splitting. The choice of terms used to frame biometrics is significant for a number of reasons. From a legal perspective, the classification of data as 'personal' brings with it certain legal rights and protections, which can differ depending on the legal and regulatory context. Indeed, as I draft this section, the Information Commissioner's Office in the UK is seeking to clarify the meaning of 'personal data' within the Data Protection Act, stating that new technologies and forms of identification are complicating these issues and the organization's capacity to regulate (ICO 2010).

Following from this legal classification are certain technical implications. For example, the ICAO (the body responsible for setting standards for travel documentation) requires that the use of fingerprints in travel documents such as passports be protected by special advanced cryptographic means, known as Extended Access Control (EAC), because fingerprints are considered ‘personal’ data. These protections do not apply to facial biometric data because, in contrast, they have been determined not to be personal (NAO 2007, p.20).

A story from the US further illustrates how these meanings matter. In 2008, the former US Secretary of Homeland Security sparked controversy when he referred to fingerprint data as “hardly personal” and “not particularly private” in the context of discussions on the international sharing of citizens’ biometrics. This drew criticism from Canadian privacy regulators, among others, who called fingerprints “extremely personal” (Swire 2008). Such disputes about the meanings and attributes of new technologies are ongoing.

Another related dispute emerges around whether biometrics are ‘identifiable’. In general, fingerprints are considered identifiable information, whereas photos of the face are not. However, if the facial recognition process is computerized and automated, and satisfies certain performance requirements, then face biometrics can be said to be identifiable. In these scenarios, information technology plays a central role in determining the *identifiability* of biometrics. Importantly, this debate about the identifiability of certain data extends beyond biometrics such as fingerprints, to other technologies and policy arenas. For example, recently courts in the US and EU have debated whether Internet Protocol (IP) addresses should be considered identifiable information. The US has declared that they are not whereas the EU is leaning in the other direction (Anderson 2008; Whitten 2008).

Moreover, DNA – a very special type of biometric – presents further complications to this thinking, as it can be used to identify not just certain individuals, but also their genetic relatives (i.e., family members) (Bieber et al. 2006). These ongoing debates about how different types of data engender varying interpretations and degrees of identifiability beg the question of what we really mean by identity and identification.

While some of the frames from Table 6.5 appear relatively infrequently in the policy communications (e.g., biometrics as 'identifying'; 'measurable'; 'singular'), others recur regularly (biometrics as 'personal'; 'secure'; 'unique'). Some were even repeatedly recycled verbatim throughout the government's discourses (biometrics as 'personalized'; 'specific'). This recycling of discourses about biometrics and other components of the Scheme in policy documents complicates the project of studying organizational discourses on the proposals. That is, how original are these frames for biometrics and where do they originate? How can one assess the extent of organizational knowledge when much of these communications appear to be boilerplate? What do decision-makers truly understand about what they are saying in these situations?

Certain of these frames about the attributes of biometrics were contested by other actors. For example, the question of whether biometrics are ‘sensitive’ is challenged in the policy discourses that I analyzed, with the Home Affairs Committee describing them as such, and Baroness Scotland sharply disputing this claim by noting their previous, uncontroversial inclusion in passport documents (in the form of facial photos) (House of Lords Select Committee on the Constitution 2005, p.18).

Another contested frame is the reliability of biometrics. When the Scheme was first launched, the predominant sentiment in much of the expert testimony, studies of public attitudes, and Home Affairs Committee discourses was that there were outstanding concerns and misgivings about the reliability of biometrics.

> Some concern was expressed on what the public reaction would be to the concept of biometrics. Other comments were on the expense of setting up systems subject to change and rapid advancement. *Systems could also be error-prone and unreliable initially.* (Home Office 2003a, p.102, emphasis added)

Or as the Home Affairs Committee noted:

> The security and reliability of biometrics are central to the Government's proposals. No comparable system of this size exists. (House of Commons Home Affairs Committee 2004, p.4)

And as was stated in a House of Commons research paper on identity cards from 2004:

> The Association of Payment and Clearing Services, which has taken the lead in credit and debit card security, is reported to have doubts about the quality of biometric identification. Such a system was under consideration for the new generation of chip and PIN credit and debit cards but it was reportedly rejected because no system was found to be reliable enough. (House of Commons 2004, p.42)

In these discourses, reliability was conceived in very different ways, ranging from security concerns, to questions about the technological maturity of biometrics, to doubts that biometrics would prevent people from enrolling multiple identities. It was a very loaded category.

Over the course of the proposals, the government seized on these various disputes around the reliability of biometrics and began targeting its discourses to address the issue. In doing so, government actors re-framed the debate by removing one of the perceived barriers to using biometrics in the NIS. If biometrics were understood as reliable, then the identity systems based on biometrics being pursued by the Home Office could be said to robust and practicable. As such the Home Office went to great lengths to demonstrate their ongoing successes and achievements with biometrics – that is, to prove their reliability.

> [The] UK Border Agency will be launching identity cards for foreign nationals on 25th November [2008]. The robustness of the UK Border Agency process and technology has been tested through a pilot phase in Croydon. To date in the region of 12,000 migrants have already had their fingerprints recorded and checked against immigration records under the pilot biometric enrolment process. (IPS 2008e, p.3)

Or as former Home Secretary Jacqui Smith noted in a public speech a week later, regarding the same pilot tests of biometrics

> To date, more than 15,000 people have enrolled, and we have identified a number of fraudulent applications and people trying to use multiple identities. *The technology is working well - and in case you're wondering, there have been no cases where we've been unable to enrol someone's fingerprints*. (Smith 2008a, p.4, emphasis added)

Simultaneously, a report from the IPS stressed that

> [The National Identity Scheme] will be *reliable because it will use physical evidence – photograph and fingerprints* – to bind personal information to its owner. These are more difficult to lose, steal or fake than paper, password or signature. (IPS 2008d, p.15, emphasis added)

These discursive attempts at settling the reliability debate drew on apparently successful uses of biometrics. Whether these successes would continue as the technology was scaled did not appear important at the time. What mattered was exhibiting that biometrics were reliable and that the government was capable of using them in its program for national identity cards.

## Unquestionably unique?

The most repeated claim about the use of biometrics in the NIS, by far, was that they would provide a 'unique' form of identity to everyone who enrolled. This argument was predicated on the common assumption that biometrics are indeed unique to an individual. This belief is best summed up by the saying that 'no two fingerprints are alike', although it can be applied to other biometrics. For many actors within government, the entire point of biometrics was to achieve uniqueness in identity. The frame recurred throughout the government discourses that I analyzed. To present just a small fraction of these discourses:

1) Things which you 'are' i.e. your biometric identity. These are attributes which are *unique* to an individual and include fingerprints, iris patterns (the coloured part of the eye around the pupil), and DNA profile. (Home Office 2002)

2) It is recognised that the inclusion of a biometric encrypted on a smartcard chip would be a way to link identity to a particular person by way of a *'unique'* physical characteristic. (Home Office 2003a)

3) What is biometric information? A *unique* identifying physical characteristic. (Home Office 2003b)

4) A biometric is a *unique* identifying physical characteristic. (Home Office 2004c)

5) The Government intends to introduce a national compulsory ID cards scheme using *unique* biometric identifiers linked to a new national database. (Blunkett et al. 2004)

6) Most [respondents] seemed to know that fingerprints and iris patterns are *unique* and understood that they could be used to generate a unique record of identity for each card holder. (Cragg Ross Dawson 2004c)

7) It is known that around 35% of those involved in serious organized crime and terrorism routinely use false or multiple identities. The use of a secure and *unique* biometric identifier will disrupt their activities by making it impossible for them to enrol more than once on the Register. (Home Office 2004b)

8) The rigour of the application process and the *uniqueness* of the biometric will mean that, in time, the identity card will become the gold standard way of proving identity throughout the UK. (Home Office 2004b)

9) The benefits of using biometrics were largely undisputed – *almost all knew that fingerprints and iris patterns are unique*, and accepted that their use would probably make ID cards more

difficult to forge or misuse. (Home Office 2004a)

10) There can't be 2 people with the same biometric on the same database claiming to be the same person. I think it's quite important to spell that out because there is terrific misunderstanding about the issue about being able to forge or multiply identity. (Blunkett 2004)

11) As with any project of this size and complexity there is a great deal of development work to be done before it is possible to finalise all the operational details, including the precise technical arrangements for recording biometric identifiers such as facial image, finger scans and iris images, which will provide a way of *uniquely* confirming the identity of cardholders. (Home Office 2004c)

12) A biometric is a unique personal physical characteristic such as a fingerprint or iris pattern. (Central Office of Information 2004)

13) The Register will also link each individual's record to a biometric that is unique to that person. (House of Commons 2004)

14) A biometric is a unique identifying physical characteristic such as facial recognition, iris pattern or fingerprints. (House of Commons 2004)

15) The database linked to the cards will carry only basic information such as name, address and date of birth, besides the *unique* biometric information – such as the image of your face, iris, or fingerprints – which ensure your identity is protected for use by you and you alone. (The Faith Community Consultation Consortium 2005)

16) A biometric is a unique personal physical characteristic such as a fingerprint or iris pattern. To what extent do you think having biometric details on your identity card will be effective at stopping other people stealing your identity and using your card, making it easier to prove your identity (e.g. by not having to remember a PIN number) (Home Office 2005b)

17) Why now? Now is the right time to introduce an ID cards scheme because of advances in technology. An ID cards scheme is more than just issuing pieces of plastic. It is about recording on a central database basic personal information such as name, address and date of birth securely. This data is then linked to biometric information - such as facial image, fingerprints and iris patterns - which is *unique* to that individual. (Home Office 2005c)

18) Financial security: The ID card will provide a more secure way for you to apply for financial products and perform financial transactions, whilst making it more difficult for someone else to try fraudulently to access your finances. It is more secure as your ID card is linked to your biometrics (e.g. fingerprint) which are *unique* to you and no one else can use it. (Home Office 2005e)

19) Police checks: The ID card will make it easier for the Police to make our society safer. ID Cards carry our biometrics which are *unique* to each one of us - no one else can use them. This means the police will more easily trace and identify suspects. (Home Office 2005e)

20) The creation of a register of limited registrable facts where a person's record is linked to a set of *unique* biometrics will combat attempts to create multiple identities. (Home Office

| |
|---|
| 2005h) |
| 21) As the ID card will link your identity to your unique set of biometrics, it will be much more difficult for fraudsters to use this document in order to impersonate others. (IPS 2006a) |
| 22) Biometric technology now means that we can link people to a *unique* identity. (Home Office 2006) |
| 23) Identity authentication through biographics does not, however, provide proof of *uniqueness* of an identity. For this, biometric data is required. (Crosby 2008) |
| 24) The [foreign national identity] card will contain details about the holder's immigration status and entitlements in the UK which include their unique biometric data. This will enable us to tie an applicant to a fixed identity. (UK Borders Agency 2008a) |

Table 6.6: Instances of biometrics being described as 'unique' in analyzed government texts (ordered chronologically)

From Table 6.6 it is evident that the uniqueness of biometrics was virtually unquestionable in these communications, even as other aspects of the Scheme were so uncertain. For example, as is stated in the quotation from the *Identity Cards Bill Regulatory Impact Assessment* (number 11 in the table), the project for biometrics was deemed large and complex and most of the operational aspects of the system, such as how biometrics were to be recorded and used, remained unknown for most of the Scheme's lifespan. Yet, having noted the very tentative state of biometrics and the many uncertainties surrounding them, the Home Office then went on to re-iterate the apparently obvious claim that biometrics provide a way of "uniquely confirming" identity. It is as though this point was indisputable, even while everything else was unsure.

However, the debate about uniqueness and the claims that can be justified by the supposed uniqueness of biometrics such as fingerprints encompasses several complex issues. Cole (2009) summarizes the epistemological problems with many of these claims.

First, the generally accepted understanding that biometrics are unique is not uncontroversial. There is a growing consensus in the academic literature (particularly the forensics literature) that the uniqueness of biometrics remains unproven and is, perhaps, something that cannot be proven or disproven. It is, in many ways, a thing of faith that both the general public and many professionals working in the fields of forensics and law, for example, assume to be true. The subsequent claim that biometrics can be used to individuate (Cole uses the term ‘individualization’) because they are unique is equally specious he says. Going further, Cole claims that the entire discussion about uniqueness is both irrelevant (2009, pp.241-242) and banal, arguing that what really matters is having the analytical tools necessary to distinguish one fingerprint from another, for example, or knowing the sample size for comparison. “Since all objects in the universe are in some respects the ‘same’ and in other respects ‘different’ from all other objects in the universe, according to Wittgenstein, what really matters is not uniqueness but rather what rules we articulate by which we make the determinations of ‘sameness’ and ‘difference’” (2009, p.243). Recognition of these criticisms of the frames of uniqueness was entirely absent in the government’s discourses.

## 6.6 Defining and measuring success

The fifth dimension of Orlikowski and Gash's framework relates to the success of new technology, how to define it, and the assumptions that factor into determining how it should be assessed. They argue that these criteria may be based on business-related concerns, technical capabilities, or some other aspect such as usability.

The definition of success and how to measure it with respect to biometrics in the UK case is a wholly complicated issue. On one level, we could argue that the biometrics in the NIS were a failure, especially considering the high visions for the technology in the early stages of the Scheme and its eventual demise. But this would be unfair considering how the program ended; that is, with the election of a new government intent on scrapping the system wholesale. One could argue instead that biometrics were never really given a chance to succeed.

To start, as we have already established, biometrics are not a unified thing. The criteria for determining the extent of success in deploying iris or fingerprint biometrics should therefore probably differ from those criteria for measuring the implementation of digital facial photographs in e-passports, for example. While the former programs never really got off the ground, the latter venture did, with the National Audit Office reporting in 2007 that the IPS had achieved important successes, with certain provisos. However, recent media reports are casting doubt on the successes of facial biometrics in passports as well (see, for example, Hough 2010).

Questions of success and failure also depend on the level of analysis. The meaning of successful biometrics for the Home Office or IPS will differ from an individual's experience of having his or her biometrics accepted or rejected during enrollment or when trying to access a vital medical service that requires a fingerprint scan, for example. Success is, of course, a relative concept. Moreover, the metrics used to rate success are very often political artifacts that must not be taken for granted.

This section critically explores how the 'success' of biometrics was articulated in different government discourses. There are two parts to this analysis. The first part deals with the discourses used by the government to demonstrate their achievements in biometrics. These are discourses on technological successes. The second part explores success in terms of 'customer satisfaction' with biometric identity cards.

In its discourses on biometrics in the NIS, the Home Office was keen to draw attention to its successes in *other* programs: in issuing biometric visas, new passports, and biometric identity documents for asylum seekers, as well as in the Iris Recognition Immigration System (IRIS) used in select UK airports, and the use of mobile biometric readers by police, among other systems (Home Office 2006, pp.6-7). For example, in response to a question during an on-line web chat about the lack of usability trials for biometrics in the NIS, the former chief executive of the IPS stated that

> We are planning trials during the procurement process. And this is not new technology - we have already issued three million passports with facial biometrics. If you are concerned whether or not it works, and you have an ePassport, you can take it to any of our regional offices to test that it can be read. And 400 passengers a day are using IRIS at Heathrow airport. (Hall 2006)

In trying to foreshadow the future success of biometrics in the Scheme, Hall relies on drawing attention to the accomplishments of other ongoing Home Office-sponsored biometrics programs. The thinking being, if the technology works in other application areas, there should be no problems with using biometrics in a national ID scheme. Likewise, as Jacqui Smith stated in a speech on 'making identity cards a reality':

> Since April, our fingerprint enrolment pilot [for foreign national biometric identity documents] has demonstrated how important these checks can be in weeding out those who have no right to stay.
>
> To date, more than 15,000 people have enrolled, and we have identified a number of fraudulent applications and people trying to use multiple identities. The technology is working well - and in case you're wondering, here have been no cases where we've been unable to enrol someone's fingerprints. (Smith 2008a, p.4)

In both examples, we read that the technology works – that there is no reason to doubt its eventual success in the NIS. Of course, this way of thinking about success overlooks a host of political, social, and economic concerns which might hinder the success of using multiple biometrics in a national program for identity cards.

The government was also interested in demonstrating customer satisfaction with the use of biometrics. It ran 'customer proposition' studies in the early days of its proposals to gauge the public's reaction to the prospect of using biometrics. Recall also that the Atos Origin trial was said not to be a trial of technology but rather a trial of 'customer experience'. Later on, as the IPS began exploring options for outsourcing the biometrics function of the ID cards program, it stated that

> *The introduction of 2nd biometric passports and ID cards transforms IPS's application and enrolment customer service proposition,* not least in moving from a model where IPS services only a small percentage of customers in person to one where all customers will need to be serviced in person. In bringing this new model of operation into service, IPS intends to increase efficiency, reduce fraud and *maintain its very high levels of customer satisfaction.* (IPS 2007b, p.35, emphasis added)

Besides the interesting point that these discourses speak of 'customers' rather than 'citizens', thus reflecting an ideology of 'new public management' (cf. Hood 1991; Osborne & Gaebler 1992; Mosse & Whitley 2009), they also imply that the perceived success of biometrics in the NIS depended, in part, on customer satisfaction.

To show the extent to which the IPS went to demonstrate ‘successes’ in customer satisfaction with respect to biometric identity cards, we briefly turn to a remarkable episode. In a (much delayed) response to a Freedom of Information Act request submitted by the No2ID activist group, the IPS revealed that of the nine people quoted on a section of its website dedicated to sharing positive customer experiences with biometric ID cards, eight of these ‘happy’ customers “at the time either worked for the Identity and Passport Service, the Home Office or another government department or agency" (IPS 2010). Such “astroturfing”[19] of customer satisfaction (as it was described at the time in media reports (Lettice 2010)) lends further support to idea that, as an organization the IPS was so concerned with demonstrating success, particularly as it appeared that a new government administration might terminate the Scheme, that it was willing to manufacture it as necessary.

## 6.7 Anticipating impacts

The sixth dimension in Orlikowski and Gash’s framework relates to the *impacts* of a technology on individuals and tasks, as well as an organization’s strategy, structure, culture, and way of doing business. Considering the scope of the proposals for the NIS, we target this dimension of their framework to

[19] “Astroturfing” is a pejorative term to describe the use of political, advertising, or public relations campaigns that are formally planned by an organization, but disguised as spontaneous grassroots movements.

examine *discourses around the expected social impacts of deploying biometrics.*

During the literature review on biometrics we summarized a paper by Clarke (2001), calling for social impact assessments to be conducted with any new biometrics implementation. Such assessments would provide an opportunity for sponsors to a) disclose fully the technologies they are interested in and how they would be used, b) analyze the potential social impacts of these technologies, c) publish their results for public consultation, and d) accordingly involve the public in the design of new systems. These steps can be considered as best practices for trying to understand the eventual impact of launching a new technology such as biometrics. Importantly, they assume a certain level of specificity regarding the plans for biometrics, without which assessing impacts will be difficult.

Any discussion about the expected social impacts of introducing biometrics in the UK as part of the NIS therefore ought to acknowledge and understand the impact assessments that the government conducted during the course of its proposals, including a regulatory impact assessment and a race equality impact assessment, as well as a separate equality impact assessment for foreign national biometric ID documents. The preparation and publication of these documents granted the government and Home Office a chance to consider the various problems that might arise as a result of their proposals. From these documents, we can discern two main groups that the government thought might have been impacted by its proposals: both private and public sector organizations, and citizens.

In its regulatory impact assessment, the Home Office stated as a matter of fact:

> The Bill as drafted places no burdens on business, charities or voluntary bodies. There are no provisions in the Bill which will allow the Government to require business, charities or voluntary bodes to make identity checks using the identity cards scheme. The required identity checks power relates only to public services. (Home Office 2004d, p.3)

However, while the legislation did not mandate the use of identity cards and biometrics by businesses, it was generally understood that for the Scheme to have any longevity the private sector’s participation was crucial. Furthermore, the extent of public sector organizations’ participation in the Scheme was equally important yet just as uncertain throughout the course of Scheme.

Concerning biometrics in particular, the regulatory impact assessment conceded that the details of biometrics remained underspecified, thus complicating the effectiveness of any impact assessment.

> As with any project of this size and complexity there is a great deal of development work to be done before it is possible to finalise all the operational details, including the precise technical arrangements for recording biometric identifiers such as facial image, finger scans and iris images. (Home Office 2004d, p.2)

Elsewhere, we discover a range of other discourses related to the potential social impact of the widespread use of biometrics in British life. Many of these discourses emerged in the early stages of the Scheme, following public consultation by government. The concerns raised in these discourses include questions of accountability, civil and human rights, privacy, cultural and religious objections, discrimination as the result of the uneven use of biometrics (as is the case currently in the National DNA Database in the UK), embarrassment (if and when systems were to fail), empowerment, exclusion (as a result of a medical condition preventing someone from being able to provide biometrics), gender issues, health risks related to hygiene and biometric scanners, safety, and aspects of resistance to biometrics.

It is laudable that so many of these issues received attention and were subject to public debate, albeit to varying degrees. For example, ID cards and biometrics for transgendered people was an issue of special concern for the government (see, for example, IPS 2009), whereas the question of exclusion was a tricky one to settle, especially with the disappearance of iris over the course of the proposals. Other concerns might have been reconciled had the Scheme survived the general election (e.g., ensuring that female attendees were available to oversee the enrollment of Muslim women's biometrics). However, for most of these concerns, including the issues of privacy, security, and accountability, the government paid minimal attention to the complexity of the problems. For example, the issue of accountability was understood in very simplistic terms.

> Finally, there is a requirement for accountability. The National Identity Register (NIR) will set new standards for best practice in protecting document, physical, staff and building security.
>
> The IT systems holding the National Identity Register biographical and biometric information will be fully accredited by the government's security authorities. (Byrne 2007)

As in this quotation, one of the fundamental problems with these discourses was a lack of specificity regarding how biometrics would be used in practice, especially post-enrollment. We have already noted some of these issues. Statements such as “the process will be quick, easy, and safe” (Cragg Ross Dawson 2004c, p.95) provided very little detail on which to appreciate the numerous issues that might arise in practice; that is, the real life ‘impacts’. This is partly a limitation of impact assessments in general, but moreover it is an outcome of a general vagueness and degree of uncertainty in the government’s discourses about its plans.

## 6.8 Framing publics

The final dimension in Orlikowski and Gash’s analytical framework regards relations with other players in the computing social world, including actors such as managers, users, and technologists; and third parties such as vendors, consultants, customers, and government regulators. We already identified many of these actors in chapter 5, and then again throughout the course of this chapter, including the different branches of Parliament that oversaw developments in the Scheme; external actors such as the ICAO, EU, and US which emerged discursively to justify certain policy decisions regarding biometrics; activists, experts, and academics who regularly provided informed criticism of the government's decision-making; and various commercial actors with an interest in the Scheme, among many others.

Instead of repeating these efforts in this section, my aim is rather to focus on one actor (or set of actors). That actor is the public, or perhaps more accurately stated, the 'publics' of biometrics (Michael 2009). These are interesting for a number of reasons.

First, in a literal sense, without the public biometrics simply cannot happen. That is, as a concept, a technology, or a process, biometrics necessarily involve people and the recording and reading of their bodies. Within the IT domain, biometrics are fairly unique in this respect. Therefore the public-technology relationship, and the discourses that address it, are particularly important in this case. Second, the critical public understanding of science undercurrent to this thesis persuades us to examine not only the discourses that constitute new technology, but also those about the people who are said to benefit from technology. By analyzing these government discourses about the public, we can better understand how certain actors actively and strategically framed publics in ways that were favorable to the aims and objectives of the NIS. Last, critical discourse analysis is particularly interested the study of social relations, of which government-citizen relations are an important component.

The public made numerous appearances in the government's discourses, including discourses about their perceptions and understandings of biometrics and whether they approved of and accepted the technologies. We covered some of these in the first section of this chapter as we tried conceptualizing biometrics through government discourse. In what follows we explore the discourses on the different publics rendered by biometrics, including the various 'others'.

An important discursive distinction made in the data is between those who are capable of using biometrics and those who are not. These discourses divide the population of potential publics of biometrics into two categories: the 'able-bodied' and the 'biometrically-challenged'. As regards the former category, we were told throughout the course of the Scheme that they were more or less OK with the concept:

> There were few objections to the proposed biometric procedures among *the able bodied.* (Home Office 2005b, p.15, emphasis added)

The latter category, however, proved much more complicated to resolve in government discourses. For the government, the solution for such individuals was technological in nature. That is, during the Home Office's market soundings, specialized equipment was pursued for those with physiological or psychological problems that would prevent them from 'doing' biometrics properly.

> Suppliers are encouraged to provide additional or specialised equipment to assist with the recording of biometrics that may be challenging to record successfully on standard equipment (meaning that standard equipment that is suited to the general working population may not be ideally suited to persons whose biometrics are challenging to record successfully) (Home Office 2005g, p.23)

Such discourses connote a 'standard' or 'general' population, and a group of biometric 'others'. These others – those with bodily or mental 'challenges' – included the blind, the disabled and ill (e.g., those with Parkinson's disease), the vulnerable and elderly, children, the homeless population, and people with "complex lives". Rather than re-thinking its decision to pursue biometrics for these people, the government made efforts to be as inclusive as possible. In its discourses the government was careful to promote "a scheme that works for everyone", with according processes for biometrics.

> We will work with such organisations to agree, for example, how we enroll people with complex lives such as the homeless and how an address should be recorded for them – such lifestyles will not be a barrier to enrolling. Special provisions will be required, for example, for the small group of people transitioning between genders who have complex

> identity needs but will not be excluded from the Scheme – we will offer an identity card in both genders – *or for those unable to give full facial or fingerprint biometrics due to disability, for example.* (IPS 2008d, p.13, emphasis added)

On the one hand, these discourses could be seen as being about empowering publics through biometrics, and thus resonate with arguments that in certain contexts surveillance can be empowering for some segments of society (see, for example, Murakami Wood & Firmino 2010). On the other hand, these discourses appear not to have appreciated the logic of arguments by authors such as Lyon (2002), who points out that biometrics are discriminatory *by design* – that the Scheme would not "work for everyone" in the same way and that there are large swathes of the population that would be treated differently *simply because* of the use of biometrics (e.g., those without readable fingerprints or irises suitable for biometric scans). However, we ought to be careful not to assume too much about the future practices of the Scheme, as it is these that determine the degree to which biometrics would have been empowering or repressing, and as we know the Scheme never got to this stage.

Furthermore, in these discourses public acceptance and resistance was framed in a very instrumental fashion. Resistance was seen as something that could and should be squashed, through the right mix of public engagement and public relations activity, thus smoothing public acceptance. For example, regarding the possibility of resistance to biometrics, the Home Office stated:

> It was thought that the public may be wary of providing fingerprint details as this was associated with criminality. Whilst there was potential for some resistance to the provision of iris imaging, it was considered that this could be overcome rapidly. (Home Office 2003a, p.113)

When Gordon Brown stated in an interview in 2008 with the Guardian newspaper that, “in fact, I don't actually think most of the general public think that the use of biometrics is in itself wrong, either for private transactions or for passports or whatever” (Watt 2008), it was not entirely clear who he believed this “general public” to be. Presumably, they were the ‘able-bodied’ public assumed by most of the policy discourses on the NIS, but might they have included the ‘biometrically-challenged’ as well? We need to move beyond moral discussions of right and wrong to understand how these ‘others’ of biometrics might have taken issue with the introduction of a technology that presented such challenges to so many different people.

And, of course, public acceptance and resistance meant something very different to the foreign nationals and asylum seekers who were mandated to provide their biometrics to the UK government in order to enter and reside in the country. As previously mentioned, these publics technically do not belong to the case of the NIS, as the programs fall under different legislation than the *Identity Cards Act 2006*. However, as we are interested in the statements that exist within discourses about the case of the NIS, we find that these publics made repeated appearances in government talk about the Scheme. A brief exploration of these discourses reveals the other 'other' of biometrics in the case at hand.

If the 'biometrically-challenged' were the 'other' to the 'able-bodied general public' of biometrics, then the various foreigners who unwillingly took part in different government-led biometrics programs, and provided 'evidence' that biometrics are workable in a national identity card program, can be considered another 'other'.

As we have seen, the UK government mandated certain (non-EEA) foreign nationals and asylum seekers to provide biometrics (including 10 fingerprints). This collection of biometrics meant that the Home Office was able to develop a capacity for biometrics whilst it tried to sort out the numerous kinks in the NIS. Remarking on the successes of these programs, Liam Byrne said in 2007 that:

> Already we have found 4,000 hits against immigration databases. 70% were applying for visas from abroad, had already claimed asylum in Britain. Many claimed in [sic] a different identity. Nearly 1 in 10, we found was subject to removal directions. Including a Ghanaian, who applied for a visa in Accra, who biometric checks established had claimed asylum in the UK under a different identity as a Liberian national. (Byrne 2007, pp.1-2)

The programs underpinning these discourses provided the government an opportunity to build the infrastructure necessary for biometrics, making asylum seekers and foreign nationals the guinea pigs for the testing of biometrics. This is a point that was lost on many of the critics of the NIS, who did not take issue with the use of biometrics in these other areas, failing to fully appreciate the role that the development of infrastructure for biometric immigration documents played in the national ID card scheme. And now that the *Identity Cards Act 2006* has been abolished by the new Conservative-Liberal Democrat coalition government, it is only these foreigners who are required to participate in the government's biometrics programs.

## 6.9 Conclusion

This chapter presented a critical discourse analysis of various statements about biometrics from government communications found in legislative and parliamentary texts, policy reports, research publications, corporate documents, public presentations and speeches, public interviews, corporate newsletters, leaked documents, and publicly-available responses to Freedom of Information requests. The analysis revealed how government actors strategically framed the concept of biometrics in their arguments about the Scheme, the changes these frames underwent over time, the underlying uncertainty and ambiguity in much of this 'talk' about a new technology, and the politics that were played out in these discourses. The next chapter further elaborates on these ideas by exploring additional streams of public discourse.

# Chapter 7: Analysis (II)

> Experts admit that biometrics, the storing of genetic data, is not infallible. People can have fake fingerprints - if they can have penis extensions live on television weekly, then that's really not an issue. – Column from the Independent (2005)

> You've got to laugh. Apparently people with fat fingers cause problems with the ID card technology. What? We can send men to space but that's the extent of the high-tech, high-cost cards? – Letter from a Sun (tabloid) reader (following the publication of the Atos Origin biometrics trial results) (2005)

> The shadow chancellor, George Osborne, described the security breach as "catastrophic", urging Gordon Brown *to drop his search for a vision* and "just get a grip". He said: "Public confidence in the government and its ability to protect information has been destroyed." – Guardian article reporting on the parliamentary debate following the large-scale loss of data by HMRC (2007, emphasis added)

## 7.1 Introduction

In this chapter we analyze two streams of data which run in parallel to the discourses analyzed in chapter 6. The data sources are the Hansard record of parliamentary debates and the mainstream UK newspaper coverage, both centered upon discourses on biometrics in the National Identity Scheme (NIS). As explained in chapter 4, these two sets of data do more than simply provide us with more of the same; rather, they provide new perspectives on the underlying dynamics of the case. Whereas the official policy statements found in the speeches and documents reviewed in chapter 6 were surely carefully prepared and edited before their dissemination, the debates in Parliament produced a more spontaneous set of discourses with which to understand the trajectory of biometrics. Even if these parliamentary speeches are based on previously drafted notes, the venue permits questioning and dialogue around these scripts. Analyzing the media coverage allows us to track how the messages about biometrics travelled once government discourses ‘entered the wild’.

Whereas the data in chapter 6 were analyzed around the seven dimensions from Orlikowski and Gash’s framework for understanding new technology and organizational change, this chapter is structured around the six critical events first identified in chapter 5, drawing, of course, on the debates and themes identified in chapter 6. These events represent moments when either the Scheme or biometrics in particular underwent significant policy activity, whether highly publicized (such as with the HMRC data breach) or muffled (as in the case of the government’s de-emphasizing the role of iris biometrics). As with the data analyzed in chapter 6, I conducted a critical discourse analysis on the Hansard and media discourses, leveraging the micro-analysis approach where useful (Corbin & Strauss 2008, p.59).

In the sections that follow I very briefly re-summarize each of critical events, recapping why they are important, before presenting an analysis of the relevant Hansard debates and the attendant media coverage that occurred.

## 7.2 Re-introducing the Identity Cards Bill

The first event in our timeline is the re-introduction of the *Identity Cards Bill* to Parliament after the general election of 2005. The Bill that was presented in May 2005 was virtually the same document that had been previously unsuccessful. However, having won the 2005 election, the re-invigorated Labour government was determined to pass its legislation, arguing that national identity cards were an election manifesto commitment. At the same time, the government released findings from the trial of biometrics conducted by Atos Origin, thus piquing public interest in these technologies.

During the period following the re-introduction of the Bill, much of the parliamentary debate about the proposed Scheme focused on concerns related to the expected costs of issuing biometric passports and the uncertain reliability of biometrics. As regards the latter, there were several discussions about the outcomes of the Atos Origin trial, with government ministers stressing in Parliament that "the objective of the trial was to test the processes, and record customer experience and attitude during the recording and verification of facial, iris and fingerprint biometrics. *The trial was not* *aimed at testing the biometric technology"* [9 Jun 2005: Column 655W-656W[20], emphasis added].

However, at the time there was another recurring theme in the parliamentary discourses which was less prevalent in the official policy documents about the Scheme. This topic concerned the possibility of including DNA information in identity cards. On two separate occasions shortly following the Bill's re-introduction the issue of DNA was raised. The first instance is as follows:

> Mr. Gordon Prentice: To ask the Secretary of State for the Home Department what assessment he has made of the merits of using DNA identifiers in the proposed identity cards; and if he will make a statement. [3175][21]
>
> Mr. McNulty: The Identity Cards Scheme is not proposing to use DNA as one of the biometric identifiers. Clause 43 of the Identity Cards Bill defines a biometric as data about a person's external characteristics, e.g., facial image, iris pattern or fingerprints. DNA is not included in the list of information at schedule one of the Identity Cards Bill that may be held on the National Identity Register and there is no power under clause five of the Bill (applications relating to entries in the register) for the Secretary of State to require a person to provide a DNA sample. [13 Jun 2005: Column 159W]

In his response Tony McNulty, then-Minister of State for Immigration, Citizenship and Nationality, dismisses the possibility of using DNA in the Scheme, justifying his reasoning with reference to the language about biometrics in the Bill. However, as discussed in the previous chapter, the

[20] This notation designates the location of the exchange in the Hansard record.
[21] These numbers are Parliamentary Question reference numbers.

language concerning biometrics in the various drafts of the *Identity Cards Bill* was far from unambiguous. Indeed, it is very open to interpretation whether the collection and use of DNA in the Scheme would have been impossible according to the terms of the legislation. For sure, it would have been a different and difficult project compared to collecting digital photographs of people's faces, but that is not to say it could have been ruled out entirely based simply on a reading of the proposed legislation.

One week later a similar question was posed in Parliament. Using virtually the same language, McNulty restates the government's intentions not to enroll DNA in the Scheme, again citing the Bill's language on biometrics as the reason why. In addition, medical records are mooted and subsequently dismissed, although as is acknowledged in the final part of the quotation below, the legislative language about what data could be stored on the National Identity Register (NIR) was not as firm as one might expect.

> Mr. Khan: To ask the Secretary of State for the Home Department whether there are plans to include (a) DNA and (b) medical records on the National Identity Register in the second stage of the identity cards process. [4172]
>
> Mr. McNulty: The Identity Cards Scheme is not proposing to use DNA as one of the biometric identifiers. Clause 43 of the Identity Cards Bill defines biometric information as data about a person's external characteristics, e.g. facial image, iris pattern or fingerprints and therefore excludes DNA. DNA is not included in the list of information at Schedule one of the Identity Cards Bill that may be held on the National Identity Register and there is no power under Clause five of the Bill (applications

> relating to entries in the Register) for the Secretary of State to require a person to provide a DNA sample.
>
> The Identity Cards Scheme is not proposing to include medical records on the National Identity Register. Clause one and Schedule one of the Identity Cards Bill sets out what information could be held on the Register. In general the storage of medical information on the Register would not be allowed by the Bill as medical information does not fall within the definition of registerable (sic) facts as set out in Clause 1(5) of the Bill.
>
> *The Bill does allow for the storage of voluntary information with the consent of both the person who is registered and the Secretary of State.*
> [20 Jun 2005: Column 763W-764W] (emphasis added)

These discussions about DNA and identity cards would not end here. The topic would re-emerge in later debates. The recurrence of the DNA option in parliamentary talk about the government's program for identity cards represents a confounded state of affairs. For many in the technical community, DNA-based identity cards are still very much a thing of science fiction. However they were an alluring prospect for politicians and policy-makers, who were captivated by the power of DNA and genetics. We return to this point shortly.

In the media coverage during this period, specific discussions about biometrics are absent in many of the reports on the proposed Scheme. When biometrics do appear in these articles it is very often as a passing remark to 'biometric passports', for example, without much engagement with the concept of biometrics itself. However, on other occasions the coverage is especially critical and focused on the poor performance of biometrics in the Atos Origin trial (despite the government's pleas that it was not supposed to be a technology trial). Oddly, in a Guardian article from this period Tony McNulty is quoted as claiming that the poor performance of biometrics in the government's trial was a reason to collect *even more* biometric information from people. In doing so, however, he appears to be contradicting the government's stance that the biometrics testing was not a technology trial.

> The Home Office minister Tony McNulty, said the failure rates were partly the reason the decision had been taken to incorporate all three forms of biometric on the identity card/passport.
>
> "Those who know far better than I say things are going in the right direction," he said. "The combination of the three biometrics add (sic) to the integrity of the process. Some say that goes too far." (Travis 2005) [26 May: The Guardian]

In this passage, McNulty conveys his relative ignorance of technical matters ("those who know better than I"). We are not told who these experts are, or on what basis they are making this assessment. And again, we are confronted by the issue of the role of expertise in technological decision-making.

Debates about the costs of biometrics also emerged following the release of the LSE Identity Project's interim report on 29 May 2005. In particular, the media focus was on the cost of biometric readers and the cost of frequent re-enrollment. Notably, the frame of 'uniqueness' is much less prevalent in these media discourses around the first critical event, in contrast to the government discourses. However, the debates about international obligations do make their way into the media coverage, with inaccurate reporting being the norm.

> The Identity Card Bill has another great advantage. *The United States and the European Union are forcing Britain to use biometric data on visas and passports. So the Government might as well look as if it is bravely taking the lead rather than meekly following one dictated from elsewhere*. (Smith 2005, emphasis added) [31 May: The Times]

This is an odd take on the motivations behind the government's pursuit of biometrics. While obfuscating the issues by stating that the US and EU were forcing the UK to adopt biometrics (recall that the only international obligation was the ICAO requirement for facial images in passports), it also claims that the government was putting on a brave face by taking the reins and collecting their own biometrics from citizens.

## 7.3 Identity Cards Act 2006

Attaining Royal Assent on 30 March, the *Identity Cards Bill* therewith became the *Identity Cards Act 2006*. For such a momentous period, both the parliamentary activity following its passage and the media reporting of the event was rather muted. This is, perhaps, the result of fatigue, as the Bill was debated and 'ping-ponged' in Parliament for several months until its eventual passage.

The only biometrics-related exchange to take place in Parliament the week following the passage of the Act dealt, yet again, with the possibility of using DNA information in ID cards. In response to a question about collecting DNA from foreign nationals entering the country, Andy Burnham (then-Parliamentary Under Secretary of State) remarked that the extent of the government's plans for foreign nationals was to collect "external identifiers, commonly known as biometrics". (Burnham seemed unaware that DNA is, by definition, a biometric identifier.) Unsatisfied with this response, the inquisitive MP (Spink) then turned to take issue with the reliability of biometrics.

> Bob Spink: The Minister might not be aware that the Science and Technology Committee has looked at biometrics, including iris and facial recognition and fingerprints, and found no evidence from any large-scale project that using multiple biometrics in the way that the Government propose would work technologically. The Government are simply making an assumption that they would work, but there is no evidence of that. In the absence of a working biometrics system, would the Minister consider the use of DNA?
>
> Andy Burnham: No, I would not. I do not believe that people would accept that. Even for someone often accused, as I am, of not having regard for such matters, it would raise substantial civil liberties implications. On that basis, I would rule it out categorically. As to the questions that the hon. Gentleman raises about the effectiveness of biometrics, I do not accept that that is the case. I do not know whether he has travelled to the United States recently, but it has a large-scale immigration system that uses biometric information extremely successfully. His assertion that there is no evidence of external biometrics providing a higher standard of identification in travel documents is therefore wrong. [30 Mar 2006: Column 1126]

Again, we encounter discourses and counter-discourses regarding the appropriateness of using DNA in an identity card scheme. What is especially peculiar about this exchange is that it is based on doubts about whether other biometrics such as fingerprints, irises, and facial images are practicable at the scale of a national identity program. Spink does not seem to have the same doubts about DNA. However, as mentioned above, the use of DNA in a national identity card system is a qualitatively different type of undertaking than using other biometrics. Most experts in biometrics discount the idea of using DNA in such day-to-day citizen identification and authentication contexts as wishful thinking, which is motivated by Hollywood's portrayals of the technologies (a controversial phenomenon that is referred to in the social science and criminology literature as the 'CSI effect' (cf. Shelton 2008; Ley et al. 2010; Cole & Dioso-Villa 2009)). Why, then, did certain political decision-makers consider the idea tenable, when the science and technology necessary for such a project was highly tentative at best? These discussions about using DNA in the NIS would persist, with the media reporting as late as March 2007 that certain government figures (e.g., Charles Clarke) wanted DNA to be stored on identity cards (see, for example, Buchanan 2007).

The media coverage of the passage of the *Identity Cards Bill* is similarly thin. The major focus in the coverage is on the so-called compromise reached between the House of Commons and the House of Lords which allowed citizens who renewed their passports before 2010 to opt out of receiving an identity card. Only a few outlets picked up on the point that while ID cards might have been optional for those citizens renewing their passports early, their biometrics would still be stored on the NIR. This “compromise” did not affect the biometrics component of the Scheme. It appears the most intuitive and historically salient aspect of the Scheme (i.e., possessing and showing an ID card) was the most worrisome.

## 7.4 De-emphasizing iris biometrics

The next major event in the Scheme in terms of biometrics was the eventual disappearance of iris biometrics in government discourses. More accurately stated, iris biometrics began to be de-emphasized and spoken of as a future “option” towards the end of 2006, following the Identity and Passport Service’s (IPS) publication of its *Strategic Action Plan* for identity cards. This publication initiated a series of debates in Parliament about the future of the NIS; however none of these specifically addressed the question of the role of iris biometrics. In fact, during this period the two instances of parliamentary questioning involving the topic of irises in the Scheme were both about the (extremely unlikely) prospect of the government recording iris images for passports.[22]

> Lord Roberts of Llandudno asked Her Majesty's Government: How iris scans and fingerprints for the new passport interview regime will be obtained by the video links for remote areas. [HL758]

[22] Note that no country in the world is collecting iris information for storage in passports.

> Baroness Scotland of Asthal: The new passport interviews being introduced in 2007 will not require any iris scans or fingerprints to be recorded from passport applicants. The identity interview, for first-time applicants over the age of 16 only, can therefore be accomplished by video link for those in remote areas. [15 Jan 2007: Column 780W]

Or as transpired two weeks later:

> Mr. Gordon Prentice: To ask the Secretary of State for the Home Department whether iris scans are to be included in passport chips; and if he will make a statement. [111276]
>
> Joan Ryan: The e-Passport, which was introduced in 2006, contains an embedded chip which holds data on the bearer in line with ICAO (International Civil Aviation Organisation) recommendations. At present this data is limited to biographical data such as name, date of birth etc. and a digital photograph of the passport holder. In the future, in line with other European countries, we plan to include images of two of the passport holder's fingerprints but we have no plans to store images of the passport holder's irises on the passport chip. [31 Jan 2007: Column 360W-361W]

Thus, while the IPS was downplaying its plans for iris biometrics in the NIS, Members of Parliament were wondering about their (improbable) inclusion in passports. This line of questioning is significant for at least two reasons. First, during debates about the NIS a great deal was said about the public’s lack of awareness of biometrics, continuing through the Tracking Research conducted by the COI on behalf of the IPS until early 2009. These studies repeatedly ‘found’ that public awareness of biometrics was ‘low’ or that the public “had limited understanding of biometric technologies” (Home Office 2004c, p.76). These discourses mirror the assumptions of certain traditional approaches to studying the public understanding of science, in which the public's awareness or understanding of technology is treated as a measurable entity. Where deficiencies are detected, they ought to be rectified (so the thinking goes), hence the Home Office's efforts to provide 'accurate' information on biometrics in their various marketing materials. However, these statements about iris biometrics in passports reflect a lack of awareness among parliamentarians regarding the possibilities and plans for these technologies. The iris incident provides an opening to appreciate different forms of public 'misunderstanding' of biometrics, including the misapprehensions of political decision-makers. As we have seen, these concerns apply to many other aspects of biometrics in the Scheme as well. What does this mean for the processes of technological decision-making? We will reflect on these issues in the next chapter.

Second, this incident also raises questions about how organizations such as the Home Office, which are responsible for implementing and managing large-scale, technologically complex programs such as a national biometric identity system, should communicate details of their plans and major policy changes to oversight bodies such as Parliament. It appears that as iris biometrics became less explicit in Home Office's plans for the Scheme, current organizational thinking was not clearly and timely communicated to parliamentarians and to the public, and thus the implications of this shift were not fully considered or appreciated. These are issues that I discuss in the next chapter.

Accordingly, the media coverage of this incident (that is, the shelving of iris biometrics in the Scheme) was especially quiet. Following the publication of the *Strategic Action Plan*, media reports were focused on the government's plan to re-use existing databases and the implications for costs and data security. It was not until late January 2007, over a month later, when media outlets first started reporting on the implications of dropping iris biometrics from the NIS. As was very succinctly reported:

> Iris scan 'optional'
>
> Plans to use scans of both eyes in biometric data for the national identity card scheme have been shelved owing to technical uncertainties and cost. Despite previous ministerial statements that iris scans were vital in making the cards secure, a strategic plan published last month said iris scanning was only an option. (Anonymous 2007b) [22 January: The Times]

This delay could be explained by the timing of the release of the documents (which took place in December, just before the Christmas holiday). Journalists might have required extra time to review and digest contents of the *Strategic Action Plan*.

With the policy decision not to pursue iris biometrics, many of the claims about what biometrics would do needed to be re-evaluated. For example, the policy aim of ‘securing’ everyone to a ‘unique’ identity turned even more unrealistic and unattainable with the decision not to use iris biometrics in a country with a population of over 60 million people. However these implications were not fully appreciated by many of the actors in the case, despite warnings from its own experts (see, for example, Daugman in BBC News 2007).

## 7.5 Strategic Supplier Framework

The fourth event is the IPS’s publication of its *Strategic Supplier Framework* in August 2007, which initiated the procurement process for the identity cards program. Among those technologies, resources, and services being procured, many were for implementing biometrics. The future direction of the Scheme was plotted in this procurement framework, with plans to outsource a large portion of the program to the private sector. The publication of this document was an important milestone in the Scheme’s ongoing development as it marked the first step in the formalization of relationships with technology and security companies such as IBM, Thales, CSC, EDS, and Fujitsu Services.

The silence in Parliament during this period can be explained by the political calendar: it was summer recess. Later on, however, parliamentary questions about the framework began to emerge and focused on whether short-listed suppliers were forced to sign non-disclosure agreements [252607]; the value of the contracts issued under the framework [318321]; and the value of any penalty and cancellation clauses in the contracts [224720] in the event that a new government decided to cancel the Scheme (which, indeed, happened in the end).

This event resonated in many of the mainstream UK newspapers, some of which covered biometrics-related aspects of the framework. For example, noting the absence of iris biometrics in the strategy document, both the Times and the Independent reported the Home Office’s plans to suspend its pursuit of irises. This policy was finally being publicly discussed, with the Guardian quoting then-CEO of the IPS, James Hall, as stating that

> Our current plan is to capture 10 fingerprints and record those. They won't all necessarily be on the card but we will have a record of them. I say 'current plans' because we are continuing to review every opportunity to reduce cost and risk. (Hall as quoted in Woodward 2007) [10 August: The Guardian]

Such statements reaffirmed the ongoing uncertainty in the Scheme. The business-friendly Financial Times also covered the developments around the release of the Strategic Suppler Framework. Regarding the status of iris it reported that

> In an effort to keep costs down and the initial technology relatively simple, the cards will use fingerprints rather than the more complex iris technology as the initial identifier.

> But with 100,000 frequent-flyer passengers now registered with the iris-reading system at Heathrow, Mr. Hall said "if in due course we want to move to a second biometric, iris would be the obvious place to go".
>
> The IPS was continuing to refine its thinking, he said, and was determined to keep the scheme cost-effective. It planned to use framework contracts that would be able to adapt as new technology came forward. (Timmins 2007b) [4 August: Financial Times]

These reports are the closest the IPS came to publicly acknowledging their intent not to incorporate iris biometrics in the Scheme. All of the Financial Times' reports were critical of the state of the program at this juncture, referring to the Scheme as either "controversial" or "contentious", or quoting business representatives with certain misgivings about the government's approach (Palmer 2007; Timmins 2007a; Timmins 2007b; Eaglesham 2007).

## 7.6 HMRC data breach

In November 2007 UK government officials revealed that Her Majesty's Revenue and Customs (HMRC) had lost two compact discs with the personal records of 25 million British citizens stored on them. This unexpected data breach is the only event on this timeline which is not technically part of the NIS. However, while it occurred outside the case itself, its impact on the case study should not be understated. The proposals for identity cards had remained relatively controversial yet salvageable in the months preceding the data loss, but the government's announcement in Parliament about the misplaced discs initiated a period of sustained criticism and public skepticism regarding the future of the Scheme, despite the fact that the breach did not occur within the Home Office but rather HMRC.

Following the announcement of the breach, ministers and officials worked furiously to manage public perceptions of the government's handling and processing of personal data. This was discursive work. Many of these debates took place in Parliament, with attempts to "enroll" (Callon 1986) biometrics into the debates as a means of preventing or mitigating any future data loss. During this period there was a flurry of talk about biometrics, some of which I quote in extended form below. This talk revealed very important tensions in the hopes for, and known realities, of biometrics.

Alistair Darling, then the Chancellor, was questioned in Parliament about how his announcement affected plans for national ID cards:

> Mr. Douglas Carswell (Harwich) (Con): If the Government have managed to lose 25 million confidential personal records in this way, how can we possibly trust them to run an ID card scheme nationally?
>
> Mr. Darling: As I said, one of the problems is that the information we have at the moment can, in certain circumstances, be used for fraudulent purposes by people who have no right to use it. *The point about ID cards is that because they will introduce biometric information they will mean that one can be more certain that the person asking for or dealing with that information has a legal right to do so.*
>
> Mr. Andrew Robathan (Blaby) (Con): The Chancellor has given my right hon. Friend the Member for Hitchin and Harpenden (Mr. Lilley) and my

> hon. Friend the Member for Harwich (Mr. Carswell) reassurances that any personal information stored for ID cards will be safe. However, after this astonishing display of incompetence, why would anybody have any faith in the Government or trust them to be able to keep personal information secure?
>
> Mr. Darling: *For the reason that ID cards match up biometric information with the information that is held, so that the person holding the information knows that the person asking for it is legally entitled to it. That is the difference between many other systems, which do not have that biometric lock, and the ID card system, which would have that biometric lock.* It seems to me that that would give me and the hon. Gentleman, as individuals, far more protection than there is at the moment. [20 Nov 2007: Column 1110] (emphasis added)

Speaking in the vaguest of terms, Darling assures his inquisitors (and the interested public) that biometrics would somehow provide security against future risks to information held by government, without providing substantive details. The choice of the term “lock” can be understood as a strategic rhetorical frame to assure listeners of the security of the Scheme, yet we are left wanting details about *how* these locks would secure personal information.

The following day, the then-opposition leader and now current Prime Minister (David Cameron) asked the then-Prime Minister (Gordon Brown) specifically about the repercussions of the breach on the Scheme.

> Mr. Cameron: If the Prime Minister really wants to learn some lessons, will he recognise that this appalling blunder comes at a time when the Government are planning a national identity register to draw together private and personal details of every single person in this country? Will the events of the past few days cause him to stop and think about that policy?

> The Prime Minister: I have already announced the inquiries that we have set up, but let me say that 22 out of 25 European countries have identity cards. The right hon. Gentleman's own security adviser proposes identity cards. His own reviewer of the national police force - the border force - says that he is in favour of identity cards. *What we must ensure is that identity fraud is avoided, and the way to avoid identity fraud is to say that for passport information we will have the biometric support that is necessary, so that people can feel confident that their identity is protected*. [21 Nov 2007: Column 1181]

We are told again that it was the biometrics in the proposed Scheme which would have provided the necessary support, confidence, and protection to citizens. These words came from not just anyone: This was the leader of the UK government speaking *for* biometrics in front of an eager Parliament.

Days later MP David Davis returned to the issue of data security, focusing on the issue of the irrevocability of biometrics; in other words, the problems with using biometric data once they are compromised. This was a topic that hitherto had not been discussed in the policy discourses about the Scheme and it was unusual to see such a technical topic raised in Parliament. It is a complicated issue which then-Home Secretary Jacqui Smith tried to sidestep, providing what appears a rote response about the merits of biometric security.

> David Davis (Haltemprice and Howden) (Con): May I ask the Home Secretary about the subject of identity cards? If the Government give away someone's bank account details, that is a disaster, but at least they can change their bank account. *What, precisely, does someone do if the Government give away their biometric details?*
>
> The Secretary of State for the Home Department (Jacqui Smith): There is of course an important protection in an identity card system, through

> the use of biometrics. *Biometrics will link a person securely and reliably to his or her unique identity.* It will therefore become much more difficult for people to misuse other people's identity, even if full details of their biographical information are already known. The current plan for the national identity register is for biometric information to be held separately from biographical information, thereby safeguarding against the sort of eventuality that the right hon. Gentleman described.

In an unusual turn of events, Davis then asked the Home Secretary about an EU data-sharing initiative (known as STORK), which she seemed unaware of – calling his query an "allegation". Again she reiterates the merits of biometrics.

> David Davis: I do not look forward to the day when the National Audit Office or anybody else asks for that information and is sent it. Let us look at the other aspect of identity cards: the question of protection. The Home Office is currently prototyping a European-wide identity card project called Project Stork. How will it prevent a repetition of the disaster of the past few weeks when sensitive personal data are held not by one Government but by 27?
>
> Jacqui Smith: If the right hon. Gentleman wants to give me more information about the particular allegation that he is making, I will of course be willing to follow it up, but the point that I made remains. *The advantage of a national identity register is that it enables the linking of biometric information, maintained on one database, with biographic data, maintained on another, thereby strengthening the protection for individuals in circumstances where, for example, biographic data were stolen or went missing.* That is a strengthening of the current position, which is why any Government or Opposition who are serious about public protection and identity fraud should be thinking seriously about how we address those issues, instead of making hay. [26 Nov 2007: Columns 17-18]

In fact, STORK ("Secure idenTity acrOss boRders linked") is a project for building interoperable identity systems across the EU, which the Home Office has been involved in for years. It appears the Home Secretary was either uniformed or misremembered this program when she was confronted about it in Parliament.

In a final exchange, a member of the Labour government (Kali Mountford) suggested that the NIS would permit on-line, 'card-not-present' biometric checks against a central database. When questioned on this vision, she backtracked to offer a much more modest claim that biometrics merely provide "added protection".

> Kali Mountford: The Opposition's suggestions about ID cards would result in our throwing the baby out with the bathwater. ID cards are a separate issue. *Everyone always forgets that our biometrics stay with us continually. We would not have to carry cards; that is a separate issue. We cannot leave home without our biometrics; they are with us always*. To say that, because of this one mistake- [ Interruption. ] It is a huge mistake; I do not take issue with that fact. But however big it is, and wherever those discs are*, my biometrics are with me now, and no one can take them off me. Wherever I go, they are with me. I could go into a bank and put my fingerprint down, but it would not be on that database because it would be separate from my biographical details.*
>
> Stewart Hosie: *The hon. Lady is making a valiant case, but she seems to be suggesting that any transaction that she wishes to carry out will require her to be scanned and checked against a central repository. I am sure that that contradicts the answer that we got from a Minister some time ago.* From memory, I think that we were told that it would be up to each organisation to determine how the system was used. Is the hon. Lady really suggesting that every single transaction would be checked against a central repository?

> Kali Mountford: I obviously did not say that, but Opposition Members have been implying that this mistake means the end of ID cards. *I was simply suggesting that an added protection for us, in having an ID register, is the fact that it contains our biometrics.* It is there in the proposed legislation that, if organisations want to use our biometrics, that additional safeguard is there for us. I think that it is an additional safeguard that many people would want to have. [28 Nov 2007: Column 318-319]

During this abnormal period of discursive activity about biometrics in Parliament, there was also extended media coverage of the issues. Most of it was damning regarding the future prospects of the Scheme following the HMRC data breach. Some, but not all, of the media's coverage engaged the specific issue of the role biometrics in these information-sharing practices, with representatives from the Home Office emerging immediately in some news reports to attempt to manage public perceptions.

> The Home Office insisted that the biometric elements in its database, the electronic fingerprints and facial scans, will keep it secure and proof against identity theft, even if there were to be a major breach and stolen confidential data.
>
> *"The biometric means that it will be much more difficult to use somebody else's identity, as they will have to provide the correct fingerprint or facial image at the same time. You can't create a fingerprint or a face,"* said a Home Office spokesman. He also emphasised that the identity register would also be protected by a chip-and-PIN with severe penalties for those who tried to access the database illegally. (Travis 2007, emphasis added) [21 November: The Guardian]

Again, these discourses assumed a set of practices around the use of identity cards and biometrics, which in this instance would involve regular biometric checks. Such discourses aimed to set expectations about the future use of biometrics, and in so doing assuage concerns about potential identity fraud in relation to the government's identity program.

At the time a former Home Secretary, David Blunkett, also wrote to the Sun to express his beliefs about the role of biometrics post-HMRC data loss.

> We must separate our understandable concern about access to specific databases from the issue of identity.
>
> A clean biometric identity base, like the one to be used for ID cards, is not the issue. Those who say it is are simply using it as a smokescreen because they never wanted them for phoney 'civil liberties' reasons.
>
> In reality, cards will make it EASIER to protect your identity because they stop other people being able to pretend they are you just because they know your details. (Blunkett 2007) [22 November: The Sun]

Here, as before, Blunkett tried to separate the issue of the data loss from the future prospects of the NIS. He painted concerns about privacy as “phony” and re-iterated the much-exercised claim that biometric ID cards would, in fact, protect against future harms rather than aid them.

Despite such assurances from the government that biometrics would prevent this from happening again, some journalists used the occasion to ponder futuristically and humorously about what a loss of biometric data on the scale of HMRC's breach might be like.

> Tomorrow’s news today. On the eve of the issue of compulsory ID cards all round, a computer disc packed with the highly personal biometric details of 30 million people, that were to have been transferred to the plastic pocket-sized cards once fingerprints and iris-scans had been checked to prevent forgery, has vanished into thin air.
>
> This means, in effect, that for all official purposes, unless the unencrypted disc turns up behind the cushion or stuck to somebody's shoe, half the population no longer exists. (Waterhouse 2007) [26 November: The Daily Mail]

The episode even resulted in a *Bad Science* article, in which science journalist Ben Goldacre mixed scientific wit and sarcasm to criticize the government’s discourses around biometrics.

> Sometimes just throwing a few long words about can make people think you know what you're talking about. Words like "biometric". When Alistair Darling was asked if the government will ditch ID cards in the light of this week's data cock-up, he replied: "The key thing about identity cards is, of course, that information is protected by personal biometric information. The problem at present is that, because we do not have that protection, information is much more vulnerable than it should be."
>
> Yes, that's the problem. We need biometric identification. Fingerprints. Iris scans. Gordon Brown says so too: "What we must ensure is that identity fraud is avoided, and the way to avoid identity fraud is to say that for passport information we will have the biometric support that is necessary."…
>
> So will biometrics prevent ID theft? Well, it might make it more difficult for you to prove your innocence. And once your fingerprints are stolen, they are harder to replace than your PIN number. But here's the final nail in the coffin. Your fingerprint data will be stored in your passport or ID card as a series of numbers, called the "minutiae template". In the new biometric passport with its wireless chip, remember, all your data can be read and decrypted with a device near you, but not touching you….

> Ah biometrics. Such a soothingly technical word. Repeat it to yourself. (Goldacre 2007) [24 November: The Guardian]

Perhaps the most interesting aspect of this entire episode is how the controversy around HMRC's data breach implicated the ID cards program so strongly; however, it did not affect most of the government's other large IT projects in the same way (i.e., with public calls originating from various corners that the systems be immediately scrapped).

## 7.7 ID cards for foreigners and a market for biometric enrollment

The final event on our timeline is, in fact, a double event. In November 2008 the Home Office launched new biometric identity documents for foreign nationals. These were technically visa documents based on new storage and security technologies, but in their discourses about these documents officials regularly referred to them as 'identity cards', even holding a press conference at which (then) Home Secretary Jacqui Smith posed for photographs with a card. The same day, the Home Office published another strategy document relating to so-called front office services. Its intention was to reach out to the market for help in enrolling the country's biometrics.

Taken together, these events generated lots of parliamentary activity. In one exchange, it was admitted that the recurring government vision for on-line biometric checks against the NIR was something that would only occur in the most exceptional of circumstances.

> Lynne Jones: To ask the Secretary of State for the Home Department whether the process of verification of an individual's biometric identifiers for the identity card scheme will check the biometric against a local copy held on the card or against the biometric stored on the National Identity Register. [219764]
>
> Meg Hillier: Verification checks of biometrics identifiers will be made against the card in most cases using the biometrics stored in the chip, for example if the facial image or fingerprint biometrics are verified as part of an immigration check at the border. Only in specific circumstances, for example if an ID card has been lost, would verification of identity take place against the biometrics held on the National Identity Register. Such checks will provide a very secure and reliable means of proving identity. [17 Nov 2008: Column 52W]

As late as November 2008, these debates in Parliament reflected the continuing uncertainty about the Scheme and biometrics therein, even as foreign nationals were being issued biometric identity documents. Much of this uncertainty was technical in nature, but these technical uncertainties had unknown organizational consequences. Another of these was revealed when the (then) Under-Secretary of State was asked about the errors that would likely arise with the use of fingerprints in one-to-many biometric checks in the NIS.

> Lynne Jones: To ask the Secretary of State for the Home Department what estimate she has made of the number of false matches likely if fingerprint biometrics alone are used for the biometric verification for the identity card scheme after the enrolment of (a) one million, (b) six million, (c) 40 million and (d) 60 million individuals. [219765]

> Meg Hillier: The Identity and Passport Service is still in the process of procurement of specific biometric systems, hence we are unable to give an estimate of false matches that may occur. In the event of an uncertain fingerprint match the scheme will make use of human fingerprint experts to resolve uncertain fingerprint matches from the automated fingerprint matching system.
>
> This procedure is used in all large-scale fingerprint systems to control false matches and the process will apply irrespective of the size of the database.

In her response Hillier made assurances that human experts would reconcile false matches, arguing that these measures would apply “irrespective of the size of the database”. This point ignores the need for significant numbers of human experts capable of analyzing increasingly large numbers of false matches as a database the size of NIR grows over time. Consider that the current back-logs in forensic fingerprint analysis in police departments in the US have been blamed on insufficient organizational capacity, including low numbers of trained fingerprint analysts (see, for example, Rubin & Winton 2008).

In similar fashion, Hillier deflected a question about the need for biometrics ‘exception handling’ in the Scheme. This was an issue raised by the Home Office’s own biometrics expert body.

> Lynne Jones: To ask the Secretary of State for the Home Department what response she has made to the views expressed in the annual report for 2007 from the Biometrics Assurance Group on exception handling and fingerprint biometrics of the over 75 year olds for the purposes of the identity card scheme. [224278]

> Meg Hillier [holding answer 12 September 2008]: Responses were only made to the specific recommendations of the Biometrics Assurance Group and as no specific recommendation was made regarding exception handling or the collection of fingerprint biometrics for the elderly, no comment was made. [17 Nov 2008: Column 53W]

Further technical queries in Parliament brought similar non-responses.

> Lynne Jones: To ask the Secretary of State for the Home Department what discussions she has had with the police on the use of (a) non-unique digital representations of fingerprint biometrics and (b) unique pure biometric images obtained via the National Identity Card scheme. [219756]
>
> Meg Hillier: The Identity and Passport Service holds regular discussions with the police on all aspects of the performance of biometric systems and their relevance for the operation of the national identity scheme, via the National Policing Improvement Agency. [20 Nov 2008: Column 724W]

During this period ministers also claimed that the excessive collection of fingerprints from foreign nationals who were then applying for identity documents was needed as a precautionary measure. However, in doing so they risked portraying fingerprint biometrics as unreliable.

> Mr. Grieve: To ask the Secretary of State for the Home Department for what reason 10 fingerprints will be collected from foreign nationals applying for identity cards instead of the two fingerprints required under EC Regulation No. 380/2008. [226409]
>
> Jacqui Smith [holding answer 13 October 2008]: Capturing and enrolling all 10 fingerprints onto our system will allow us to search other biometric databases providing a more robust approach to confirming identity. In the unlikely event we are unable to make a match against the two

> fingerprints held on the identity card for foreign nationals, we can make a further check against the applicant's other fingerprints.
>
> In addition, we can verify identity with other fingerprint records we hold. As such, we are able to tie a person to a single identity which will help tackle immigration abuses and identity fraud. [24 Nov 2008: Column 823W-824W]

The media coverage during this period focused on the prospect of citizens enrolling fingerprints at places such as post offices or high-street shops. Some reports claimed that this was a way for government to channel new business into the struggling post office network, thus propping up the Royal Mail. In these news reports it was understood that the decision to outsource the enrollment of biometrics was driven by concerns about managing the costs of the Scheme, although it was not pointed out that the costs would simply be deferred to citizens rather than be saved.

The mainstream newspaper reports on the launch of biometric immigration documents for foreign nationals were few and far between and framed in very particular ways. Only a few of the major broadsheets and tabloids covered the event, and when they did they tended to blur the distinction between identity cards (for UK citizens) and immigration documents (for foreign nationals). For example

> The first compulsory identity cards in Britain since the 1950s will be issued this week to thousands of foreigners living in this country, the Home Office will announce today. (Ford 2008) [25 November: The Times]

This was, in part, due to how the government publicized the Scheme. In branding the biometric immigration document as an ‘identity card’ in its informal public discourses, it was able to prove its successes in delivering the proposals. The week following the announcement of foreign national ‘identity cards’, only one of the mainstream newspaper articles drew the connection between the collection of fingerprints from foreign nationals and the eventual use of the technologies in the NIS.

> For the first time since 1952, the British government is issuing identity cards. In order to test the system and ease its introduction, there is to be a cynical requirement for foreign nationals resident in the UK to register. To begin with, this will affect students and the foreign spouses of British citizens. The fact that they already possess an identity document - a passport and/or a visa - does not seem to enter into the Government's thinking, principally because they are guinea pigs. Over time, residents from outside Europe will be fingerprinted and have to account for their movements. Starting in 2010, so will the rest of us. (Anonymous 2008) [26 November: The Daily Telegraph]

This comment piece noted that the people from whom multiple biometrics were then being collected were the ones who already possessed identity documents in the form of passports, which they required to enter the UK in the first place. Issuing them with a new document seemed overkill – unless, of course, what mattered was not the ID document itself but rather the additional information that was being collected during the document issuance process, including fingerprint information. Requiring foreigners to attend a special appointment to enroll these biometrics, which often involved travelling long distances, created additional burdens as they endured what was supposed to be a “quick, easy, and safe” process. It was in this respect that foreign nationals were said to be the “guinea pigs” for another government biometrics program: the National Identity Scheme.

However, as it turned out, “the rest of us” were never mandated to enroll our biometrics for identity cards. This was not because the technology failed miserably during experiments on the foreign national “guinea pigs”, but rather due to the political forces that resulted in a change of government in 2010 and eventually legislation that terminated the program for national identity cards. Yet it is still compulsory for non-EEA foreign nationals to submit their biometrics in exchange for the right to remain in the UK and, in doing so, endure many inconveniences and doubts about issues of proportionality. It is not the case that the experiments are over. They are ongoing, although the media attention on these issues remains especially limited.

## 7.8 Conclusion

This chapter built on the initial analysis of government discourses on biometrics by exploring how parliamentarians discussed the concept during certain moments of interest in or around the NIS, as well as the attendant media coverage of these events. We discovered what appear to be misunderstandings about biometrics in Parliament, in addition to some highly politicized exchanges following HMRC’s data loss. Over time, the media reporting on the Scheme became increasingly critical, although the coverage of the biometric component was patchy and usually lacking in detail. In the next chapter we further reflect on these discourses and the role they play in innovation and policy processes.

# Chapter 8: Concluding discussion

## 8.1 Introduction

This final chapter presents an extended discussion on the major findings from the case study analysis. These findings offer contributions to knowledge, including an extension of theory on visions and new technology. The insights drawn in this chapter are applicable to ongoing worldwide efforts to replace existing methods of identifying, profiling, monitoring, and tracking individuals with high-technology applications meant to improve organizations' ability to perform these tasks. If this research is to offer an enduring scholarly contribution, it is likely that the lessons learned about the technological discourses and visions from the case of the National Identity Scheme (NIS) will be applicable in other settings where there is an apparent rush to embrace high-technology solutions to myriad and complex policy dilemmas (real or perceived), even whilst the direct and broader implications and consequences of applying the technologies are largely unknown.

## Looking back

Before delving into these findings and discussing their implications, I first want to revisit the intellectual journey to this point. This summary will help us to appreciate the scope, significance, and limitations of the research findings.

A critical review of the relevant technology and social science literature revealed that the research, to date, has not analyzed biometrics as a *political and organizational process*. The computer science literature remains focused on refining the technologies and techniques for bodily identification, largely unconcerned with larger social and political implications of ‘perfecting’ the technology. In contrast, an important limitation of the social science literature is that it often reifies the concept of biometrics and ignores important differences between and within the different technologies (other than sometimes acknowledging performance variances). These ethical and sociological critiques frequently take biometrics and their practicability as a given, rather than as a complex outcome of various political, organizational, and technological negotiations.

Finally, the information systems research on biometrics has to date been committed to building and improving technology acceptance models. Such approaches take user acceptance as a generally positive and desirable goal. These technology acceptance studies fail to accommodate the role that context plays in adoption-related decisions; that is, how context constructs and gives meaning to the technological artifact, as well as how it affects acceptance and resistance dynamics. Moreover, these studies do not explicitly acknowledge that in many contemporary adoption contexts, biometric technologies are compulsory or pseudo-voluntary, which upsets the notion of 'acceptance'.

I chose to use discourses about biometrics as a means of representing context because in the case biometrics were largely the *product* of language and discourse. In other words, our access to the technology was through the words used by actors to describe, frame, and makes sense of the government's proposals. Furthermore, the timing of the case study and the eventual demise of the program meant that our primary analytical access to 'biometrics' in the Scheme was not through actual interaction and/or use, but instead through the public discourses intending to bring them to life.

To address the research lacunae in the literature, I proposed to leverage the concept of organizing visions, in particular, to explore the organizational discourses that accompanied the proposals for biometrics in the NIS. I chose to supplement this concept with ideas from the sociology of expectations – which implore us to interrogate the different functions of future-oriented discourses around new science and technology – as well as critical approaches to the study of the public's understanding of technology. This theoretical framework provided a conceptual guide to address three research questions:

1. How did government spokespeople portray a vision for biometrics in the National Identity Scheme, and to what extent did this vision organize efforts and mobilize actors to innovate?
2. How did policy debates and attendant media reportage discursively capture biometrics, and what were the limitations of these discourses in revealing the complexities and perplexities of the technologies?
3. How were the 'publics' of biometrics portrayed in these discourses?

To answer these questions, I chose to analyze every publicly available government-issued policy-related document pertaining to the NIS published between 2002 and the end of 2008. These documents conveyed the government's vision for the implementation and eventual use of biometric identity cards throughout the UK. In particular, my focus was on public statements made about biometrics and their perceived attributes, applications, reliability, and social impact, as these issues were flagged by Orlikowski and Gash's framework. These statements were analyzed using techniques from critical discourse analysis, in which language is understood as a form of social practice that should be contested and unpacked by informed researchers.

Beyond these formal policy documents, I also analyzed the parliamentary debates and media reportage about biometrics, revolving around certain ‘critical moments’ during the development of the Scheme. These were moments when the NIS was in the public spotlight following a major event or when biometrics underwent an important policy re-think. The discourses that emerged in these arenas provided different perspectives on the government’s vision for biometrics and the public life of a controversial technological innovation.

Through this two-part analysis, we found answers to the research questions. Section 8.2 reviews the history of the government’s vision and summarizes the answers to the first and second questions. The timing of the case study and coincidental demise of the National Identity Scheme allowed us to go beyond simple exploratory questions to look more closely at *why* the government’s vision did not succeed, which we do in section 8.3. Section 8.4 focuses on the theoretical contributions emerging from the discussion on visions and technology. Section 8.5 summarizes the findings from the third research question, concerning technological publics, and observes some areas for theory development. Section 8.6 reflects on the insights afforded by my research lens, which combined a qualitative IS approach with ideas from science and technology studies (i.e., sociology of expectations and PUS). This in-between position allowed me to view biometrics in novel ways, differentiating my approach from the technical studies on biometrics and the critical sociological studies. Sections 8.7 and 8.8 discuss the limitations of this project and areas for future research, respectively.

## 8.2 The unraveling of biometrics

In chapter 3 we explored the concept of an ‘organizing vision’, which tries to explain how organizations seeking to develop and implement new technologies deal with their inherent uncertainty and ambiguity. By unifying and coordinating discourses, organizing visions help to reduce doubts or unknowns about the future adoption and use of technology. With a single vision and a single goal, it becomes easier to implement a new technology, all the more so if potential defects or imperfections can be discursively diminished. These discourses draw on a pool of conceptual resources that exist within and beyond the organization, and which are shared by a larger community that is also interested in the technological innovation. When the organization brings together these cognitive and discursive resources in a *cohesive* manner, the organizing vision is said to be more stable, and thus sustainable. However, problems may arise – “where the innovation entails novel technology, this task can appear especially speculative and problematic” (Swanson & Ramiller 1997, p.459). In these cases, formulating and sustaining an unproblematic vision may prove difficult.

Recall that the basic functions of an organizing vision include *interpretation*, *legitimation*, and *mobilization*. Because new technology is always uncertain and its essential features are difficult to articulate pithily, an organizing vision provides a means for actors to interpret novelty within conveniently limited cognitive boundaries – to imagine complexity without polysemy – whilst bestowing upon the technology and its purpose a coherence and simplicity that are required for non-experts to talk meaningfully about it.

The organizing vision's legitimizing function seeks to answer the question: 'Why do it?'. If the vision provides a clear and intelligible rationale for pursuing an innovation, then another crucial hurdle to success is lowered. An organizing vision mobilizes actors by activating, motivating, and structuring the forces needed to realize the innovation, including actors within the organization as well as external players (such as those in the marketplace).

In the case of the NIS, the government attempted to develop a vision for introducing and scaling biometrics, although it was ultimately stillborn. What happened?

In the nascent stages (2002-2004) of the UK government's proposals for a national identity system, the vision for biometrics was bold and aspirational. The stated goal was to collect at least four biometrics (face, fingerprint, iris, and signature) from virtually everyone in the country, including citizens and long-term visitors. Certain politicians also openly contemplated the collection of everyone's DNA. The government's aim was to provide 'unique identities' to everyone in the UK and biometrics provided a technological means to achieve this goal. In these early moments, the stated purposes of enrolling and storing multiple biometrics were focused primarily on facilitating and managing access to social entitlement programs, although the prime motivation was said to be the international requirement for biometrics in next-generation travel documents. Specific details regarding how the government would collect, store, and use these data were sparse at this point, for in these early days the objective was to aim high and captivate both citizens and the public sector and business organizations that would need to be involved in the government's project. It was literally visionary.

As time went by, and following the high-profile terror attacks of July 2005, the government's stated reasons for collecting extensive biometric data shifted to emphasize security and counter-terrorism priorities, thereby focusing less on social welfare. In their public discourses, the government remained intent on enrolling face, fingerprint, and iris biometrics, although as 2006 closed iris biometrics featured less prominently in government discourses. Influenced by growing concerns about costs (that had been spurred by academic researchers and civil society groups), the government concurrently began stressing that the Home Office already had the requisite skills and expertise in-house, which were being developed in its visa and asylum programs, to accomplish its mission for the national biometrics program. Different components of the vision for biometrics were being reformulated in response to external resistance.

By 2007 it became apparent in government discourses that iris biometrics were no longer an immediate option in the Scheme, which affected the stated aim of securing unique identities for everyone in the UK. This made the vision for biometrics less compelling, for iris recognition was both the most futuristic and best performing (in terms of match rates) of the different technologies. It is plausible that, had the government excluded iris biometrics from its proposals prior to the parliamentary passage of the *Identity Cards Bill*, it would have been much more difficult to make a convincing case that the choice of biometrics was capable of achieving the aim of uniqueness. But once the Bill had officially become an Act, there was less pressure on the government to justify certain design decisions to Parliament, so it was able to shelve the iris biometrics component of the Scheme without major political backlash.

During this period, government discourses on the reasons for using biometrics increasingly centered on resolving or fixing a generic set of identity-related problems and crimes. It was as though the messaging on their motivations for using biometrics grew less specific as time passed – that the reasons for pursuing biometrics were obvious. Claims of achieving unique identities through biometrics persisted, despite doubts about the technologies' capacity to fulfill these hopes. In 2007 it was also revealed through a leaked Home Office document that there were doubts within the organization about the need to fingerprint everyone in the Scheme, although these were not reflected in the public discourses on the project, which would soon begin attempting to mobilize a market for biometric enrollment involving private sector stakeholders.

Before these efforts to involve the private sector in the collection of citizens' biometrics were ramped up, however, an unexpected data breach at HMRC dealt a serious blow to the government's proposals. The vision for securing citizens' identities through biometrics became less believable once the government announced that 25 million personal records had been lost during a routine data transfer. The government made attempts to discursively portray biometrics as a solution to, rather than a victim of the breach, but these did not resonate amongst the media and public, who grew increasingly skeptical. Resistance to the program was mounting and the future of the Scheme grew increasingly in doubt.

Political parties took varying positions on the proposals for biometrics and made them an important point of policy differentiation. While the Labour party stuck to its guns and continued to endorse its policy, every other major UK political party came out in opposition to the program as the 2010 general election neared (Whitley & Hosein 2010a). With the main political opposition (i.e., the Conservatives and Liberal Democrats) intensifying their anti-ID card rhetoric throughout 2008 in the run up to the election, which further jeopardized the future of the Scheme, the Home Office aimed to demonstrate that identity cards were already a reality (so as to try to prevent the Scheme from being terminated in the event of a change in political leadership). It did so on two different fronts. First, by issuing biometric identity documents to non-EEA foreigners from November 2008 and labeling them ‘ID cards’ in their public rhetoric. Second, by offering national ID cards to a limited number of citizens (who already held e-passports) starting in 2009. These national ID cards were biometric in the sense of involving the collection of face and fingerprint data from citizens, but this outcome was a far cry from the original vision of capturing multiple biometrics, including iris, with which to conduct 1-to-many biometric checks against a large centralized data store in real-time.

These politics also affected the content of the government’s vision for biometrics, with spokespeople reworking the main message to focus on frames of ‘empowerment’ and ‘inclusion’ as the Scheme’s fate grew more and more uncertain. But in the end, the Conservative-Liberal Democrat coalition government dismantled not just the NIS and biometric identity cards, but also plans for second-generation biometric passports (with fingerprint data), sparing only foreign nationals from their change of plans. The government’s vision had unraveled and the coalition’s counter-vision triumphed.

Concerning the second research question, on the capacity of policy debates to capture the complexity and perplexity of biometrics, we discovered several dynamics. First, the technical complexities of biometrics emerged when MPs such as Lynne Jones quizzed ministers in Parliament on technical specifics. How would the Home Office approach ‘exception handling’ in the event of biometric errors? Would the NIS store raw images of fingerprints or biometric templates? However, by and large these technical and scientific deliberations were absent from the public discourses. They were virtually non-existent in the policy documents reviewed in chapter 6. In Parliament, spokespeople mainly provided non-answers to such overtly technical queries and stayed on script to highlight the ‘obvious’ strengths of biometrics, such as the ‘uniqueness’ of identity they afford every individual.

The government also obscured or avoided the technological when it proved rhetorically convenient to do so. Talk of ‘international obligations’ for biometrics overlooked the exact requirements for particular biometrics (i.e., facial images) in passport documents, which were more relaxed than those envisioned in the NIS. Spokespeople deflected or shied away from questions about the limitations of fingerprints in achieving ‘unique’ identities (after iris biometrics were ruled out on costs grounds). In these instances, the technological was conspicuously and strategically left out. Generic talk about ‘biometrics’ facilitated many of these discursive strategies.

Finally, in the case study many of the political discourses on biometrics tried to simplify complexity and de-politicize the choice of technology. In certain instances, biometrics were described as “just like having a picture taken” (Home Office 2005c, p.6). On other occasions, talk about the benefits of ‘biometric checks’ grossly simplified the complexity of 1-to-many identification against large numbers of enrolled records. Spokespeople sought to proactively set public expectations by asserting, for example, that the biometric process would be “quick, easy, and safe” (Cragg Ross Dawson 2004c, p.95).

## 8.3 From muddled discourses to stunted visions

One outstanding matter concerns the reasons the government’s vision failed to organize the actors and resources necessary to realize its innovation. Why did the vision fail? The answers are complex. What is clear from the narrative above is that the term ‘biometrics’ served an important interpretative function in the government’s vision. As we first discovered in the analysis, the concept provided a convenient discursive catchall for capturing a variety of different technologies and techniques, including not only fingerprinting, iris scans, and facial recognition, but also modes such as signatures (at least when it was rhetorically convenient). ‘Biometrics’ was an ambiguous and unsettled concept in this vision. Being perhaps unfamiliar with the intricacies of the technologies, government actors were often inexact and unclear in their discourses on the subject. They nonetheless spoke in terms of ‘biometrics’ and roughly communicated their plans and objectives for the technology in the Scheme, particularly focusing on assigning everyone a unique identity.

These are observations that fit within Swanson and Ramiller’s organizing visions theory, which permits a degree of flexibility in actors’ interpretations of, and discourses on, what technologies do and what they can be used for, especially in the early stages of innovation. A relatively plastic vision allows different actors to assign their own meanings to a new technology and work locally with the concept, with each more or less believing in their contribution to the greater vision.

However, it is arguable that in the case the government's use of the term 'biometrics' was *too* loose, especially in the later stages of the Scheme's development when it was realized that specific technologies (such as iris) would not be used and when more meaningful messaging was required to mobilize external actors. While the ambiguity inherent in the term often afforded spokespeople a degree of rhetorical currency, there were important occasions when the complexity and diversity of the concept was lost on many actors (such as after HMRC's data loss). Over time, the government's messages on biometrics – and particularly those by public-facing politicians – turned increasingly mixed and confounded[23] and its vision for biometrics was stunted.

The second function of an organizing vision is its capacity to legitimize an innovation. To that end, the case study revealed that biometrics were paired to a wide range of pressing governance priorities, which changed over time. Beyond being an international obligation or something that all 'good' governments were doing, they were variously supposed to provide every individual with a unique and secure identity (although this alone did not provide a policy motivation for biometrics – secure, unique identities *for what?*), improve public service delivery and make it more efficient, assist in

[23] For example, I recall attending a public lecture in 2009 by Labour MP Meg Hillier on the topic of ID cards. After her speech, experts from the IPS felt it necessary to approach the journalists in the room (with whom I was sitting) to correct many of her statements about the Scheme, including those about biometrics.

immigration procedures, aid and secure personal finance, facilitate international trade and travel, secure the UK's borders, help to fight terrorism and prevent crime, and ease the administration of police work, among other policy goals. In sum, government actors found the concept of biometrics so compelling that they attempted to discursively frame the technologies as a solution to a wide range of different policy problems. But this failed to convincingly legitimize their use.

One of the reasons for such sweeping enthusiasm was the immense chorus speaking for the technology, including numerous politicians, many of whom experienced abbreviated terms in office, and also various civil servants. Representatives from the Home Office and its sub-departments (the Identity and Passport Service (IPS) and the Borders Agency), and the Cabinet Office all chimed in. But their reasons for doing so were diverse.  At times this resulted in mixed discourses that confused the overarching vision. The trustworthiness of the vision's authors also emerged as a problem, with increased skepticism of the government's motives apparent in media reporting on the NIS. And occasionally the content of the government's discourses was in competition. A vision incapable of organizing and mobilizing due to such factors eventually unraveled and debilitated, destabilizing the project as a whole.

According to Swanson and Ramiller, the extent to which a vision supports the interpretation and legitimation functions depends on how *compelling* it is. They speculate that a vision's compellingness is based on a number of factors, including its a) *distinctiveness* (does it attract and hold actors' attention?), b) *intelligibility* (is the vision coherent?), c) *informativeness* (is it rich in meaning?), d) *plausibility* (can it realistically be achieved?), and e) *perceived practical value* (is it worth pursuing?). I contend that during the rollout of the Scheme, the government only satisfied the first and last of these factors (i.e., distinctiveness and perceived practical value) in its discourses. As the factors that went unaccomplished:

*Intelligibility*: While the government's plans for biometrics were grand and attractive, they lacked an enduring coherence, both in terms of what they were supposed to accomplish and the government's plan for making the system a reality.

*Informativeness*: The discursive fixation on uniqueness resulted in a superficial and relatively uninformative vision that could not convincingly explain *how* biometrics would achieve unique identities in practice and why uniqueness was even necessary. It was not enough to simply say that biometrics were unique; assuming that they are, this presumed characteristic needed to be consistently linked to a pressing policy priority for it to be informative and worth pursuing.

*Plausibility*: The vision's plausibility was undermined as the Scheme unfolded, as it remained highly uncertain throughout the case how the government would achieve its program. Although there was arguably considerable practical value in the idea of using biometrics as the cornerstone of a national identity system (especially in a country such as the UK without a legacy ID system), the government failed to formulate a compelling discourse on how it would garner the technological and organizational resources required to make it happen, which hindered the processes of mobilization.

And thus, the third function of an organizing vision involves mobilizing actors for the purposes of materializing an innovation. There were at three main groups of actors that the government aimed to mobilize in the case: the companies engaged to help the Home Office build the NIS – including systems procurement and the outsourcing of biometric enrollment; a wide range of other public sector departments (which were expected to adopt the technologies and contribute to their diffusion); and the public, who were supposed to be the eventual end users of the system.

We will never know for certain whether the vision for biometrics would have successfully mobilized industry to develop and implement the biometric systems and services required for the NIS had the Labour won the 2010 general election. By 2008, several firms had been engaged through the *Strategic Supplier Framework*, and certain contracts had even been agreed, but the program for biometric identity cards was ended well before large-scale procurement and system design were completed. Before, during, and after the election, we witnessed the demise of the Scheme, not because there were not any commercial actors willing to work with the Home Office, or because the technology failed to live up to expectations, but rather due to the course of political change. In brief, mobilization efforts were cut short by politics and in the process the debates about the technology's readiness, reliability, and practicability were never entirely resolved.

As of 2010, none of the government departments that were expected to take up the biometric systems being developed for the Scheme had committed to using them (with the possible exception of the UK Border Agency, which was already collecting biometrics from foreigners[24]). Champions of the NIS had failed to mobilize these important organizational actors into their cause. But as

[24] The National Identity Scheme and the UKBA's program for biometric immigration documents were different programs despite the public discourses that regularly blurred the distinction. In addition, the UKBA's systems were arguably easier to implement because they owned the operational spaces in which the systems would run. They were also the sole intended users of these systems, unlike the NIS, which was expected to operate across public and private sector organizations.

before, this was arguably a matter of timing. The Home Office had cautioned that uptake by government departments would only begin once its identity infrastructure was in place. The general election disrupted the original time frames for this project.

Finally, the third set of actors to be mobilized in the Scheme was the public. Suffice it to say, this was an enormous and diverse group of people, whose bodies were intended to be read, recorded, and repeatedly validated by biometric devices. Their mobilization was especially critical to the Scheme's success but the government's program for identity cards and new (fingerprint) biometric passports was terminated before the public were to begin enrolling their biometrics *en masse*. The systems required for mass enrollment were never implemented. Critics such as No2ID had argued that it was at the point of enrollment that public resistance would mount, but this is a hypothesis that remains untested. What is known is that by the time the Scheme was finally scrapped, only 14,670 Britons had volunteered for an identity card. A significant fraction of these – nearly 3,000 airside workers from select airports – received their identity cards for free. In addition, an unknown number of the enrollees were civil servants who were privately encouraged to apply for an identity card before the election (Lettice 2010). I further explore the category of the 'public' later in this chapter, where I focus on the discourses on the public and its understandings of biometrics.

Table 8.1 summarizes the outcomes of the three functions of the government’s vision for biometrics in the Scheme and offers summary explanations for the failed vision.

| Function | Findings | Explanation |
|---|---|---|
| Interpretation | The term 'biometrics' played an important interpretive role in government discourses, providing a generic yet attractive concept with which to sell the merits of the Scheme. But it was not robust enough to sustain a long-term vision. The discourses that comprised the vision could not cope with the complexity and diversity of the technologies being proposed. They failed to capture the important differences across the various techniques and technologies under consideration, particularly as iris recognition disappeared in government discourses and was excluded from procurement documents. The concept's interpretive value diminished over time. | The interpretive function of an organizing vision must be able to bestow meaning to a novel technology *and sustain it*. The concept of 'biometrics' failed to do so in the case study. Despite being relatively distinctive and offering some practical value, the vision was not sufficiently intelligible, informative or plausible to enable the intended innovation in the case. |
| Legitimation | The many different reasons espoused for using biometrics in the Scheme, including disputable international obligations, resulted in government actors not being able to persuasively and coherently articulate *why* the proposed biometrics were needed. Over the course of the Scheme, their vision encountered considerable resistance in discourse arenas such as the media. The master frame of 'uniqueness' was repeatedly employed to combat these counter-discourses and help legitimize biometrics, but by itself it did not offer a compelling policy justification for the technologies. | This result was partly due to the large number of officials speaking on behalf of the Scheme, who felt it necessary to discursively link biometrics with a wide range of policy dilemmas. The result also reflects a level of distrust in the messenger (i.e., government officials). Proposals for a system with more trustworthy spokespeople, or one with a more narrowly specified and convincing purpose for biometrics, may have been better at legitimizing their use. |

| | | |
|---|---|---|
| Mobilization | The government was unable to mobilize the extended network of actors in the case, including commercial parties, public sector organizations (that were intended to adopt the government's biometric systems), and members of the public. | This is an artifact of the short-lived development of the Scheme, which was terminated before major mobilization efforts began. Mobilization takes time, and politics cut short the government's plans. There is, however, an outstanding question regarding whether mobilization is possible if the interpretive and legitimizing functions of an organizing vision remain unfulfilled. I explore this point in the next section. |

Table 8.1: Summary of outcomes of the government vision for biometrics in the Scheme

## 8.4 Extending visions theory

What can we learn from this episode that might offer a contribution to theory? A number of themes arose during the case study that merit further theoretical exploration.

Incongruent discourses: There were multiple organizations motivating the National Identity Scheme. It was a Labour party policy, which the Home Office and IPS were responsible for implementing. The presence of several spokespeople (including both politicians and civil servants), who are responsible for jointly articulating and conceptualizing a coherent vision for a new technology, may lead to coordination problems such as those that we encountered in the case study. While Swanson and Ramiller acknowledge that disagreements over a vision’s content may arise, the cases they present do not account for the complexities of coordinating and promulgating visions across multiple organizational contexts.

Competing discourses: One of these contexts – arguably the most important and challenging one in the case – was the political sphere. We must also account for the role of politics in organizing visions, and in particular how politics lends itself to competing visions for new technology.

A vision for the implementation of an ERP system in a bank may encounter resistance, which may even be political in the sense that the introduction of the technology alters institutional hierarchies and work routines, but it is unlikely to be tightly bound to notions of citizenship, freedom, and political identity. By contrast, as the result of ongoing counter-discursive work by activist groups and political opposition parties, the government’s proposals for biometric identity cards elicited considerable political distrust, fears of government tracking innocent citizens, and worries about unwarranted privacy intrusions and security risks, as was represented in the media reporting on the NIS.

There is a qualitative difference between a vision for a corporate accounting system, for example, and a government-sponsored national identity system.

The former is a solution to a perceived problem. The latter is a political choice about how society should be organized, where the search for a solution may precede the event of a problem (as was demonstrated by the government's inability to successfully legitimize biometrics in the Scheme). Where the impetus for such a large effort seems the stuff of choice and not necessity, political opposition is difficult to surmount. Not surprisingly then, the government's proposals became highly politicized over time as the urgency that supposedly underpinned them grew more and more elusive. Resistance originated in different arenas, including civil society and opposition parties. Groups such as No2ID offered counter-discourses for biometrics in the Scheme, portraying them as expensive and invasive.

**When is a vision?** Finally, organizing visions theory takes for granted that discourses about a new technology assemble to form a vision, which then organizes actors and resources to innovate (or not). The success or failure of the organizational effort is the main focus, rather than the existence of the vision itself. It is largely assumed (or overlooked) that a vision exists. However, the government's frustrated efforts to envision biometrics in the case force us to consider analytically the criteria of a vision for new technology. That is, when is a plan for new technology a vision (as opposed to merely a set of ideas)? What distinguishes ideas and visions and explains their varying capacity to facilitate innovation?

Swanson and Ramiller also accept that there may be different visions emanating from a discourse community that disrupt one another during innovation processes. However, in the case of the National Identity Scheme we encountered more than a simple inter-community contest of visions. The combination of the incongruous discourses emanating from the Home Office, the Labour party and its associates, the complexity and magnitude of the proposals for biometrics, and the politics of privacy and surveillance that emerged over time (fed by the counter-discourses of activists and opposition politicians), had a unraveling effect on the government's proposals. Despite their best efforts, the Labour government could not recover control of their vision, nor could they refine it after certain key policy decisions, such as the eventual exclusion of iris recognition from the Scheme. These were developments that the organizing visions concept as originally conceived does not easily accommodate. We therefore need to account for these dynamics in a contribution to IS theory on visions and technological change.

Therefore, in this section I juxtapose Swanson and Ramiller's conceptual formulation with my own contributions to theory on technological visions, which are derived from the case study. This comparison is focused around three dimensions: the ontology of visions, temporality, and resistance to visions for IT innovation.

## Ontology

We must examine the basic relationship between ideas and visions. In their original paper, Swanson and Ramiller's focus was on the capacity of visions to organize actors and resources to innovate using new information technology, but they did not define or theorize visions per se. They defined an *organizing* vision as "a focal community idea for the application of information technology in organizations" (1997, p. 460), but took for granted the ontology of a vision itself. According to their definition, visions are understood in terms of ideas, but not all ideas are visions. Swanson and Ramiller believed that a community must exist to adopt and develop an idea (or set of ideas) for it to become a vision. Visions are thus understood as shared ideas. But does the sharing of an idea necessarily constitute a vision? I argue that it does not. An idea shared by few individuals is in itself not a vision (cf. Dierkes et al. 2006), but Swanson and Ramiller did not provide a thorough account of what makes a vision. Organizing visions theory, therefore, insufficiently conceptualizes its core concept (i.e., the vision) and what distinguishes it ontologically from other phenomena, such as ideas. I argue that, before it can organize, an organizing vision must first actually be a vision, and not simply a mere idea, belief, or expectation (or collection thereof) about new technology. We must thus tease out the differences between these concepts.

Building on the ideas of Dierkes et al. (2006, p.104), I assert that a vision requires a) the presence of a potentially visionary idea, b) the development of this idea by a community, and c) the broadening of consensus around this idea beyond its original community. They argue that consensus is a "constituent element of visions" and that the "ideas of a few individuals, no matter how innovative or brilliant, obvious, captivating, fascinating, or logical they might be, are in themselves not visions" (Dierkes et al. 2006, p.101). These points provide a basis to theorize more thoroughly the vision concept.

While the relative size of the community entertaining an idea is important for its development as a potential vision, I would argue that the *essential* feature distinguishing ideas from visions is *agency*. My suggestion is that an idea becomes a vision when it begins to assume its own agency, independent of its spokespeople. Without agency, a potential vision remains a loose collection of ideas about a new technology, and requires a group to continually nurture it in order to keep it active and sustain it. A vision, however, can temporarily exist independently of the community that defines and shapes it. Through its agency, a vision traverses the discursive arenas where innovation happens. Having become a vision, an idea can be taken for granted by the community, although not indefinitely – visions still require discursive work, specifically to keep them intelligible in light of technological and organizational change. A vision's agency is what provides its capacity to organize and mobilize. In fact, it requires it. But it does not last forever.

This distinction makes way for an alternate theoretical explanation for why the government's proposals for biometrics were unsuccessful. Rather than pointing out, according Swanson and Ramiller's theory, that the plans for biometrics failed because the government's vision was unable to provide a coherent interpretation and compelling legitimation for biometrics, we can conceptually distinguish between ideas and visions to explore *whether the government was ever even able to develop a vision for biometrics*. That is, instead of taking the concept of a vision for granted, as Swanson and Ramiller seem to do, we can instead seek it out empirically. Whereas visions may or may not organize people and resources to innovate, by definition ideas by themselves cannot due to abovementioned limitations of consensus, scale, and agency.

The first step for a researcher, therefore, is to decide whether the innovation-related phenomenon in question is best classified as an idea or a vision. To do so, one should determine whether there is relative consensus about the concept and, more importantly, study the organizational discourses that comprise visions for signs of agency. That is, does the phenomenon assume a 'taken-for-grantedness' by the community or does it require ongoing discursive work to keep it active? If the former, then it is probably a vision and is more likely to facilitate and organize innovation, so long as the three functions of an organizing vision can be satisfied. If the latter, then it is likely merely an idea and its capacity to enable innovation will be severely limited. Importantly, just because spokespeople call their idea a vision (as was repeatedly the case in the case study) does not make it so. This fact must be discerned empirically by studying the relevant discourses.

## Temporality

This leads us into a theoretical discussion on the temporality of visions. While Swanson and Ramiller discuss the ‘career dynamics of organizing visions’ (pp.468-469) to address how visions are successful or not in terms of enabling IT innovation, their account of the processes of visioning leaves a number of questions unanswered.

Picking up on the previous section, the temporal processes through which ideas become visions are not discussed by Swanson and Ramiller. In their account, the life and career of an innovation begins with a vision – the vision’s pre-history is not studied. Nor do they explain how visions progress to become organizing visions. In the preceding section I provided a working hypothesis for how ideas become visions through their acquisition of agency, which allows them to assume an independent discursive existence, albeit necessarily provisional. Once an idea matures into a vision, however, what processes are at work to enable it to aid innovation and how do these processes connect temporally?

Focusing on the three *functions* of an organizing vision (interpretation, legitimation, mobilization) in particular, it is not entirely clear *how* they interrelate temporally in previous empirical accounts. It appears that Swanson and Ramiller did not view the functions as separate and distinct temporal phases that must conclude before the next starts (e.g., first interpretation, then legitimation, and finally mobilization). Instead, functions appear to operate in conjunction, with interpretation, legitimation, and mobilization sometimes occurring at the same time, depending on the innovation context. For example, it is often the case that visions provide degrees of interpretation and legitimation for new technology simultaneously, particularly when questions arise about a new technology's purpose and capacity to solve a problem. Yet it is doubtful that mobilization can be successfully achieved if the interpretation and legitimation functions of an organizing vision are retarded. How would market actors mobilize without a reasonable understanding of *what* an innovation aims to achieve and *why* it is necessary? We encountered such a dilemma in the case study, in which mobilization efforts were stunted partly because the government's project for biometrics remained uninformative and unpersuasive. We therefore need to account theoretically for the temporal ordering of visions and the functions of organizing visions.

The insights provided by the case study do not permit a conclusive account of the temporality of visions – such are the limitations of the case study approach. However, a tentative theoretical model can be suggested, based on the findings from the case of the NIS. Figure 8.2 represents a temporal model of visions, which complements and extends Swanson and Ramiller's original account of organizing visions.

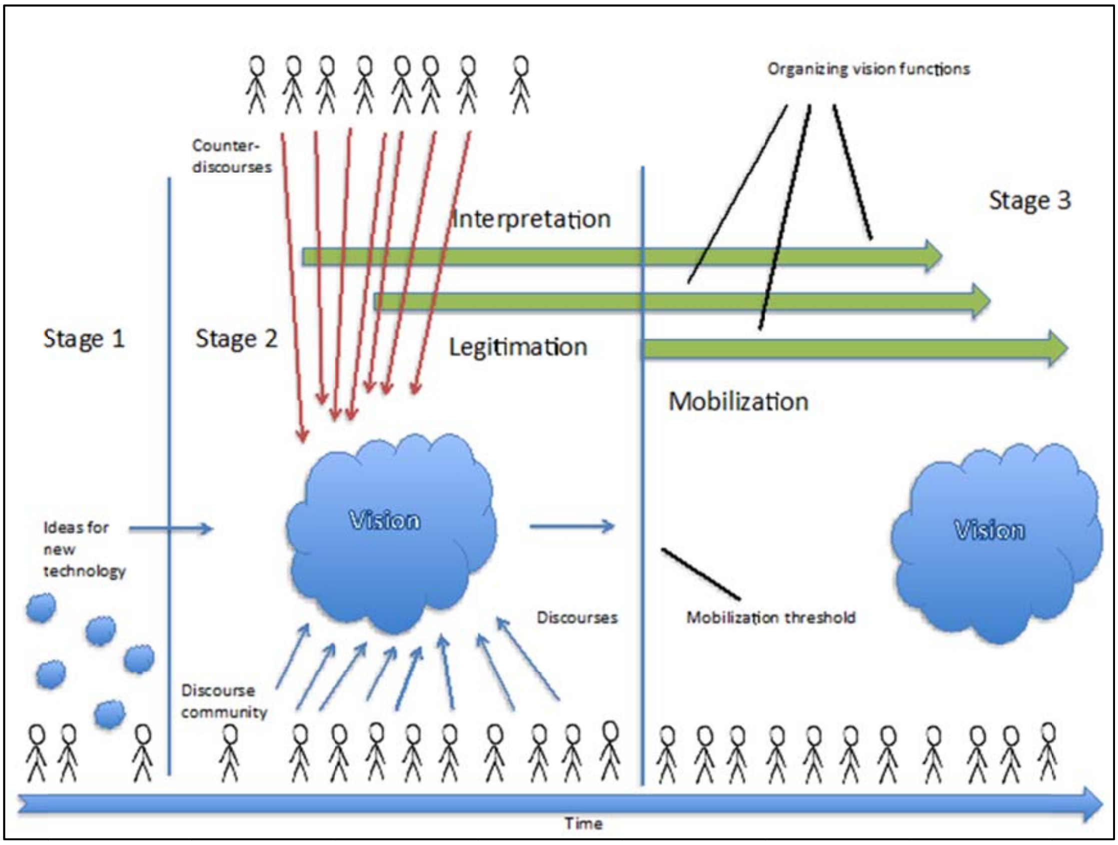


Figure 8.2: Temporal model of visions for new technology

The model depicts three main temporal stages of technological visions:

The first stage represents the pre-history of a vision for the use of new technology, when it is merely an idea or set of ideas possessed by a single person or small number of people. At this stage, the potential vision lacks the discursive coherence required to be a vision and it is only a concern of a relatively small number of actors.

As an idea develops into something that more people are interested in understanding and engaging with, and as it grows more compelling and self-evident, it gradually matures into a vision. This is stage 2 of the temporal model for technological visions. Importantly, in this second stage the vision exists beyond the immediate community of actors involved in its development and maintenance (by virtue of its agency). It occupies a discursive plane where different parties are able to make sense of and interact with it. This is the ‘innovation chorus’. The more compelling and powerful the vision becomes, the lesser the control that any single individual or group has over it. It begins to take on a life of its own. For a vision to prosper at this stage, it must expose itself to the varying interpretations and discourses that are inevitable during technological change, and be capable of coping with disagreement from both within and outside the immediate discourse community (more on this in the next section).

During this stage, the core functions of interpretation and legitimation that comprise an ‘organizing vision’ in Swanson and Ramiller’s sense of the term are initiated. This is also the stage when the most intense discursive contests over the meaning and purpose of a new technology take place. Many visions for new technology will dwell in the second stage indefinitely, as their capacity to mobilize and legitimize an innovation weakens or unravels over time, in which case they are incapable of triggering the third function of an organizing vision. The barrier separating this stage and the next marks a threshold through which a vision passes into the mobilization stage of innovation.

In this third stage, mobilization occurs. Importantly, these activities require more than simply discursive work. Mobilization necessarily entails material effort, which goes beyond discourse. However, the primarily discursive functions of interpretation and legitimation continue into this stage, serving to explain and justify the technology to those involved in the mobilization project.

Importantly, although this model depicts visioning in a linear fashion, it accepts that a vision may regress at any stage during the innovation process, in which case it may devolve back to an idea, belief, or hope. The model also accounts for the role of counter-discourses that emanate from outside the immediate discourse community, which were evident in the case study. I focus on these communities and their discourses in the next section.

## Resistance

Finally, the role of context remains under-theorized in Swanson and Ramiller's treatment of visions. Specifically, they do not explore in depth how visions compete and encounter resistance, particularly outside of the community interested in innovating. While these external communities may not be particularly important in the context of IT innovation in business corporations, where the majority of IS research takes place, in our case study they played a significant role in derailing the government's proposals. Similar dynamics are likely to arise in other government-sponsored or public sector-led innovation projects, especially those involving controversial science or technology (such surveillance systems), as was the case in this study. We must therefore attempt to theorize these observations for future research.

For Swanson and Ramiller, the "discourse community consists of a variety of participants, united in their commitment to the innovation's public interpretation, but differentiated by the interests that motivate them and the roles they play in the marketplace" (1997, p. 464). Theirs is thus a generally positive and inclusive notion of community, whereby conflict is understood in terms of market competition or standards development, as opposed to other forms of social or political discord. This notion of conflict only accommodates inter-community disagreement over a vision's content or meaning, and excludes more extreme forms of resistance that may arise from other domains, such as those outside the main discourse community. In the case of the National Identity Scheme, the technologies of biometrics were the subject of outright hostility by certain members of the political opposition and civil society, for whom, right or wrong, the technologies were entirely unacceptable. These actors are captured in Figure 8.2, in which a community (or communities) generates and communicates its own counter-discourses on a new technology.

Despite Swanson and Ramiller's suggestion, the discourse community surrounding many new IT innovations is not always open and equal. Some agents are not permitted access to the official venues and formal arenas in which meaning making around proposals for a new technology takes place. For example, many important actors in the case of the National Identity Scheme were not part of the policy and technology communities in which decisions were made about biometrics, but their discourses and activities were nonetheless significant to the project's outcome. In particular, despite being officially banned from some public meetings on the NIS, No2ID's sustained resistance to the government's ID cards program, including the resistant discourses communicated not just to the public, but also Members of

Parliament and even business actors, were effective in debilitating the Scheme. Despite not being privy to official discourse channels, these actors were still heard. And their messaging was effective.

Another previously unaccounted for community that arose in our case study includes those actors without a voice during an innovation project, such as the foreign nationals the government targeted for biometric enrollment. They were especially disempowered – forced to participate in the government's biometrics program and unable to meaningfully dissent or resist, without being denied entry and leave to remain in the UK. Actors such as these are altogether missing from Swanson and Ramiller's account of technological change, arguably due to the scope of the organizations that they were most interested in. But, as I have argued, we cannot ignore non-business organizational contexts as we devise theories to understand innovation, discourse, and resistance. While these often-silent actors may not directly affect a technology's trajectory during innovation processes, they are no doubt affected by its outcome (cf. Darking and Whitley 2007 on the 'absent other').

Based on the findings from the case study, this section has expanded on organizing visions theory to explore the constitution of visions, what distinguishes them from mere ideas about new technology, and their temporality. It has also re-theorized the context of organizing visions to account for two additional communities involved in certain types of innovation: counter-discourse communities and the voiceless publics of new technology. Moving beyond considering IS theory on visions and technology, I now turn to further explore the concept of the publics of innovation from the critical public understanding of science perspective.

## 8.5 Discourse, publics, and technological innovation

Much like the talk about *technology*, discourses about the *public* and their *understanding* and *acceptance* of biometrics persisted throughout the case analysis. Taken literally and uncritically, these discourses are simply descriptions of public opinion and the eventual users of a new technology. However, these discourses can also be seen as simultaneously constructing the future users of a system. More than merely describing matters of fact, such talk about the public and its relationship to a new technology also serves to generate expectations and shape attitudes. In other words, these discourses are *performative* (Borup et al. 2006; Horst 2007).

This section reflects critically on discourses about the public and its relationship to biometrics. The discussion first reviews the previously analyzed discourses about public understandings and acceptance of biometrics, then the discourses on future users themselves, before shifting to a more general reflection on discourses about new technology and their capacity to construct publics.

## Acceptance misunderstood?

Recall from the analysis how the government's discourses on biometrics portrayed an *unaware* yet *accepting* public. The public were said not to fully understand biometrics ("the term was rarely known"), though surveys repeatedly showed, and government spokespeople often reiterated, that members of the public generally 'approved' of their use within the NIS. Indeed, public acceptance of biometrics was said to remain high over the course of the Scheme despite various 'misunderstandings'.

This correlation between poor understandings and high acceptance rates is interesting, if not odd. The commonly held sentiment within traditional research on public understanding of science (PUS) is that 'undeveloped' understandings of new science and technology are a barrier to the public's acceptance of the innovation – that knowledge deficiencies breed bad attitudes (Bauer et al. 2007) – however this case reveals something different. This can arguably be attributed to the concept of 'biometrics' itself, which as we have discussed, is alien and ambiguous. Specific awareness of fingerprinting technologies, for example, would almost certainly have been much greater – with associations with criminality to be expected in many contexts – than would the intricacies of iris photography. But it also has to do with the way in which the Scheme came about: as a government-mandated program for biometric national identity cards. In this context, acceptance takes on a very different meaning and so the PUS knowledge-approval dynamic proves especially complicated.

Of course, perception studies on the NIS were loaded with assumptions about the technologies involved and their 'certainty'. The science and technology were taken as steady and settled, as were their future applications within the Scheme. Certain studies of public perception claimed that people did not understand the simple 'facts' of biometrics. For example, people "tended to find it difficult to grasp that biometrics would only need to be provided once" (Cragg Ross Dawson 2004c, p.74), noted one study. In actuality, such 'facts' and others are provisional and still unsettled, with research ongoing to try to better understand these complexities (see, for example, Bowyer et al. 2009 concerning the disputable permanence of iris biometrics). What is interesting is how government discourses on public understandings of biometrics glossed over and simplified much of this scientific uncertainty and technological complexity.

Moreover, there was a subtle politics to the survey methods used to measure such understandings and perceptions. For example, the government's own longitudinal ‘Tracking Research’ (conducted by the COI) was serially inconsistent. Whereas the first and second surveys posed an open-ended (if not problematic) question regarding the public's ‘awareness and understanding’ of biometrics – “What do you think ‘biometric information’ is?” – , the third survey asked a different question, also open-ended, about where people would be most ‘comfortable’ recording a particular biometric: “Where would you feel comfortable having your fingerprints recorded?” In the fourth survey respondents were asked a ‘yes/no’ question about whether they would be “happy” to have their fingerprints recorded (64% said ‘yes’), followed by a question asking them to choose from a set list of places where they would prefer to enroll their biometrics: “In which of the following locations would you consider having your fingerprints, photo, and signature recorded?” The fifth survey again posed a slightly different question: “Respondents were asked to choose from a list where they would *not* consider having their fingerprints, photo, and signature recorded”. The sixth, seventh, and eighth surveys avoided specific questions about biometrics altogether. At the very least these shifting goalposts make longitudinal tracking very difficult. It is notable that other questions from these tracking surveys were not subject to such regular changes. The questions on biometrics moved from exploring general understandings and interpretations, to asking whether respondents would be “happy” having their fingerprints taken, to not asking about them at all. Considering these frequent changes, it is not clear what was being tracked. A skeptical interpretation of these reformulations might conclude that they were not accidental but rather carefully framed such that the Home Office could find evidence to justify its ongoing policy changes.

Elsewhere, the Home Office argued that public understandings would improve as people began to record their biometrics: “Surveys have shown that people who have experienced the process find it convenient *and understand the benefits* of having the information recorded” (2005c, emphasis added). This formulation represents a strange and twisted logic whereby members of the public are sold on the merits of an innovation after having been mandated to use it. As mentioned, the Home Office’s acceptance contortionism upsets the traditional thinking about the relationship between knowledge and acceptance of new science and technology. Where it is commonly believed that better knowledge facilitates greater acceptance, the logic evidenced in this quotation from the Home Office implies that knowledge improves after adoption. This resembles a form of ‘understanding by doing’ and, importantly, ignores a raft of ethical and privacy concerns related to informing data subjects *before* their data are collected and processed.

## Politico-understandings of biometrics

The analysis also shed light on the extent of political decision-makers' knowledge of biometrics. These are another important public in this case study, though as a group they are often neglected by PUS studies – most probably for methodological reasons. What is not entirely clear is the extent of parliamentarians' actual 'understanding' of biometrics. Their discourses often revealed misunderstandings and confusion about the technology behind biometrics, but we must be careful not to equate discourse with understanding or belief. In politics, it is often hard to distinguish between the willfully ignorant and the naturally ignorant. For all we know, MPs knew more than they let on. As we saw, calculated misrepresentations of certain aspects of biometrics in policy documents and prepared speeches were common, such as when officials spoke of 'international obligations' for biometrics. It is very plausible that these were discursive strategies rather than knowledge gaps. However, there were also moments, particularly during parliamentary debates, when MPs (especially those on the backbench) did indeed seem puzzled or poorly briefed on the issues, such as when they posed odd and seemingly misplaced questions about the use of DNA information in identity cards, or when statements about the state of iris biometrics did not reflect current thinking in the Home Office.

It is nearly certain that there were experts within the Home Office who did understand the science and practice of biometrics well. However, I did not have direct access to these individuals – just their organizational knowledge as transmitted through carefully sanitized discourses in official policy texts. There is therefore an outstanding empirical question regarding the communication and reporting channels that exist between an organization such as the Home Office and those politicians responsible for making policy decisions and communicating policy changes to the public. It appears that the Home Office was not entirely forthcoming in its communications about changes to plans for biometrics. For example, the Home Office took several months, if not an entire year, before finally clarifying the role of iris biometrics, with both frontbench and backbench MPs appearing not to know the actual status of the technology in the Scheme. There are important implications for such uneven and inconsistent knowledge sharing and policy communication practices between those organizations responsible for system implementation (e.g., the Home Office) and oversight bodies (e.g., Parliament). These dynamics grow even more complicated as third parties – such as IT contractors – enter the picture. This topic demands further research and may require creative and opportunistic research approaches and methodologies.

## Technologically-rendered publics

Finally, I want to return to the issue of how discourses on new technology render different types of public. We first looked at these issues in chapter 6, in the context of biometrics. We discovered a recurring discursive distinction between those who were said to be capable of using biometrics  – what the Home Office termed the ‘able-bodied’ – and those who are not – what I called the ‘biometrically-challenged’. The major take-away from that phase of the analysis was that every innovation necessarily engenders a sub-population of users who are said to face problems with the technology. In the case of biometrics, this included a range of people that presented various challenges, including physiological ones (e.g., those with worn down fingers or people suffering from Parkinson’s disease, for whom holding still for an iris scan is difficult) or “life-style-related” ones (e.g., members of certain religions, homeless people, and transsexuals). In the case study, officials aimed to accommodate these users by pursuing specialist systems during the procurement phase. The idea was that these technology-induced ‘anomalies’ also had a techno-fix.

However, the fate of the Scheme (with it ending the way it did, before any major roll-out of biometrics except for certain categories of non-EEA foreign nationals and refugees) meant that these pre-emptive measures were never tested. It remains to be seen whether the discrimination that is said to be inherent in the use of biometrics can be resolved with better technology, capable of reading and recording an unknown number of ‘non-standard’ or ‘non-compliant’ bodies. Until biometrics are actually employed on a national scale, we will not know the extent of their discriminatory effects, whether feasible remedies will emerge to mediate biometrics-related discrimination, how technology will contribute to those remedies, and what discursive dynamics will organize and maintain the sub-system for the biometrically-challenged. Similar proposals for biometric national identity systems in Mexico and India provide another test bed for these technologies and their attendant discourses.

## 8.6 Reflections on the research approach

Following the literature review in chapter 2 I called for an approach to studying new technology such as biometrics that avoids three different traps. A first trap that often catches technical studies involves ignoring the raft of political, social, organizational, and ethical aspects of introducing new technologies. In most technical studies, these issues are intentionally scoped out of research models and excluded from the questions that researchers pose. The focus is on technological improvement rather than concerns such as the motivations of the actors and organizations involved in deploying a new system or the ethics of building exceedingly accurate technologies to identify, profile, monitor, and track people. These oversights, I argued, ought to be addressed by my approach.

A second trap catches many sociological treatments of biometrics, which lump together a wide range of different biometric methods and technologies in their broad critiques of the *potential* discriminatory or ethical consequences of the technology. The problem with such generalizations is that crucial differences in the technical artifacts are overlooked or ignored – differences that matter to the claims made by social scientists. By black-boxing technology in this way, important insights and nuances are missed. My approach, therefore, aimed to take technology 'seriously' by being attentive to the technical specifics of the government's proposals.

A third trap afflicts IS research, which to date has been predominated by studies of user acceptance of biometrics. I argued that, beyond being normatively loaded, acceptance research is also misplaced in contexts such as the case of the National Identity Scheme. This is because it was not clear *who* was accepting the technology (politicians who voted to include them in the legislation, organizations that were expected to adopt them, citizens who were expected to use them, those foreign nationals who could not *not* accept, etc.) and *what* exactly they were accepting (i.e., there were no technical devices in place throughout the majority of the Scheme's lifespan). I therefore proposed that the research instead focus on the discourses on biometrics attending public discussions and debates over the NIS, and in particular how these discourses were *framed* and the *changes* they underwent over time.

This tailored approach allowed us to focus more carefully on the technologies, actors, and institutions involved in the proposals for the National Identity Scheme and to appreciate how loosely aligned spokespeople attempted to form and propagate a vision for biometrics. It permitted us to explore the dynamics of this fragile vision – how it attempted to portray a plan for nationwide implementation of biometrics and how this vision unraveled as critical events transpired and an election neared. The critical discourse analysis was especially sensitive to changes in the government's framing of its proposals, particularly as the vision encountered resistance and unforeseen dilemmas. Motivated by debates from research on the public's understanding of science, the research lens also highlighted how discourses on new technology render an array of publics. I suggest that this research model can be appropriated for future studies involving visionary technology projects that implicate various organizations, stakeholder groups, and users.

## 8.7 Limitations of the study

There are inescapable limitations to any research project, and this study is no different. While I believe the story I have told has provided important insights into the early life (and eventual demise) of proposals for an innovative, undoubtedly politics-laded government information technology, the arguments and findings presented here are naturally limited.

Perhaps most obvious is that I only studied discourses around a new technology prior to its implementation, without observing and comparing the subsequent discourses following its introduction. Even if the biometrics component of the NIS had been developed as planned, the original research schedule for this dissertation would have precluded access to government, media, and public discourses about the fully operational Scheme. Suffice it to say I acknowledge the implications of my 'time capsule' approach, devoid as it is of extensive post-implementation data.

This thesis focused its analysis on publicly available discourses, as one must surely do with such a topical matter of public security provision where classification and industrial secrecy loom large. I would have liked to get inside the organizations responsible for delivering the NIS in order to access those individuals responsible for overseeing its creation, design, and implementation. These include civil servants in the Home Office and IPS, who I believe would have provided another interesting source of data. However, this was not possible for various reasons, the most obvious of which is the sensitivity of the project and institutional concerns about protecting what was said to be ‘commercially confidential’ and ‘security sensitive’ information regarding the program. Unfortunately, my attempts to approach these organizations to engage their members through interviews and other methods were fruitless.

Likewise, I was also interested in systematically studying the supply side (i.e., vendors) of biometrics in the Scheme, much like Pollock and Williams (2008) have done with enterprise resource planning systems, but my access to these venues was similarly limited. I was able to attend biometrics industry conferences on a regular basis to get an informal feel for the discourses at work in these arenas and speak with players in the biometrics industry who sought contracts on the government’s identity cards program. These were fascinating venues in which the business of expectations is bustling, though I must admit that it is difficult to convince people to talk on the record in these venues. In future I hope to study more systematically the role that these gatherings play in IT innovation dynamics (cf. Pollock & Williams 2010).

Finally, this research project was a single case study, supplemented at times by informed observations from other, related cases. Under more liberal research parameters than those afforded to doctoral students, I would have undertaken a comparative case study of national biometric identity programs, to generate, as Pollock and Williams (2010) argue, a more complete biography of technology. Pollock and Williams encourage researchers to trace and compare the careers of numerous systems, rather than simply studying a single site. Notwithstanding the constraints of graduate study, the two other national programs for biometrics (namely, Mexico and India, which both aim to enroll multiple biometrics (including irises)) have just recently launched, and so the timing for a comparative study would have been somewhat awkward. However, a biography of large-scale biometrics programs may be assembled in future.

## 8.8 Future research

While I have alluded to different aspects of resistance that emerged in the case study, in future I wish to expand on these initial observations to provide a fuller account of the resistance dynamics at play in the case. In particular, the role of politics in ending the Labour government's plans for biometric identity cards (and the accompanying database) merits a focused and extended analysis of its own. This future research would be based on initial research that colleagues and I have already conducted relating to the actors and modes of resistance at play in the Scheme (Martin et al. 2009), which would need to incorporate a stronger understanding of the reasons for resistance.

There are several similar large-scale projects underway in different countries with body surveillance technologies and identification systems at their core. Future research may apply my revised theoretical model and research approach to these implementations to better understand the public discourse framing processes that underlie sponsor actors' visions for these technologies, how these discourses cope with and overcome counter-discourses, and the role that the public plays in the discourses on technological innovation.

For instance, the introduction of 'advanced imaging technologies' (abbreviated as AITs and known colloquially as full-body scanners) in airports worldwide offers an interesting case. These scanners are able to peer beneath clothing and generate what have been described as extremely intimate and revealing images of the subject's body, including the genitalia region (see Appendix 8).

Resistance to the scanners is mounting, sparked by concerns about its intrusiveness, indignity, and potential radiation hazards, as well as concerns about their use on certain populations such as children (and whether this might violate child pornography laws in some jurisdictions (Travis 2010)).

Unlike the case of biometrics in the NIS, which went through years of public consultation and deliberation before eventually dissolving by the currents of political change, the proposals for the use of AITs in US airports were put forth and implemented immediately following a thwarted terrorist attack on Christmas Day 2009, thereby short-circuiting public debate about their use. By December 2010 they had been introduced in over 70 airports in the US. It has been disclosed that the American public was not informed in advance about the details of the scanners' roll-out due to concerns that doing so might provide a "roadmap or blueprint for terrorists" (Pistole as quoted in Pugh 2010). The Transportation Safety Administration (TSA) has stated that its policy was to implement the scanners first, and then try to "educate" the public about their benefits (Pugh 2010).

However as was the case in the NIS, these 'benefits' are as yet unknown, and presently unknowable. It is unclear how effective body scanners are at detecting dangerous material concealed below the clothing of the subject (DHS Office of Inspector General 2010; Strickler 2010). There are also unanswered questions about the health risks posed by radiation exposure and little consideration given to the effects of repeated exposure of the kind frequent travelers would undergo (Cox 2010). One particular technology-related controversy concerns whether the systems are capable of storing and saving the images, which some say would make them more privacy-invasive. Officials from the US Department of Homeland Security (DHS) originally claimed that the systems are designed so that images cannot be saved locally and that all images are automatically deleted immediately after analysis. However, a Freedom of Information request by the Electronic Privacy Information Center (an advocacy group) revealed that the functionality to save images of scans does indeed exist.

There are two sets of concerns related to the 'publics' of innovation, in particular, that future research could explore. First is a familiar methodological politics in the surveys being conducted concerning these systems, which are said to provide an unbiased scientific measure of public attitudes towards the technology. In its public relations efforts to respond to the outcry over the claimed invasiveness and inappropriateness of body scanners, the TSA has stressed that the public overwhelmingly approves of the use of AITs. One of the surveys was conducted just weeks following the failed Christmas Day bombing, and before any major roll-out of the technology. The poll found that 78% of respondents said they approved of scanners, with 84% believing that the technologies would help to prevent terrorists from bringing explosives on board. The (then) acting administrator of the TSA, Gale Rossides, interpreted these poll results as "demonstrat[ing] public understanding" of the need to use the scanners (as quoted in Frank 2010). Such ‘understanding’ had been arrived at before the technology was in widespread use, before any conclusive, independent testing or analysis had been carried out to determine the systems’ effectiveness in preventing dangerous objects from being snuck onto airplanes, and in the absence of any substantial public knowledge base about the social or ethical benefits and drawbacks of full-body scans.

If we are to believe the poll results, which are strikingly similar to those about biometrics in the lead up to the roll-out of the NIS, then they represent general public acceptance of an innovation about which public knowledge and experience is limited and zero, respectively. However, if we critically question these discourses on acceptance, other explanations may arise. Future research could study these poll results through the lens of the sociology of expectations, which encourages us to view such statements as a means to condition future expectations about technology. Theorizing discourses on public acceptance in this way resonates with Law’s remarks on method: “Method is not, I have argued, a more or less successful set of procedures for reporting on a given reality. Rather it is performative. It helps to produce realities” (Law 2004, p.143). It also draws our attention to the ‘reactivity’ of public measures such as opinion polls, and the extent to which they create social worlds; that is, whether they are self-fulfilling prophecies or commensurating mechanisms (Sauder & Espeland 2007). That is not to say that these discourses on public opinion deterministically produce the publics they seek to represent, but rather that future research should analyze the extent of their agency.

A second issue for future research concerns how the use of these technologies is turning certain members of the ‘travelling public’ into problem subjects; that is, how they discursively engender standard and non-standard, or compliant and non-compliant, users. Whereas in the case study biometrics were never given a chance to speak for themselves as a practical reality of daily life (despite the discourses that tried to address these concerns), body scanners are now in relatively widespread use in airports in the US and abroad. Certain religious leaders have raised concerns about the use of AITs, including Muslim leaders, some of whom have endorsed a fatwa against the technology (Stanglin 2010), and even the Pope, who spoke on the topic of body scanners to an audience of aerospace industry representatives, stating that “the primary asset to be safeguarded and treasured is the person, in his or her integrity” (Hooper 2010). Such warnings, combined with other concerns such as the perceived health risks or usability issues (such as for menstruating women wearing thick panty liners that obstruct the scanner’s view of certain parts of the body (GladRags 2010), or for those who wear medical devices which appear suspicious during scans), have resulted in a situation in which many people are opting for what are termed ‘enhanced’ pat-downs by security officers. These secondary measures unevenly affect certain types of travelers (Cate 2010).

Security agents who perform this work form another technological public. While they are the ones often facing ridicule from upset travelers, they are not responsible for the policy decisions mandating the procedures. Many of them say they do not enjoy such humiliating, degrading, and demoralizing work (Masnick 2010). As such, they may prove to be a very important point of resistance whereby the surveillance mission set by policy-makers is not enforced or is altered to accommodate shared notions of right and wrong (cf. Gilliom 2001 on similar dynamics in the US related to welfare surveillance).

A grassroots movement of emergent privacy activists has attracted sustained public attention to these incidents in recent months, forming their own counter-discourses against the technology. So a sustained controversy is likely to continue as the TSA adapts, modifies its processes, learns from its experiences as an organization, and begins to accommodate the multiplicity of bodies it encounters. As the controversy unfolds, it offers many exciting avenues for research.

And finally, a much more critical analysis of the discourses of ‘innovation’ that persisted in this case study is desperately needed. By and large, this thesis has accepted that the biometrics proposed in the case where somehow new and innovative, based on the scale of the proposals and the technologies considered therein. However, as Pollock and Williams (2008) point out, the rhetorics of technology supply serve to delete certain past experiences which might otherwise show us how the innovation we often take for granted is, in fact, not so new or groundbreaking as first assumed. These discourses aim to reassure us that a new solution overcomes the shortcomings of its predecessors (p. 55), yet at the same time they rely on the old to generate meanings about the new. Future research on these discursive dynamics of innovation is urgently needed, to build on the critical studies of innovation by Suchman and others (see Suchman & Bishop 2000).

Page intentionally left blank

# Bibliography

2006. *Identity Cards Act 2006*, Available at: http://www.opsi.gov.uk/acts/acts2006/ukpga_20060015_en_1.

2005. *Identity Cards Bill [as amended in Committee]*, Available at: http://personal.lse.ac.uk/martinak/Bill_as_amended_in_Committee.pdf.

2007. *UK Borders Act 2007*, Available at: http://www.statewatch.org/news/2007/nov/uk-borders-act-2007.pdf.

Adler, A., 2003. Can images be regenerated from biometric templates? In *Proceedings of the Biometrics Consortium Conference*. Arlington, VA.

Agar, J., 2005. Identity cards in Britain: past experience and policy implications. *History and Policy*. Available at: http://www.historyandpolicy.org/papers/policy-paper-33.html.

Agarwal, R. & Lucas, H.C., 2005. The Information Systems Identity Crisis: Focusing on High-Visibility and High-Impact Research. *MIS Quarterly*, 29(3), 381-398.

Alterman, A., 2003. "A piece of yourself": Ethical issues in biometric identification. *Ethics and Information Technology*, 5(3), 139-150.

Amoore, L., 2006. Biometric borders: Governing mobilities in the war on terror. *Political Geography*, 25(3), 336-351.

Anderson, N., 2008. IP addresses could become "personal information" in Europe. *Ars Technica*. Available at: http://arstechnica.com/old/content/2008/01/ip-addresses-could-become-personal-information-in-europe.ars [Accessed October 29, 2010].

Anderson, R. et al., 2009. *Database State*, Joseph Rowntree Reform Trust. Available at: http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf.

Anderson, R. et al., 2007. Biometrics are not a panacea for data loss: Letter to the Joint Committee on Human Rights, 26/11/2007. Available at: http://doooooooom.blogspot.com/2007/11/biometrics-are-not-panacea-for-data.html.

Anonymous, 2007a. In the Face of Danger: Facial Recognition and the Limits of Privacy Law. *Harvard Law Review*, 120, 1870-1891.

Anonymous, 2007b. Iris scan 'optional'. *The Times*. Available at: http://www.timesonline.co.uk/tol/news/uk/article1295209.ece.

Anonymous, 2008. Britain can't afford ID cards. *The Daily Telegraph*. Available at: http://www.telegraph.co.uk/comment/telegraph-view/3563758/Britain-cant-afford-ID-cards.html [Accessed November 4, 2010].

Anonymous, 2009. Major city votes against ID cards. *Public Service*. Available at: http://www.publicservice.co.uk/news_story.asp?id=11598 [Accessed October 30, 2010].

Atos Origin, 2005. *UK Passport Service Biometrics Enrollment Trial Report*, Home Office.

Ball, K., 2005. Organization, Surveillance and the Body: Towards a Politics of Resistance. *Organization*, 12(1), 89-108.

Ball, K. et al., 2006. *A Report on the Surveillance Society*, Information

Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

Bauer, M.W., 2000. "Science in the Media" as a Cultural Indicator: Contextualizing Surveys with Media Analysis. In M. Dierkes & C. von Grote, eds. *Between Understanding and Trust: The Public, Science and Technology*. Amsterdam: Harwood Academic, pp. 157-178.

Bauer, M.W., 2002. Arenas, Platforms, and the Biotechnology Movement. *Science Communication*, 24(2), 144-161.

Bauer, M.W., 2009. The Evolution of Public Understanding of Science—Discourse and Comparative Evidence. *Science Technology & Society*, 14(2), 221-240.

Bauer, M.W., Allum, N. & Miller, S., 2007. What can we learn from 25 years of PUS survey research? Liberating and expanding the agenda. *Public Understanding of Science*, 16(1), 79-95.

Bauer, M.W. & Gaskell, G., 2000. Towards Public Accountability: beyond sampling, reliability and validity. In M. W. Bauer & G. Gaskell, eds. Qualitative researching with text, image and sound: a practical handbook. London: Sage, pp. 336-350.

Bayley, P., 2004. *Cross-cultural perspectives on parliamentary discourse*, Amsterdam: John Benjamins Publishing Company.

BBC News, 2007. ID cards will give 'false' data. *BBC*. Available at: http://news.bbc.co.uk/1/hi/programmes/file_on_4/6922882.stm [Accessed November 5, 2010].

BBC News, 2008. Technical glitches hit T5 opening. *BBC*. Available at:

http://news.bbc.co.uk/1/hi/uk/7314816.stm [Accessed July 18, 2010].

BBC News, 2010. Row over gamers' true identities. *BBC*. Available at: http://www.bbc.co.uk/news/10543100 [Accessed December 1, 2010].

Benbasat, I., Goldstein, D.K. & Mead, M., 1987. The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, 11(3), 369-386.

Benbasat, I. & Zmud, R.W., 2003. The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties. *MIS Quarterly*, 27(2), 183-194.

Benford, R.D., 1997. An insider's critique of the social movement framing perspective. *Sociological Inquiry,* 67, 409-430.

Benford, R.D. & Snow, D.A., 2000. Framing Processes and Social Movements: An Overview and Assessment. *Annual Review of Sociology*, 26(1), 611-639.

BIA, 2008. *Introducing Compulsory Identity Cards for Foreign Nationals*, Home Office. Available at: http://www.statewatch.org/news/2008/mar/uk-compulsory-id-for-foreign-nationals.pdf.

Bieber, F.R., Brenner, C.H. & Lazer, D., 2006. Human Genetics: Finding Criminals Through DNA of Their Relatives. *Science*, 312(5778), 1315-1316.

Bijker, W.E., 2003. The Need for Public Intellectuals: A Space for STS: Pre-Presidential Address, Annual Meeting 2001, Cambridge, MA. *Science, Technology, & Human Values*, 28(4), 443-450.

Blunkett, D., 2004. Identity Cards Speech. Available at:

http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/docs3/identitycards_041118speech.htm.

Blunkett, D., 2007. ID not the issue... our attitude is. *The Sun*. Available at: http://www.thesun.co.uk/sol/homepage/news/article492939.ece.

Blunkett, D. et al., 2004. *Identity Cards: Home Office PLP Briefing*, Home Office.

Boland, R.J., Boland, R.J. & Hirschheim, R., 1987. The in-formation of information systems. In *Critical issues in information systems research*. Chichester: John Wiley & Sons, Inc., pp. 363-394.

Bolle, R.M., Connell, J.H. & Ratha, N.K., 2002. Biometric perils and patches. *Pattern Recognition*, 35(12), 2727-2738.

Borup, M. et al., 2006. The sociology of expectations in science and technology. *Technology analysis and strategic management*, 18(3/4), 285-298.

Bowyer, K.W., 2004. Face Recognition Technology: Security versus Privacy. *IEEE Technology and Society Magazine*, 23(1), 9-20.

Bowyer, K.W., Hollingsworth, K. & Flynn, P.J., 2008. Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding*, 110(2), 281-307.

Bowyer, K.W. et al., 2009. Factors that degrade the match distribution in iris biometrics. *Identity in the Information Society*, 2(3), 327-343.

Bridgman, T., 2007. Reconstituting Relevance. *Management Learning*, 38(4), 425 -439.

Brooke, C., 2002. What does it mean to be 'critical' in IS research? *Journal of Information Technology*, 17(2), 49-57.

Brown, N. & Michael, M., 2003. A sociology of expectations: Retrospecting prospects and prospecting retrospects. *Technology analysis and strategic management*, 15(1), 3-18.

Buchanan, K., 2007. DNA 'will be stolen' from ID cards. Available at: http://personal.lse.ac.uk/martinak/DNA.pdf.

Buckland, M.K., 1991. Information as thing. *Journal of the American Society for Information Science*, 42(5), 351-360.

Burge, M. & Burger, W., 2000. Ear Biometrics in Computer Vision. In *International Conference on Pattern Recognition*. Los Alamitos, CA, USA: IEEE Computer Society, pp. 822-826.

Burnham, A., 2005a. 'Identity Cards - Economy, Efficiency, Effectiveness' speech at the Cityforum Roundtable.

Burnham, A., 2005b. Letter from Andy Burnham to Professor Ian Angell. Available at: http://ips.gov.uk/identity/downloads/letter-to-burnham.pdf.

Burnham, A., 2006. Letter to MPs regarding the Identity Cards Bill.

Byrne, L., 2007. Securing Our Identity: A 21st Century Public Good. Available at: http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/225.htm.

Cabinet Office, 2002. *Identity Fraud: A Study*, Cabinet Office. Available at: http://www.statewatch.org/news/2004/may/id-fraud-report.pdf.

Cabinet Office, 2006a. *Identity Risk Management for e-Government Services*, Cabinet Office.

Cabinet Office, 2006b. *Transformational Government Implementation Plan*, Cabinet Office. Available at: http://webarchive.nationalarchives.gov.uk/20060802153712/http://cio.gov.uk/documents/pdf/transgov/transgovt.pdf.

Callon, M., 1986. Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In *Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay*. London: Routledge, pp. 196-223.

Cate, F., 2010. Letter to Chairman Rockefeller and Ranking Minority Member Hutchison regarding the TSA's new full-body pat-down policy. Available at: http://cacr.iu.edu/sites/cacr.iu.edu/files/TSA-Policy.pdf.

Central Office of Information, 2004. *Identity Cards 2004*, Home Office.

Central Office of Information, 2007a. *National Identity Scheme Tracking Research Wave 1: February 2007*, Identity & Passport Service.

Central Office of Information, 2007b. *National Identity Scheme Tracking Research Wave 2: October 2007*, Identity & Passport Service.

Chau, A., Stephens, G. & Jamieson, R., 2004. Biometrics Acceptance - Perceptions of Use of Biometrics. In *Proceedings of the 15th Australasian Conference on Information Systems*. Hobart, Tasmania, Australia, pp. 1-6.

Clarke, N.L. et al., 2002. Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices. *Computers & Security*, 21(3), 220-228.

Clarke, R., 1994a. Human Identification in Information Systems: Management

Challenges and Public Policy Issues. *Information Technology & People*, 7(4), 6-37.

Clarke, R., 1994b. The digital persona and its application to data surveillance. *The Information Society: An International Journal*, 10(2), 77-92.

Clarke, R.A., 2001. Biometrics and Privacy. Available at: http://www.rogerclarke.com/DV/Biometrics.html.

Cole, S.A. & Dioso-Villa, R., 2009. Investigating the 'CSI Effect' Effect: Media and Litigation Crisis in Criminal Law. *Stanford Law Review*, 61(6), 1335-1374.

Cole, S.A., 2009. Forensics without uniqueness, conclusions without individualization: the new epistemology of forensic identification. *Law Probability and Risk*, 8(3), 233-255.

Collingridge, D., 1992. *The management of scale: big organizations, big decisions, big mistakes*, London: Routledge.

Corbin, J.M. & Strauss, A.L., 2008. *Basics of qualitative research: techniques and procedures for developing grounded theory*, London: Sage.

Council of the City of Sheffield, 2009. Sheffield council's motion to oppose ID cards. Available at: http://www.no2id-sheffield.net/index.php/Local_Issues:Council_motion.

Cox, L., 2010. Are Security Scanners Safe? *Technology Review*. Available at: http://www.technologyreview.com/printer_friendly_article.aspx?id=26774 [Accessed November 24, 2010].

Cragg Ross Dawson, 2004a. *Identity cards - People with special issues: Response to the proposed customer experience report*, Home Office.

Cragg Ross Dawson, 2004b. *Identity cards: The public's response to proposed customer propositions*, Home Office.

Cragg Ross Dawson, 2004c. *Public perceptions of identity cards: Qualitative Research Report*, Home Office. Available at: http://www.craggrossdawson.co.uk/pdf/CRD_ID_Perceptions2.pdf.

Crosby, J., 2008. *Challenges and opportunities in identity assurance*, London: HM Treasury.

Darking, M. & Whitley, E.A., 2007. Towards an Understanding of FLOSS: Infrastructures, Materiality and the Digital Business Ecosystem. *Science Studies*, 20(2).

Davidson, E., 2006. A technological frames perspective on information technology and organizational change. *Journal of Applied Behavioral Science*, 42(1), 23–39.

Davies, S., 1998. Biometrics - A Civil Liberties and Privacy Perspective. *Information Security Technical Report*, 3(1), 90-94.

Davis, C.J. & Hufnagel, E.M., 2007. Through the Eyes of Experts: A Socio-Cognitive Perspective on the Automation of Fingerprint Work. *Management Information Systems Quarterly*, 31, 681-704.

Davis, F.D., 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319-340.

Deane, F. et al., 1995. Perceived acceptability of biometric security systems. *Computers and Security*, 14(3), 225-231.

DHS, 2006. *The Use of RFID for Human Identification: A Draft Report from*

*DHS Emerging Application and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee (Version 1.0)*, US Department of Homeland Security.

DHS Office of Inspector General, 2010. *Evaluation of Newly Deployed and Enhanced Technology and Practices at the Passenger Screening Checkpoint (Unclassified Summary)*, Department of Homeland Security.

Dierkes, M., Hoffmann, U. & Marz, L., 1996. *Vision of technology: social and institutional factors shaping the development of new technologies*, New York: St. Martin's Press.

Eaglesham, J., 2007. ID card contracts on offer. *Financial Times*. Available at: http://www.ft.com/cms/s/0/cca41da2-46aa-11dc-a3be-0000779fd2ac.html.

Einsiedel, E.F., 2001. Citizen voices: public participation on biotechnology. *Politeia*, 17(63), 94-104.

Epstein, C., 2007. Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders. *International Political Sociology*, 1(2), 149-164.

Escudero-Pascual, A. & Hosein, I., 2004. Questioning lawful access to traffic data. *Communications of the ACM*, 47(3), 77-82.

Fairclough, N., 1995. *Media Discourse*, London: Hodder Education.

Fairclough, N., 2010. *Critical Discourse Analysis: The Critical Study of Language* 2nd ed., New York: Longman.

Faundez-Zanuy, M., 2004. On the vulnerability of biometric security systems.

*Aerospace and Electronic Systems Magazine, IEEE*, 19(6), 3-8.

Faundez-Zanuy, M., 2005. Privacy issues on biometric systems. *Aerospace and Electronic Systems Magazine, IEEE*, 20(2), 13-15.

Fawcett, J. & Downs, F.S., 1986. *The relationship of theory and research*, Norwalk, Conn.: Appleton-Century-Crofts.

Finn, R. & McCahill, M., 2010. Representing the Surveilled: Media Representation and Political Discourse in Three UK Newspapers. In *PSA Conference Proceedings*. Edinburgh. Available at: http://www.psa.ac.uk/journals/pdf/5/2010/266_348.pdf [Accessed December 4, 2010].

Firth, D., 2001. The Organizing Vision for Customer Relationship Management. In *AMCIS 2001 Proceedings*.

Flick, U., 2008. *Managing Quality in Qualitative Research*, London: Sage.

Ford, R., 2008. First compulsory ID cards to be issued to foreigners, Home Office announces. *Times*. Available at: http://www.timesonline.co.uk/tol/news/politics/article5225907.ece [Accessed November 4, 2010].

Frank, T., 2010. Most OK with TSA full-body scanners. *USA Today*. Available at: http://www.usatoday.com/travel/flights/2010-01-11-security-poll_N.htm [Accessed November 24, 2010].

Furnell, S.M. et al., 2000. Authentication and Supervision: A Survey of User Attitudes. *Computers & Security*, 19(6), 529-539.

Furnell, S.M. & Evangelatos, K., 2007. Public awareness and perceptions of biometrics. *Computer Fraud & Security*, 2007(1), 8-13.

Gamson, W.A. & Modigliani, A., 1989. Media Discourse and Public Opinion on Nuclear Power: A Constructionist Approach. *The American Journal of Sociology*, 95(1), 1-37.

Gaskell, G. & Bauer, M.W., 2001. *Biotechnology 1996-2000: the Years of Controversy*, London: Science Museum.

Gaskell, G. et al., 2005. Imagining nanotechnology: cultural support for technological innovation in Europe and the United States. *Public Understanding of Science*, 14(1), 81-90.

Gates, K.A., 2005. Technologies of Identity and the Identity of Technology: Race and the Social Construction of Biometrics. In C. McGarthy et al., eds. *Race, Identity and Representation in Education*. New York: Routledge, pp. 59-71.

Gates, K.A., 2006. Identifying the 9/11 'faces of terror': The promise and problem of facial recognition technology. *Cultural Studies*, 20(4/5), 417-440.

Gibson, E., 2009. The Dawning of the Biometric Age. *BusinessWeek: Innovation*. Available at: http://www.businessweek.com/innovate/content/may2009/id20090520_625039.htm [Accessed July 18, 2010].

Gilliom, J., 2001. *Overseers of the poor: surveillance, resistance, and the limits of privacy*, Chicago: University of Chicago Press.

Givens, G. et al., 2003. A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces. In *Computer Vision and Pattern Recognition Workshop*. pp. 1-9.

GladRags, 2010. TSA Groin Searches Menstruating Woman. *GladRags Gab*. Available at: http://blog.gladrags.com/2010/11/24/tsa-groin-searches-menstruating-woman/ [Accessed December 31, 2010].

Goffman, E. 1974. *Frame Analysis: An Essay on the Organization of Experience*, New York: Harper & Row.

Goldacre, B., 2007. Ben Goldacre: Now for ID cards - and the biometric blues. *The Guardian*. Available at: http://www.guardian.co.uk/commentisfree/2007/nov/24/idcards.homeaffairs [Accessed November 3, 2010].

Graham, S. & Wood, D., 2003. Digitizing surveillance: categorization, space, inequality. *Critical Social Policy*, 23(75), 227-248.

Greenbaum, J.M. & Kyng, M. eds., 1991. *Design at Work: Cooperative Design of Computer Systems*, Hillsdale, New Jersey: L. Erlbaum Associates.

Gregor, S., 2006. The Nature of Theory in Information Systems. *MIS Quarterly*, 30(3), 611-642.

Gregory, J. & Miller, S., 2000. *Science in Public: Communication, Culture, and Credibility*, Cambridge, MA: Basic Books.

Grother, P.J., Quinn, G.W. & Phillips, P.J., 2010. *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST. Available at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968.

Haggerty, K.D. & Ericson, R.V., 2000. The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622.

Hall, J., 2006. Question the head of ID card scheme. Available at: http://www.pm.gov.uk/output/Page10364.asp.

Heckle, R.R., Patrick, A.S. & Ozok, A., 2007. Perception and acceptance of fingerprint biometric technology. In *Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, Pennsylvania: ACM, pp. 153-154.

Hillier, M., 2008a. 'Passport Validation Service' presentation.

Hillier, M., 2008b. Proposal for a regulation amending Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Document 14217/07). Available at: http://www.parliament.uk/documents/upload/230108HillierGrenBioMetPassdw13.pdf.

Hillier, M., 2010. *Identity Documents Bill*, Available at: http://www.publications.parliament.uk/pa/cm201011/cmpublic/identity/100629/am/100629s01.htm.

Ho, G., Stephens, G. & Jamieson, R., 2003. Biometric Authentication Adoption Issues. In *Proceedings of the 14th Australasian Conference on Information Systems*. Perth, Western Australia.

Home Office, 2002. *Entitlement Cards and Identity Fraud: A Consultation Paper*, Stationery Office. Available at: http://www.privacyinternational.org/documents/idcard/uk/entitlement-card-consultation.pdf [Accessed July 18, 2010].

Home Office, 2003a. *Identity Cards: A Summary of Findings from the Consultation Exercise on Entitlement Cards and Identity Fraud*, Home Office.

Home Office, 2003b. *Identity Cards: The Next Steps*, Home Office.

Home Office, 2004a. *Identity Cards: A Summary of Findings from the Consultation on Legislation on Identity Cards*, Home Office. Available at: http://83.231.230.210/cps/files/ips/live/assets/documents/id-summary-doc-3.pdf.

Home Office, 2004b. *Identity Cards: The Government Reply to the Fourth Report from the Home Affairs Committee, Session 200304 HC 130*, Home Office.

Home Office, 2004c. *Legislation on Identity Cards: A Consultation*, Home Office.

Home Office, 2004d. *Identity Cards Bill Regulatory Impact Assessment*, Home Office.

Home Office, 2005a. *Identity Cards Bill Regulatory Impact Assessment [Update]*, Home Office.

Home Office, 2005b. *Identity Cards Bill: Race Equality Impact Assessment*, Home Office.

Home Office, 2005c. *Identity Cards Briefing*, Home Office.

Home Office, 2005d. *Identity Cards Scheme - Benefits Overview*, Home Office.

Home Office, 2005e. *Identity Cards Trade Off Research (Interim Report)*, Home Office.

Home Office, 2005f. *Identity Cards: An assessment of awareness and demand for the Identity Cards Scheme*, Home Office.

Home Office, 2005g. Procurement Strategy Market Soundings.

Home Office, 2005h. *Response to The London School of Economics' ID Cards Cost Estimates & Alternative Blueprint*, Home Office. Available at: http://identityproject.lse.ac.uk/HomeOffice_ResponseTo_LSE_AlternativeBlueprint.pdf.

Home Office, 2006. *Borders, Immigration and Identity Action Plan: Using the National Identity Scheme to strengthen our borders and enforce compliance within the UK*, Home Office.

Hood, C., 1991. A Public Management for All Seasons? *Public Administration*, 69(1), 3-19.

Hoofnagle, C., 2009. Beyond Google and evil: How policy makers, journalists and consumer should talk differently about Google and privacy. *First Monday*, 14(4). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2326/2156.

Hooper, J., 2010. Pope enters airport body scanners row. *The Guardian*. Available at: http://www.guardian.co.uk/world/2010/feb/21/pope-benedict-naked-scanners-airports [Accessed November 25, 2010].

Horst, M., 2007. Public Expectations of Gene Therapy: Scientific Futures and Their Performative Effects on Scientific Citizenship. *Science, Technology and Human Values*, 32(2), 150-171.

Hosein, I., 2002. A Research Note on Capturing Technology: Toward Moments of Interest. In E. A. Whitley et al., eds. *Global and organizational discourse about information technology*. Proceedings of the IFIP TC8/WG8.2 Working Conference on Global and

Organizational Discourse about Information Technology. London: Kluwer, pp. 133-154.

Hosein, I., 2004. The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. *Information Society*, 20(3), 187-200.

Hosein, I., 2005. Transforming travel and border controls: Checkpoints in the Open Society. *Government Information Quarterly*, 22(4), 594-625.

Hough, A., 2010. Airport biometric scanners 'failing to protect Britain's borders', whistleblower claims. *Daily Telegraph*. Available at: http://www.telegraph.co.uk/travel/travelnews/8090820/Airport-biometric-scanners-failing-to-protect-Britains-borders-whistleblower-claims.html [Accessed October 29, 2010].

House of Commons, 2004. *The Identity Cards Bill: Bill 8 of 2004-05*, House of Commons, Home Affairs Section.

House of Commons, 2005. *The Identity Cards Bill: Bill 9 of 2005-06*, House of Commons, Home Affairs Section.

House of Commons Home Affairs Committee, 2004. *Identity Cards*, House of Commons.

House of Lords Select Committee on the Constitution, 2005. *Identity Cards Bill*, House of Lords. Available at: http://www.publications.parliament.uk/pa/ld200506/ldselect/ldconst/44/44.pdf.

ICO, 2010. The Information Commissioner's response to the Ministry of Justice’s call for evidence on the current data protection legislative framework. Available at: http://www.statewatch.org/news/2010/oct/uk-ico-response-eu-dp-review.pdf [Accessed October 25, 2010].

International Biometrics & Identification Association, 2010. IBIA Identifies Real World Examples of Biometric Successes in Response to NRC Report, Biometric Recognition: Challenges And Opportunities. Available at: http://www.findbiometrics.com/articles/i/8338/ [Accessed December 1, 2010].

Introna, L.D. & Nissenbaum, H., 2000. Shaping the Web: Why the Politics of Search Engines Matters. *The Information Society: An International Journal*, 16(3), 169-185.

Introna, L.D. & Wood, D., 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society*, 2(2/3), 177-198.

IPS, 2005. Identity Matters for Stakeholders Newsletter (December 2005 edition).

IPS, 2006a. *First section 37 report to Parliament about the likely costs of the ID Cards Scheme*, Identity & Passport Service.

IPS, 2006b. *Safeguarding Your Identity: Identity and Passport Service Corporate and Business Plans 2006–2016*, Identity & Passport Service.

IPS, 2006c. *Strategic Action Plan for the National Identity Scheme: Safeguarding your identity*, Identity & Passport Service. Available at: http://www.identitycards.gov.uk/downloads/Strategic_Action_Plan.pdf.

IPS, 2007a. *National Identity Scheme Options Analysis - Outcome (Leaked document)*, Identity & Passport Service. Available at: http://identityproject.lse.ac.uk/NIS_Options_Analysis_Outcome.pdf.

IPS, 2007b. *NIS Strategic Supplier Framework Prospectus*, Identity &

Passport Service.

IPS, 2008a. *Introducing the National Identity Scheme: How the Scheme will work and how it will benefit you*, Identity & Passport Service.

IPS, 2008b. *Identity Cards Scheme Cost Report May 2008*, IPS.

IPS, 2008c. National Identity Scheme Delivery Plan 2008. Available at: http://www.ips.gov.uk/identity/downloads/national-identity-scheme-delivery-2008.pdf.

IPS, 2008d. *National Identity Scheme Delivery Plan 2008: A Response to Consultation*, Identity & Passport Service. Available at: http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/956.htm.

IPS, 2008e. *Identity Cards Scheme Cost Report November 2008*, Available at: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/Transcript_of_Home_Secretary_Speech_061108.pdf.

IPS, 2008f. *Identity and Passport Service Front Office Services Prospectus*, Identity & Passport Service.

IPS, 2009. Statement to address misconceptions arising from responses to a consultation paper on identity cards secondary legislation. Available at: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/09-03-10agenderStatementv4.pdf.

IPS, 2010. Reference: FOICR13955/10. Available at: http://www.whatdotheyknow.com/request/28389/response/103541/attach/3/13955 P Booth response.pdf.

Irwin, A. & Michael, M., 2003. *Science, Social Theory and Public Knowledge*, Maidenhead, UK: Open University Press.

Irwin, A. & Wynne, B., 1996. *Misunderstanding Science?: The Public Reconstruction of Science and Technology*, Cambridge: Cambridge University Press.

ISAP, 2008. *Independent Scheme Assurance Panel: Annual Report 2007*, Identity & Passport Service.

Jain, A.K., Ross, A. & Prabhakar, S., 2004. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

Jain, A. & Ross, A., 2004. Multibiometric systems. *Communications of the ACM*, 47(1), 34-40.

Jain, A.K., Duin, R.P. & Mao, J., 2000. Statistical Pattern Recognition: A Review. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22, 4-37.

Jain, A.K., Feng, J. & Nandakumar, K., 2010. Fingerprint Matching. *Computer*, 43(2), 36-44.

James, T. et al., 2006. Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. *Journal of Organizational and End User Computing*, 18(3), 1-24.

Janet Street-Porter, 2005. ID cards are simply unacceptable. *The Independent*. Available at: http://www.independent.co.uk/opinion/columnists/janet-street-porter/janet-streetporter-id-cards-are-simply-unacceptable-492079.html [Accessed November 8, 2010].

Jasanoff, S., 2000. The "Science Wars" and American Politics. In M. Dierkes

& C. von Grote, eds. *Between Understanding and Trust: The Public, Science and Technology*. Amsterdam: Harwood Academic, pp. 39-59.

Jenkins, R. & Burton, A.M., 2008. 100% Accuracy in Automatic Face Recognition. *Science*, 319(5862), 435.

Johnson, M.L., 2004. Biometrics and the Threat to Civil Liberties. *Computer*, 37(4), 90-92.

Johnstone, B., 2002. *Discourse analysis*, Malden, MA: Wiley-Blackwell.

Jones, L.A., Antón, A.I. & Earp, J.B., 2007. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*. Alexandria, Virginia, USA: ACM, pp. 91-98.

Kensing, F. & Blomberg, J., 1998. Participatory Design: Issues and Concerns. *Computer Supported Cooperative Work (CSCW)*, 7(3), 167-185.

Klein, H.K. & Myers, M.D., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly*, 23(1), 67-93.

Knight, W., 2007. Brain activity provides novel biometric key. *New Scientist*. Available at: http://www.newscientist.com/article/dn10963-brain-activity-provides-novel-biometric-key.html [Accessed December 4, 2010].

Lachoee, H., Crane, S. & Phippen, A., 2006. *TrustGuide: Final Report*, Bristol.

Latour, B., 1991. Technology is society made durable. In J. Law, ed. *A Sociology of Monsters: Essays on Power, Technology and Domination*. London: Routledge, pp. 103-131.

Law, J., 2004. *After Method* 1st ed., Abingdon, Oxon: Routledge.

Lazarick, R., 2005. Multibiometric techniques and standards activities. In *39th Annual 2005 International Carnahan Conference on Security Technology*. pp. 193-199.

Lee, A.S., 2001. Editorial. *MIS Quarterly*, 25(1), iii-vii.

van Lente, H., 1993. *Promising technology: the dynamics of expectations in technological developments*, Amsterdam: Proefschrift.

van Lente, H. & Rip, A., 1998. Expectations in Technological Developments: an Example of Prospective Structures to be Filled in by Agency. In C. Disco & N. van der Meulen, eds. *Getting New Technologies Together*. Berlin: Walter de Gruyter, pp. 203-229. Available at: http://doc.utwente.nl/34732/ [Accessed December 7, 2010].

Lettice, J., 2010. ID card astroturf - No2ID beats the truth out of IPS. *The Register*. Available at: http://www.theregister.co.uk/2010/07/29/ips_id_card_astroturf/ [Accessed October 29, 2010].

Lewis, P., 2009. Ahead of G20 summit, council told to switch off illegal £15m CCTV network. *The Guardian*. Available at: http://www.guardian.co.uk/uk/2009/mar/30/cctv-london-government-transport-g20 [Accessed November 16, 2010].

Ley, B.L., Jankowski, N. & Brewer, P.R., 2010. Investigating CSI: Portrayals of DNA testing on a forensic crime show and their potential effects. *Public Understanding of Science*. Available at: http://pus.sagepub.com/content/early/2010/05/11/0963662510367571.

abstract.

Liberatore, A., 2007. Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union. *European Journal of Criminal Policy Research*, 13(1), 109-137.

Lin, A. & Silva, L., 2005. The social and political construction of technological frames. *European Journal of Information Systems*, 14(1), 49-59.

Linder, F., 2007. Input Validation Done Wrong. *The Recurity Lablog*. Available at: http://blog.recurity-labs.com/archives/2007/06/12/input_validation_done_wrong/index.html [Accessed October 18, 2010].

Liu, Y., 2009. Identifying Legal Concerns in the Biometric Context. *Journal of International Commercial Law and Technology*, 3(1), 45-54.

Lösch, A., 2006. Anticipating the futures of nanotechnology: Visionary images as means of communication. *Technology Analysis & Strategic Management*, 18(3/4), 393-409.

LSE Identity Project, 2005. *Main Report*, London School of Economics and Political Science. Available at: http://identityproject.lse.ac.uk/identityreport.pdf.

LSE Identity Project, 2006. *Response to written submission by Dr. John Daugman*, London, UK: London School of Economics and Political Science. Available at: http://identityproject.lse.ac.uk/LSE_DaugmanResponse.pdf.

Lyon, D., 2001. Under my skin: From identification papers to body surveillance. In J. Caplan & J. Torpey, eds. *Documenting Individual Identity*.  Princeton: Princeton University Press, pp. 291-310.

Lyon, D., 2002. *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* 1st ed., London: Routledge.

Lyon, D., 2004a. ID Cards: Social Sorting by Database. *Oxford Internet Institute, Internet Issue Brief*, 3, 1-14.

Lyon, D., 2004b. The Border is Everywhere: ID Cards, Surveillance and the Other. In E. Zureik & M. Salter, eds. *Global Surveillance and Policing: Borders, security, identity*. Cullompton, UK: Willan.

Lyon, D., 2007. *Surveillance Studies: An Overview*, Cambridge: Polity Press.

Lyon, D., 2009. *Identifying Citizens*, Cambridge: Polity Press.

MacKenzie, D.A., 1993. *Inventing accuracy: a historical sociology of nuclear missile guidance*, Cambridge, MA: MIT Press.

Martin, A.K., 2008. Adapting theory for researching future expectations in information systems innovations: the case of the United Kingdom's national biometric identity scheme. Presentation at the 2008 4S conference in Rotterdam, The Netherlands.

Martin, A.K., van Brakel, R. & Bernhard, D.J., 2009. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*, 6(3), 213-232.

Marx, G.T., 1998. Ethics for the New Surveillance. *The Information Society: An International Journal*, 14(3), 171-185.

Marx, G.T., 2004. What’s new about the “new surveillance”?: Classifying for change and continuity. *Knowledge, Technology & Policy*, 17(1), 18-37.

Masnick, M., 2010. TSA Agents Absolutely Hate New Pat Downs, Find Them Disgusting And Morale Breaking. *Techdirt*. Available at: http://www.techdirt.com/articles/20101119/10225611947/tsa-agents-absolutely-hate-new-pat-downs-find-them-disgusting-morale-breaking.shtml [Accessed December 31, 2010].

Matsumoto, T. et al., 2002. Impact of Artificial Gummy Fingers on Fingerprint Systems. *Proceedings of SPIE*, 4677(1), 275-289.

McCue, A., 2005. Biometrics roadshow kicks off ID cards charm offensive. *Silicon.com*. Available at: http://www.silicon.com/legacy/research/specialreports/idcards/0,3800010140,39152175,00.htm [Accessed November 8, 2010].

Mercuri, R.T. & Neumann, P.G., 2003. Security by obscurity. *Communications of the ACM*, 46(11), 160.

Mhatre, A.J. et al., 2005. Efficient search and retrieval in biometric databases. In A. K. Jain & N. K. Ratha, eds. *Biometric Technology for Human Identification II*. pp. 265-273.

Michael, M., 2009. Publics performing publics: of PiGs, PiPs and politics. *Public Understanding of Science*, 18(5), 617 -631.

Miles, M.B., 1979. Qualitative Data as an Attractive Nuisance: The Problem of Analysis. *Administrative Science Quarterly*, 24(4), 590-601.

Miles, M.B. & Huberman, M., 1994. *Qualitative Data Analysis: An Expanded Sourcebook* 2nd ed., London: Sage.

Miyazawa, K. et al., 2008. An Effective Approach for Iris Recognition Using Phase-Based Image Matching. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 30(10), 1741-1756.

Monro, D., Rakshit, S. & Dexin Zhang, 2007. DCT-Based Iris Recognition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4), 586-595.

Monteiro, E. & Hanseth, O., 1996. Social Shaping Of Information Infrastructure: On Being Specific About The Technology. In W. Orlikowski et al., eds. *Information technology and changes in organisational work*. London: Chapman & Hall, pp. 325-343. Available at: [Accessed July 30, 2010].

Moody, J., 2004. Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use. In *Issues in Informing Science and Information Technology 2004*. Rockhampton, Australia, pp. 753-761.

Moorhouse, A. et al., 2009. The Nose on Your Face May Not be so Plain: Using the Nose as a Biometric. In *Proceedings on the IET 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP-09)*. Kingston, UK.

Moss, D., 2009. Collar the lot of us! The biometric delusion: Optimism beats evidence in the drive to fingerprint the world. *The Register*. Available at: http://www.theregister.co.uk/2009/08/14/biometric_id_delusion/print.html.

Mosse, B. & Whitley, E.A., 2009. Critically classifying: UK e-government website benchmarking and the recasting of the citizen as customer. *Information Systems Journal*, 19(2), 149-173.

Muller, M.J. & Kuhn, S., 1993. Participatory design. *Communications of the ACM*, 36(6), 24-28.

Murakami Wood, D. & Firmino, R., 2010. Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'. *Identity in the Information Society*, 2(3), 297-317.

Myers, M., 1997. Qualitative Research in Information Systems. *Management Information Systems Quarterly*, 21(2), 241-242.

Myers, M.D., 2008. *Qualitative Research in Business & Management*, London: Sage.

NAO, 2007. *Identity and Passport Service: Introduction of ePassports*, Available at: http://www.nao.org.uk/publications/0607/introduction_of_epassports.aspx.

National Police Improvement Agency, 2006. *Automated face recognition: Applications within law enforcement*, Available at: http://www.npia.police.uk/en/docs/Face_Recognition_Report.pdf.

Ng-Kruelle, G. et al., 2006. Biometrics and e-Identity (e-Passport) in the European Union: End-user perspectives on the adoption of a controversial innovation. *Journal of Theoretical and Applied Electronic Commerce Research*, 1(2), 12-35.

Nisenson, M. et al., 2003. Towards Behaviometric Security Systems: Learning to Identify a Typist. *Lecture Notes in Computer Science*, 2838, 363-374.

Office of Science and Technology, 2000. *Science and the Public: A review of science communication and public attitudes to science in Britain*, London: OST and Wellcome Trust. Available at: http://www.wellcome.ac.uk/stellent/groups/corporatesite/@msh_peda/d ocuments/web_document/wtd003419.pdf.

O'Gorman, L., 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE*, 91(12), 2021-2040.

Orlikowski, W.J., 2010. The sociomateriality of organisational life: considering technology in management research. *Cambridge Journal of Economics*, 34(1), 125-141.

Orlikowski, W.J. & Gash, D.C., 1992. *Changing Frames: Understanding Technological Change in Organizations*, MIT Sloan. Available at: http://ideas.repec.org/p/mit/sloanp/2382.html.

Orlikowski, W.J. & Gash, D.C., 1994. Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems*, 12(2), 174-207.

Orlikowski, W.J. & Iacono, C.S., 2001. Research Commentary: Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact. *Information Systems Research*, 12(2), 121-134.

Orlikowski, W.J. & Scott, S.V., 2008. Chapter 10: Sociomateriality: Challenging the Separation of Technology, Work and Organization. *The Academy of Management Annals*, 2, 433-474.

Osborne, D. & Gaebler, T., 1992. *Reinventing Government: How The Entrepreneurial Spirit Is Transforming The Public Sector* 1st ed., Reading, Mass: Addison-Wesley.

Otjacques, B., Hitzelberger, P. & 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., 2007. ID card bidders jostle for position. *Financial Times*. Available at: http://www.ft.com/cms/s/d43817ca-41f1-11dc-8328-0000779fd2ac.html.

Parker, I., 1992. Discovering discourses, tackling texts. In I. Parker, ed. *Discourse dynamics critical analysis for social and individual psychology*. London: Routledge.

Pato, J.N. & Millett, L.I. eds., 2010. *Biometric Recognition: Challenges and Opportunities*, Washington, D.C.: The National Academies Press.

Pavone, V. & Degli Esposti, S., 2010. Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. *Public Understanding of Science*, 1-16.

Perakslis, C. & Wolk, R., 2006. Social Acceptance of RFID as a Biometric Security Method. *IEEE Technology and Society Magazine*, 25, 34-42.

Pinch, T.J. & Bijker, W.E., 1984. The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, 14(3), 399-441.

van der Ploeg, I., 1999. Written on the Body: Biometrics and Identity. *Computers and Society*, 29(1), 37-44.

van der Ploeg, I., 2003. Biometrics and privacy: a note on the politics of theorizing technology. *Information Communication and Society*, 6(1), 85-104.

Pollock, N. & Williams, R., 2008. *Software and organizations : the biography of the enterprise-wide system or how SAP conquered the world*, New York: Routledge.

Pollock, N. & Williams, R., 2010. The business of expectations: How promissory organizations shape technology and innovation. *Social Studies of Science*, 40(4), 525-548.

Ponemon Institute, 2006. *Global Study on the Public's Perceptions about Identity Management*, Unisys. Available at: http://danishbiometrics.files.wordpress.com/2009/08/109_597_file.pdf.

Poster, M., 2006. *Information Please: Culture and Politics in the Age of Digital Machines*, Durham: Duke University Press.

Pouloudi, A. & Whitley, E.A., 2000. Representing Human and Non-human Stakeholders: On Speaking with Authority. In *Proceedings of the IFIP TC9 WG 9.3 International Conference on Home Oriented Informatics and Telematics*. Kluwer, B.V., pp. 339-354.

Prabhakar, S., Pankanti, S. & Jain, A.K., 2003. Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy Magazine*, 1(2), 33-42.

Prior, L., 2003. *Using Documents in Social Research*, London: Sage.

Privacy International, 1997. History of ID Cards in the United Kingdom. Available at: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-61886 [Accessed December 2, 2010].

Public Administration Committee, 2011. *Government and IT - "A Recipe For Rip-Offs": Time For A New Approach*. Available at: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubadm/715/71502.htm [Accessed September 13, 2011].

Pugh, T., 2010. TSA chief says he disregarded advice on pat-downs. *The Miami Herald*. Available at: http://www.miamiherald.com/2010/11/22/1938148/tsa-chief-says-he-disregarded.html [Accessed November 23, 2010].

Ragin, C.C., 1992. Introduction: Cases of "What is a case"? In C. C. Ragin & H. S. Becker, eds. *What is a Case?: Exploring the Foundations of Social Inquiry*. Cambridge: Cambridge University Press.

Ragin, C.C. & Becker, H.S. eds., 1992. *What Is a Case?: Exploring the Foundations of Social Inquiry*, Cambridge: Cambridge University Press.

Ramiller, N.C. & Wang, P., 2009. Community Learning in Information Technology Innovation. *Management Information Systems Quarterly*, 33(4), 709-734.

Reuters, 2010. FACTBOX-What is biometric identification? *Reuters*. Available at: http://www.reuters.com/article/idUSSGE68J0LE20100920 [Accessed November 24, 2010].

Rose, N., 1999. *Powers of Freedom: Reframing Political Thought*, Cambridge University Press.

Ross, A. & Jain, A.K., 2004. Multimodal biometrics: An overview. In *Proceedings of the 12th European Signal Processing Conference*. Vienna, Austria, pp. 1221-1224.

Ross, A., Shah, J. & Jain, A.K., 2007. From Template to Image: Reconstructing Fingerprints from Minutiae Points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 544-560.

Ryan, C., 1990. *Prime Time Activism: Media Strategies for Grassroots Organizing*, South End Press.

Rubin, J. & Winton, R., 2008. Fingerprint lab's not up to the task. *Los Angeles Times*. Available at: http://articles.latimes.com/2008/nov/17/local/me-fingerprint17 [Accessed November 5, 2010].

Ryan, J., 2006. ID cards speech at Biometrics 2006 conference.

Sarnoff Corporation, 2010. Iris on the Move. Available at: http://www.sarnoff.com/products/iris-on-the-move.

Sasse, M.A., 2007. Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems. *IEEE Security and Privacy*, 5(3), 78-81.

Sauder, M. & Espeland, W.N., 2007. Rankings and Reactivity: How Public Measures Recreate Social Worlds. *American Journal of Sociology*, 113(1), 1-40.

Scott, M., Acton, T. & Hughes, M., 2005. An assessment of biometric identities as a standard for e-government services. *International Journal of Services and Standards*, 1(3), 271-286.

Shelton, D., 2008. The 'CSI Effect': Does It Really Exist? *NIJ Journal*, 259, 1-7.

Sismondo, S., 2009. *An Introduction to Science and Technology Studies* 2nd ed., Malden, MA: Wiley-Blackwell.

Smith, J., 2008a. Making identity cards a reality. Available at: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/Transcript_of_Home_Secretary_Speech_061108.pdf.

Smith, J., 2008b. PLP Brief: Delivering the National Identity Scheme.

Smith, J., 2008c. The National Identity Scheme - Delivery Plan 2008.

Smith, R., 2005. The public won't buy this plastic folly. *The Times*. Available at: http://business.timesonline.co.uk/tol/business/law/article1080145.ece [Accessed November 1, 2010].

Snow, D.A. & Benford, R.D., 1988. Ideology, frame resonance, and participant mobilization. *International Social Movement Research,* 1, 197–218.

Snow, M., 2010. Eye scans will help keep better track of suspects, NYPD says. *CNN.com*. Available at: http://edition.cnn.com/2010/US/11/17/new.york.iris.scanners/ [Accessed December 29, 2010].

Sprokkereef, A. & De Hert, P., 2007. Ethical Practice in the Use of Biometric Identifiers within the EU. *Law, Science and Policy*, 3(2), 177-202.

Stahl, B.C. & Brooke, C., 2008. The contribution of critical IS research. *Communications of the ACM*, 51(3), 51-55.

Stanglin, D., 2010. 'Fatwa' forbids Muslims going through full-body scanners -. *USA Today*. Available at: http://content.usatoday.com/communities/ondeadline/post/2010/02/fatwa-forbids-muslims-going-through-full-body-scanners/1 [Accessed November 25, 2010].

Stevens, S.M., 2008. Speaking Out. *Science, Technology & Human Values*, 33(6), 730 -753.

Strickler, L., 2010. TSA Body Scanners: Do They Even Work? *CBS News*. Available at: http://www.cbsnews.com/8301-31727_162-20023079-

10391695.html [Accessed November 24, 2010].

Suchman, L. & Bishop, L., 2000. Problematizing 'Innovation' as a Critical Project. *Technology Analysis & Strategic Management*, 12(3), 327-333.

Sung, J.J. & Hopkins, M.M., 2006. Towards a method for evaluating technological expectations: Revealing uncertainty in gene silencing technology discourse. *Technology Analysis & Strategic Management*, 18(3/4), 345-359.

Surveillance Studies Network, 2010. *The Surveillance Society: An update report on developments since the 2006 Report on the Surveillance Society by members of the Surveillance Studies Network*, ICO. Available at: http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/surveillance_report_for_home_select_committee.ashx [Accessed December 2, 2010].

Swanson, E.B., 2003. Talking the IS innovation walk. In E. H. Wynn et al., eds. *Global and organisational discourse about information technology*. Boston: Kluwer, pp. 15-32.

Swanson, E.B. & Ramiller, N., 1997. The organizing vision in information systems innovation. *Organization science*, 8(5), 458-474.

Swanson, E.B. & Ramiller, N.C., 2004. Innovating mindfully with Information Technology. *MIS Quarterly*, 28(4), 553-583.

Swire, P., 2008. Chertoff says fingerprints aren't 'personal data'. *Think Progress*. Available at: http://thinkprogress.org/2008/04/16/chertoff-fingerprints [Accessed July 27, 2010].

The Faith Community Consultation Consortium, 2005. *A response to the* *introduction of Identity Cards: Summary of the consultation with faith communities in Britain*, Fujitsu.

Thornton, J., Savvides, M. & Kumar, V., 2007. A Bayesian Approach to Deformed Pattern Matching of Iris Images. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4), 596-606.

Timmins, N., 2007a. Bid invitations for ID system imminent. *Financial Times*. Available at: http://www.ft.com/cms/5b6e1380-41f1-11dc-8328-0000779fd2ac.html.

Timmins, N., 2007b. Invitations to bid imminent. *Financial Times*. Available at: http://www.ft.com/cms/6b376de8-4223-11dc-8328-0000779fd2ac.html.

Tolbert, P.S. & Zucker, L.G., 1983. Institutional Sources of Change in the Formal Structure of Organizations: The Diffusion of Civil Service Reform, 1880-1935,*Administrative Science Quarterly*, 28, 22-39.

Torpey, J., 1999. *The Invention of the Passport: Surveillance, Citizenship and the State* 1st ed., Cambridge: Cambridge University Press.

Traulsen, J.M., Almarsdottir, A.B. & Bjornsdottir, I., 2004. Interviewing the Moderator: An Ancillary Method to Focus Groups. *Qualitative Health Research*, 14(5), 714-725.

Travis, A., 2005. Memory chips, fingerprints, iris scans ... but will it work? *The Guardian*. Available at: http://www.guardian.co.uk/uk/2005/may/26/idcards.immigrationpolicy1 [Accessed November 1, 2010].

Travis, A., 2007. Home Office insists biometric data is secure. *The Guardian*. Available at: http://www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.econo my [Accessed November 3, 2010].

Travis, A., 2010. New scanners break child porn laws. *The Guardian*. Available at: http://www.guardian.co.uk/politics/2010/jan/04/new-scanners-child-porn-laws [Accessed November 25, 2010].

UK Borders Agency, 2008a. *A Strong New Force at the Border*, Home Office. Available at: http://www.statewatch.org/news/2008/aug/uk-border-agency-rep.pdf.

UK Borders Agency, 2008b. *Compulsory identity cards for foreign nationals: Results from the consultation on the "code of practice about the sanctions for non-compliance with the biometric regulations"*, Home Office.

UK Borders Agency, 2008c. Identity cards for foreign nationals: General guidance. Available at: http://www.ukba.homeoffice.gov.uk/sitecontent/documents/employersandsponsors/preventingillegalworking/icfn-info-guidance/icfn-general-guidance.

UKPS, 2006. *Annual Report and Accounts 2005–2006*, UK Passport Service. Available at: http://www.official-documents.gov.uk/document/hc0607/hc07/0775/0775.pdf.

Väliverronen, E., 2004. Stories of the “medicine cow”: representations of future promises in media discourse. *Public Understanding of Science*, 13(4), 363-377.

Venkatesh, V. & Davis, F.D., 2000. A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2), 186-204.

Venturini, T., 2009. Diving in magma: how to explore controversies with actor-network theory. *Public Understanding of Science*, 19(3), 258-273.

Wang, P., 2009. Popular Concepts beyond Organizations: Exploring New Dimensions of Information Technology Innovations. *Journal of the Association for Information Systems*, 10(1), 1-30.

Wang, P., 2010. Chasing the Hottest IT:  Effects of Information Technology Fashion on Organizations. *Management Information Systems Quarterly*, 34(1), 63-85.

Wang, P. & Swanson, E.B., 2008. Customer relationship management as advertised: Exploiting and sustaining technological momentum. *Information Technology & People*, 21(4), 323-349.

Washington Post, 2010. Picture or pat-down? Available at: http://www.washingtonpost.com/wp-dyn/content/graphic/2010/11/22/GR2010112204167.html [Accessed November 25, 2010].

Waterhouse, K., 2007. On the missing discs: such a fuss about this one-off lapse. *Daily Mail*. Available at: http://www.dailymail.co.uk/debate/columnists/article-496346/On-missing-discs-fuss-lapse.html [Accessed November 3, 2010].

Watt, N., 2008. Interview: Gordon Brown on ID cards. *The Observer*. Available at: http://www.guardian.co.uk/politics/2008/jan/06/uk.idcards [Accessed October 27, 2010].

Wayman, J., 2001. Fundamentals of Biometric Authentication Technologies. *International Journal of Image and Graphics*, 1(1), 93-113.

Webster, A., 2005. ID cards will cost too much and don't tackle problems. *The*

*Sun*.

Weerakkody, N., 2006a. A Comparative Analysis of Opinions of Americans, Australians and Malaysians on the Use of Biometric Devices in Workplaces for Security and Monitoring of Worker Productivity. *The International Journal of Knowledge, Culture and Change Management*, 5(6), 43-52.

Weerakkody, N., 2006b. A Comparison of Australian and Malaysian Views on the Use of Biometric Devices in Everyday Situations. *International Journal of Learning*, 12(6), 63-72.

Weick, K.E., 1995. *Sensemaking in organizations*, Thousand Oaks, CA: Sage.

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

Whitley, E.A. & Hosein, I.R., 2008. Doing the politics of technological decision making: due process and the debate about identity cards in the U.K. *European Journal of Information Systems*, 17(6), 668-677.

Whitley, E.A., 2009. Perceptions of government technology, surveillance and privacy: the UK identity cards scheme. In D. Neyland & B. Goold, eds. *New Directions in Privacy and Surveillance*. Cullompton, UK: Willan, pp. 133-156.

Whitley, E.A. & Hosein, G., 2010. *Global Challenges for Identity Policies*, Basingstoke: Palgrave Macmillan.

Whitley, E.A. & Hosein, G., 2010a. Opposition policies on identity cards. *British politics and policy at LSE*. Available at:

http://blogs.lse.ac.uk/politicsandpolicy/?p=1252 [Accessed November 10, 2010].

Whitten, A., 2008. Are IP addresses personal? *Google Public Policy Blog*. Available at: http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html [Accessed October 29, 2010].

Wickins, J., 2007. The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics*, 13(1), 45-54.

Williams, R., 2006. Compressed Foresight and Narrative Bias: Pitfalls in Assessing High Technology Futures. *Science as Culture*, 15(4), 327-348.

Wilson, C. & Harsha, P., 2008. IT policy: Advising policymakers is more than just providing advice. *Communications of the ACM*, 51(12), 24-26.

Winner, L., 1980. Do Artefacts Have Politics? *Daedalus*, 109, 121-136.

Wintour, P., 2007. Lost in the post - 25 million at risk after data discs go missing. *The Guardian*. Available at: http://www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.economy3 [Accessed November 10, 2010].

Woodward, W., 2007. 10-finger exercise for ID cards. *The Guardian*. Available at: http://www.guardian.co.uk/uk/2007/aug/10/humanrights.idcards [Accessed November 2, 2010].

Wynne, B., 1995. Public Understanding of Science. In S. Jasanoff et al., eds. *Handbook of science and technology studies*. Thousand Oaks: Sage, pp. 361-388.

Yin, R.K., 2003. *Case Study Research: Design and Methods* 3rd ed., Thousand Oaks, CA: Sage.

Zorkadis, V. & Donos, P., 2004. On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security*, 12(1), 125-137.

Zureik, E. & Hindle, K., 2004. Governance, Security and Technology: The Case of Biometrics. *Studies in Political Economy*, 73, 113-137.

Zviran, M. & Erlich, Z., 2006. Identification and Authentication: Technology and Implementation Issues. *Communications of the Association for Information Systems*, 17(4), 90-105.

# Appendix 1

Focus group interview guide[25]

*Introduction*

Welcome the participants and thank them for attending the session and for agreeing to participate in a discussion of personal identity and biometric ID in the UK

(Promise complete anonymity)

*Opening the frame (5 minutes)*

'There has been a lot of coverage of personal identity in the press and on the television lately, including things like ID theft and the troubles with proving who you are on-line. Can you think of any situations in which you have had problems **proving your identity** or have been asked to provide more **personal information** that you'd like?'

*Broaching the focal issue (5 minutes)*

'One of the things I'm interested in is "**biometrics**". Does anyone know what these are?' (**If not**, then mention **"fingerprints, eye scans** and **facial recognition"**)

*Presenting the National Identity Scheme debate (6 minutes)*

'The UK government has a plan to address some of the perceived problems related to identity by using biometric technologies. Let's watch a video which discusses this plan.' (If video facilities are not available, then use comics on biometrics as the substitute stimuli)

[25] Adapted from Focus Group Short Topic Guide in Gaskell & Bauer's (2001) *Biotechnology 1996-2000* (see Appendix 2) and the TrustGuide Project's Discussion Guide for Trust, Security and Privacy Issues, Version 3 (2007) (accessed through the authors, Hazel Lacohée and Andy Phippen)

*Focusing on biometrics (15 minutes)*

‘Who here has **previous experience** using biometric technologies? How do they **work**?’

‘In your opinion, are biometrics **a better means of verifying** someone’s identity than, say, PINs, passwords or tokens? Why (or why not)?’

‘In your mind, what **differences** are there between biometric technologies used at **home** (e.g., to log into a laptop) or at **work** (e.g., to access the office building) and a **national biometric ID scheme**, if any?’

‘How do you think the government will a) **collect,** b) **store** and c) **use** biometric data?’

*Evaluation of specific applications (8 minutes)*

‘In your mind, **what problems does this Scheme help to solve, how will it work**, and **when will it be used**? Do you imagine it will work **like other systems** you encounter daily?’

*The alternate view (6 minutes)*

Present the German/CCC videos, depending on the tone of the discussion thus far

*Risk and morals (5 minutes)*

‘What do you see as the **benefits** of using biometrics? What things make you **nervous** or **uncomfortable** about them?’

‘Do you have any **moral concerns** with the **government use** of biometrics? If so, what are they?’

‘Do you see biometrics as a positive or negative for **personal privacy**? How so?’

‘Are there any **surveillance capacities** of biometrics that you can think of?’

*Trust (5 minutes)*

‘Do you **trust** the government to handle your biometric information securely?’

‘What would the government need to do to prove that it is a) **capable of** and b) **motivated to** handle this information securely?’

*Wrapping up*

‘Have your ideas about biometrics changed as a result of this discussion? If so, how?’

# Appendix 2

Interview guide for ‘interviewing the moderator’[26]

1. *Group dynamics*: How would you rate the group dynamics compared to the other groups? Was there a lack of group dynamics?

2. *Composition of the group*: Who was who in the group?

3. *Go through the major questions*: a) Definition and experience with biometrics; b) Role of biometrics in the Scheme; c) Benefits, risks, morals and trust

4. *Surveillance and privacy*: What, if anything, did they mention about surveillance and privacy?

5. *Government*: What, if anything, did they say about the government (as the sponsor of the Scheme)?

6. *Off the record*: What did they talk about after the tape recorder was turned off? Did they ask the facilitator direct questions?

[26] Adapted from the interview guide in Interviewing the Moderator: An Ancillary Method to Focus Groups (Traulsen et al. 2004, p.724)

# Appendix 3

Primary government policy statements (listed chronologically)

| Date | Author | Title |
|---|---|---|
| 07/2002 | Home Office | Entitlement Cards and Identity Fraud: A Consultation Paper |
| 07/2002 | Cabinet Office | Identity Fraud: A Study |
| 06/2003 | Office of Government Commerce | Gateway Review of Entitlement Cards |
| 10/2003 | Home Office | Entitlement Cards Consultation |
| 11/2003 | Home Office | Identity Cards: The Next Steps |
| 11/2003 | Home Office | A Summary of Findings from the Consultation Exercise on Entitlement Cards and Identity Fraud |
| 11/2003 | David Blunkett | ID cards statement |
| 11/2003 | Cragg Ross Dawson (for the HO) | Public perceptions of identity/entitlement cards: Qualitative Research Report |
| 11/2003 | Cragg Ross Dawson (for the HO) | Identity Cards: Qualitative research on perceptions of cost |
| 11/2003 | Home Office | Entitlement Cards and Identity Fraud – the Government’s response to the consultation points |
| 01/2004 | Office of Government Commerce | Gateway Review of Identity Cards |
| 04/2004 | N/A | Draft Identity Cards Bill |

| | | |
|---|---|---|
| 04/2004 | Home Office | Legislation on Identity Cards: A Consultation |
| 04/2004 | David Blunkett et al. | Identity Cards: Home Office PLP Briefing |
| 07/2004 | Home Affairs Committee | Identity Cards |
| 08/2004 | Cragg Ross Dawson (for the HO) | Public perceptions of identity cards: Qualitative Research Report |
| 10/2004 | Home Office | The Government Reply to the Fourth Report from the Home Affairs Committee: Identity Cards |
| 10/2004 | Home Office | A Summary of Findings from the Consultation on Legislation on Identity Cards |
| 11/2004 | David Blunkett | Identity Cards Speech |
| 11/2004 | Home Office | Identity Cards Bill: Regulatory Impact Assessment |
| 12/2004 | Central Office of Information | Identity Cards 2004 |
| 12/2004 | House of Commons | Research paper on the Identity Cards Bill |
| 12/2004 | Cragg Ross Dawson (for the HO) | Identity Cards – People with special issues: Response to the proposed customer experience |
| 12/2004 | Cragg Ross Dawson (for the HO) | Identity Cards – The public's response to proposed customer propositions |
| 01/2005 | Joint Committee on Human Rights | Report on the Identity Cards Bill |
| 03/2005 | FCCC | A response to the introduction of identity cards |
| 04/2005 | Labour Party | Manifesto 2005 |
| 05/2005 | Atos Origin (for UKPS) | Biometrics Enrollment Trial: Management Summary |
| 05/2005 | Atos Origin (for UKPS) | Biometrics Enrollment Trial: Report |
| 05/2005 | Home Office | Updated Regulatory Impact Assessment for the Identity Cards Bill |

| | | |
|---|---|---|
| 05/2005 | Home Office | Identity Cards Bills: Race equality impact assessment |
| 05/2005 | Home Office | Identity Cards Briefing |
| 06/2005 | House of Commons | Research paper on the Identity Cards Bill |
| 06/2005 | Home Office | Identity Cards Scheme Benefits Overview |
| 06/2005 | Home Office | Identity Cards Trade-off Research: Interim report |
| 07/2005 | Home Office | Response to the London School of Economics' ID Cards Cost Estimates & Alternative Blueprint |
| 09/2005 | Office for National Statistics | Citizen Information Project Risk Status Paper |
| 10/2005 | Home Office | Assessment of awareness and demand for the Identity Cards Scheme |
| 10/2005 | UK Passport Service | Procurement Strategy Market Soundings [presentation] |
| 10/2005 | Joint Committee on Human Rights | Legislative scrutiny: First Progress Report (drawing special attention to the Identity Cards Bill) |
| 10/2005 | Home Office | Identity Cards Programme Procurement Strategy Market Soundings [questionnaire] |
| 10/2005 | Lords Constitution Committee | Identity Cards Bills: Report with Evidence |
| 11/2005 | Cabinet Office | Transformational Government: Enabled by Technology |
| 11/2005 | KPMG (for the HO) | Cost Methodology & Cost Review Outline Business Case Review: Published Extract |
| 11/2005 | Home Office | P50: 05.11.08.HO.Summary of work in progress KPMG review |
| 11/2005 | House of Lords | Delegated Powers and Regulatory Reform Committee report on the Identity Cards Bill |
| 11/2005 | Andy Burnham | CityForum speech: Identity Cards – Economy, Efficiency, Effectiveness |
| 11/2005 | Andy Burnham | Letter to Professor Ian Angell |

|  |  |  |
|---|---|---|
| 11/2005 | Home Office | Identity cards in other countries (1) |
| 11/2005 | Home Office | Identity cards in other countries (2) |
| 12/2005 | N/A | Identity Cards Bill [as amended in Committee] |
| 12/2005 | Home Office | Assessment of awareness and demand amongst foreign nationals for biometric residence permits |
| 12/2005 | Home Office | Draft code of practice on civil penalties |
| 12/2005 | Home Office | Identity matters for stakeholders newsletter (December 2005) |
| 01/2006 | N/A | Identity Cards Bill [as amended on report] |
| 02/2006 | Andy Burnham | Note on the costs of ID cards |
| 03/2006 | Andy Burnham | Identity Cards Bills Update [letter] |
| 03/2006 | Cabinet Office | Transformational Government: Implementation Plan |
| 04/2006 | Identity and Passport Service | IPS corporate and business plans 2006-2016 |
| 04/2006 | Identity and Passport Service | IPS framework agreement |
| 04/2006 | N/A | Identity Cards Act |
| 04/2006 | Office for National Statistics | Citizen Information Project |
| 05/2006 | Identity and Passport Service | FoI response (3112) on biometric passport standards |
| 07/2006 | Science & Technology Committee | Identity Card Technologies: Scientific Advice, Risk and Evidence |
| 07/2006 | UK Passport Service | Annual report and accounts 2005-2006 |
| 08/2006 | Identity and Passport Service | FoI response (3783) on biometric passport standards |

| | | |
|---|---|---|
| 10/2006 | Identity and Passport Service | First Section 37 Report to Parliament about the Likely Costs of the ID Cards Scheme |
| 10/2006 | Home Office | Government reply to HoC Science and Technology Committee report on Identity Card Technologies |
| 10/2006 | Joan Ryan | ID cards speech at Biometrics 2006 conference |
| 10/2006 | Science & Technology Committee | Scientific Advice, Risk and Evidence Based Policy Making (Volume 1) |
| 10/2006 | Science & Technology Committee | Scientific Advice, Risk and Evidence Based Policy Making (Volume 2) |
| 11/2006 | Tony Blair | Identity Management: Why the UK needs a national ID scheme [presentation] |
| 11/2006 | Identity and Passport Service | FoI response (10316) on biometric passport malfunctions |
| 11/2006 | James Hall | Web chat transcript |
| 11/2006 | Cabinet Office | Identity Risk Management |
| 12/2006 | Home Office | Strategic Action Plan for the National Identity Scheme |
| 12/2006 | Home Office | Borders, Immigration and Identity Action Plan |
| 02/2007 | National Audit Office | Identity and Passport Service: Introduction of ePassports |
| 02/2007 | Central Office of Information | NIS Tracking Research (February 2007) |
| 05/2007 | Identity and Passport Service | Identity Cards Scheme: Cost Report May 2007 |
| 05/2007 | Identity and Passport Service | National Identity Scheme Procurement: Briefing Presentation |
| 05/2007 | Biometrics Assurance Group | Annual Report 2006 |
| 06/2007 | Liam Byrne | Securing our identity: A 21st century public good (speech) |
| 07/2007 | Committee of Public Accounts | Identity and Passport Service: Introduction of ePassports |

|  |  |  |
|---|---|---|
| 07/2007 | N/A | UK Borders Act 2007 |
| 08/2007 | Identity and Passport Service | NIS Strategic Supplier Framework Prospectus |
| 09/2007 | Identity and Passport Service | Identity Service Proposition – A ‘joint venture’ with the Criminal Records Bureau |
| 09/2007 | Identity and Passport Service | Basic Passport Checks |
| 10/2007 |  | Memo to update the government response to the Science and Technology Select Committee report |
| 10/2007 | Central Office of Information | National Identity Scheme Tracking Research Wave 2: October 2007 |
| 11/2007 | Identity and Passport Service | Identity Cards Scheme Cost Report November 2007 |
| 11/2007 | Identity and Passport Service | Proof of Age Research |
| 12/2007 | Home Office | Government response to PAC report on ePassports |
| 12/2007 | Identity and Passport Service | NIS Delivery Strategy: Aligning strategy and delivery [presentation] |
| 01/2008 | Gordon Brown | Interview on ID cards with the Guardian |
| 01/2008 | Identity and Passport Service | NIS Options Analysis - Outcome [leaked document] |
| 02/2008 | Borders and Immigration Agency | Consultation on Compulsory Identity Cards for Foreign Nationals |
| 03/2008 | James Crosby | Challenges and opportunities in identity assurance |
| 03/2008 | Jacqui Smith | The National Identity Scheme – Delivery Plan 2008 [Demos speech] |
| 03/2008 | Jacqui Smith | PLP Brief: Delivering the National Identity Scheme |
| 03/2008 | Home Office | National Identity Scheme: Delivery Plan 2008 |
| 03/2008 | Cabinet Office | The National Security Strategy of the United Kingdom |

|  |  |  |
|---|---|---|
| 03/2008 | Central Office of Information | National Identity Scheme Tracking Research Wave 3: February 2008 |
| 05/2008 | ISAP | Annual Report 2007 |
| 05/2008 | Identity and Passport Service | Identity Cards Scheme Cost Report May 2008 |
| 05/2008 | Identity and Passport Service | Report on key projects implemented in 2007 |
| 05/2008 | Central Office of Information | National Identity Scheme Tracking Research Wave 4: May 2008 |
| 06/2008 | UK Borders Agency | Results of the Consultation on Compulsory Identity Cards for Foreign Nationals |
| 06/2008 | UK Borders Agency | Results of the Public Consultation on Compulsory Identity Cards for Foreign Nationals |
| 06/2008 | Home Office | Code of Practice about the Sanctions for Non-compliance with the Biometric Registration Regulations |
| 06/2008 | UK Borders Agency | Equality Impact Assessment (for identity cards for foreign nationals) |
| 06/2008 | Home Office | Impact Assessment of Identity Cards for Foreign Nationals - Student and Marriage Categories |
| 06/2008 | Biometrics Assurance Group | Annual Report 2007 |
| 06/2008 | Identity and Passport Service | Annual Report and Accounts (for the year ended 31 March 2008) |
| 07/2008 | Home Office | Government reply to HAC report on a surveillance society |
| 08/2008 | UK Borders Agency | A Strong New Force at the Border |
| 08/2008 | Identity and Passport Service | mylifemyID Research Programme |
| 08/2008 | Central Office of Information | National Identity Scheme Tracking Research Wave 5: August 2008 |
| 09/2008 | Identity and Passport Service | Passport Validation Service: Financial Services Industry |
| 09/2008 | UK Borders Agency | Identity cards for foreign nationals: General guidance – Level 1 |

|  |  |  |
|---|---|---|
| 10/2008 | Identity and Passport Service | Identity Cards Scheme Cost Report November 2008 |
| 11/2008 | Identity and Passport Service | Identity and Passport Service: Front Office Services Prospectus |
| 11/2008 | Identity and Passport Service | Introducing the National Identity Scheme |
| 11/2008 | Jacqui Smith | Making identity cards a reality [speech at the Social Market Foundation] |
| 11/2008 | Identity and Passport Service | National Identity Scheme Delivery Plan 2008: A response to consultation |
| 11/2008 | Meg Hillier | Passport Validation Service [presentation] |
| 11/2008 | Duncan Hine | Passport Validation Service [presentation] |
| 11/2008 | Identity and Passport Service | Identity Cards Act Secondary Legislation: A Consultation |
| 11/2008 | Central Office of Information | National Identity Scheme Tracking Research Wave 6: November 2008 |

# Appendix 4

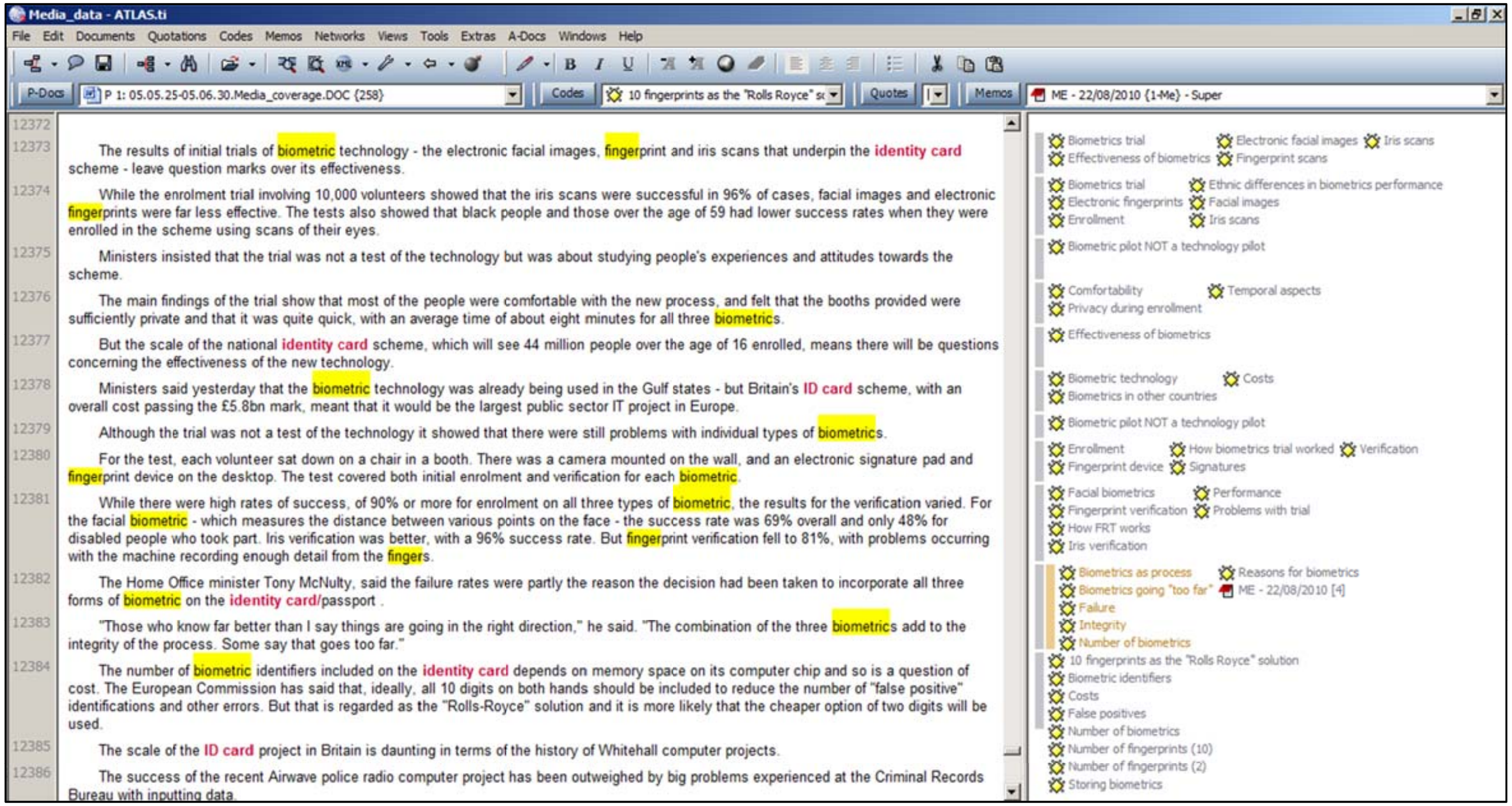
Hansard debates on biometrics in the NIS (selected around the 'critical moments' in the Scheme)

| Date | Venue | Subject |
|---|---|---|
| 13 June 2005 | House of Commons | Including DNA in ID cards |
| 20 June 2005 | House of Commons | Including DNA and medical information on the National Identity Register |
| 30 March 2006 | House of Commons | The questionable reliability of biometrics |
| 15 January 2007 | House of Lords | Obtaining iris scans and fingerprints from people in remote places for the new passport interview regime |
| 31 January 2007 | House of Commons | Whether iris biometrics would be included on new passports |
| 20 November 2007 | House of Commons | How biometrics would prevent the an HMRC-like data breach in the NIS |
| 21 November 2007 | House of Commons | How biometrics would provide identity fraud (post-HRMC) |
| 26 November 2007 | House of Commons | The revocability of biometrics |
| 28 November 2007 | House of Commons | The plausibility of 'card-not-present' biometric checks against the NIR |
| 17 November 2008 | House of Commons | The likelihood of on-line biometric checks against the NIR |
| 17 November 2008 | House of Commons | Whether the Home Office had estimated the number of false matches likely if fingerprint biometrics alone were used for the biometric verification in |

| | | |
|---|---|---|
| | | the Scheme |
| 17 November 2008 | House of Commons | On exception handling and fingerprint biometrics of elderly people |
| 20 November 2008 | House of Commons | About Home Office discussions with the police on the use of (fingerprint) biometric templates versus biometric images obtained via the Scheme |
| 24 November 2008 | House of Commons | On the government’s reasoning behind collecting 10 fingerprints from foreign nationals as opposed to 2 (as directed under European Commission regulations) |

# Appendix 5

Screenshot example of ATLAS.ti coding



Media_data - ATLAS.ti
File Edit Documents Quotations Codes Memos Networks Views Tools Extras A-Docs Windows Help
P-Docs
P 1: 05.05.25-05.06.30.Media_coverage.DOC {258}
Codes
10 fingerprints as the "Rolls Royce" sc
Quotes
Memos
ME - 22/08/2010 {1-Me} - Super

12372

12373 The results of initial trials of biometric technology - the electronic facial images, fingerprint and iris scans that underpin the identity card scheme - leave question marks over its effectiveness.

12374 While the enrolment trial involving 10,000 volunteers showed that the iris scans were successful in 96% of cases, facial images and electronic fingerprints were far less effective. The tests also showed that black people and those over the age of 59 had lower success rates when they were enrolled in the scheme using scans of their eyes.

12375 Ministers insisted that the trial was not a test of the technology but was about studying people's experiences and attitudes towards the scheme.

12376 The main findings of the trial show that most of the people were comfortable with the new process, and felt that the booths provided were sufficiently private and that it was quite quick, with an average time of about eight minutes for all three biometrics.

12377 But the scale of the national identity card scheme, which will see 44 million people over the age of 16 enrolled, means there will be questions concerning the effectiveness of the new technology.

12378 Ministers said yesterday that the biometric technology was already being used in the Gulf states - but Britain's ID card scheme, with an overall cost passing the £5.8bn mark, meant that it would be the largest public sector IT project in Europe.

12379 Although the trial was not a test of the technology it showed that there were still problems with individual types of biometrics.

12380 For the test, each volunteer sat down on a chair in a booth. There was a camera mounted on the wall, and an electronic signature pad and fingerprint device on the desktop. The test covered both initial enrolment and verification for each biometric.

12381 While there were high rates of success, of 90% or more for enrolment on all three types of biometric, the results for the verification varied. For the facial biometric - which measures the distance between various points on the face - the success rate was 69% overall and only 48% for disabled people who took part. Iris verification was better, with a 96% success rate. But fingerprint verification fell to 81%, with problems occurring with the machine recording enough detail from the fingers.

12382 The Home Office minister Tony McNulty, said the failure rates were partly the reason the decision had been taken to incorporate all three forms of biometric on the identity card/passport .

12383 "Those who know far better than I say things are going in the right direction," he said. "The combination of the three biometrics add to the integrity of the process. Some say that goes too far."

12384 The number of biometric identifiers included on the identity card depends on memory space on its computer chip and so is a question of cost. The European Commission has said that, ideally, all 10 digits on both hands should be included to reduce the number of "false positive" identifications and other errors. But that is regarded as the "Rolls-Royce" solution and it is more likely that the cheaper option of two digits will be used.

12385 The scale of the ID card project in Britain is daunting in terms of the history of Whitehall computer projects.

12386 The success of the recent Airwave police radio computer project has been outweighed by big problems experienced at the Criminal Records Bureau with inputting data

# Appendix 6

Raw codes from the analyzed government communications about biometrics in the National Identity Scheme (listed in order of frequency[27], starting with the most frequently used)[28]

| | |
|---|---|
| Fingerprints | 276 |
| Biometric information | 188 |
| Biometric passports | 145 |
| Recording biometrics | 130 |
| Costs of biometrics | 126 |
| Enrollment | 114 |
| Biometric data | 86 |
| Biometric checks | 77 |
| Storing biometrics | 74 |
| Biometrics as unique | 73 |
| Biometric visa | 70 |
| Foreign national biometric ID documents | 55 |
| International motivation for biometrics | 54 |
| Biometric identifiers | 53 |
| Verification | 50 |
| Facial image | 48 |
| Biometrics | 44 |
| Biometrics as securing identity documents | 41 |
| Digital photograph | 39 |
| Biometrics as preventing multiple identities | 38 |
| Enrollment centers | 38 |
| Biometric immigration documents | 37 |

[27] As this part of the analysis was focused around certain dimensions from Orlikowski and Gash's (1992) framework, the frequency of particular codes is only an approximate indication of their importance.

[28] I list these codes as documentation of my analysis, which is a quality criterion for qualitative research (Flick 2008; Bauer & Gaskell 2000, p.346)

| | |
|---|---|
| National Identity Register | 36 |
| Biometric technology | 35 |
| Fingerprint biometrics | 35 |
| Reliability (or unreliability) | 34 |
| Biometric readers | 34 |
| Biometrics in other countries | 33 |
| Biometric checks against the NIR | 32 |
| Iris patterns | 32 |
| Police access to biometrics | 30 |
| Infrastructure required for biometrics | 30 |
| Biometric residence permit | 29 |
| Temporal aspects | 29 |
| Asylum seekers' biometrics | 29 |
| Photo biometric (face) | 29 |
| Iris biometric | 29 |
| Other biometric information (i.e., not fingerprints) | 27 |
| Registering biometrics | 27 |
| Biometric standards | 26 |
| Facial recognition | 26 |
| Biometric details | 25 |
| Identity fraud | 24 |
| Public acceptance | 24 |
| Signature biometrics | 23 |
| Biometrics as strengthening identity checks | 22 |
| EU | 22 |
| Matching biometrics | 21 |
| Facial biometrics | 21 |
| Biometrics as "secure" | 21 |
| Awareness of biometrics | 21 |
| Biometric errors | 20 |
| Second-generation biometric passport | 20 |
| Biometric ID card | 20 |
| What biometrics is | 19 |

| | |
|---|---|
| Biometric technology trial | 19 |
| Technology pilots | 18 |
| Identity theft | 18 |
| Data security | 18 |
| Biometric database | 17 |
| Biometric enrollment requiring in-person meeting | 17 |
| ICAO | 17 |
| Examples of biometrics | 17 |
| Face biometrics | 16 |
| Public "understanding" | 16 |
| Online check | 16 |
| Biometrics as innovation | 16 |
| Religious aspects of biometrics | 16 |
| Iris image | 16 |
| Biometric identity cards | 16 |
| Benefits of biometrics | 15 |
| Biometric services | 15 |
| Cost-effectiveness of biometrics | 15 |
| Biometrics as the link between an identity (record) and a person | 15 |
| Disabled people | 15 |
| Scalability problems | 15 |
| Definition of biometric information | 15 |
| Convenience | 14 |
| Biometrics Assurance Group | 14 |
| Practicalities | 14 |
| Number of fingerprints taken (10) | 14 |
| Problems with enrollment | 14 |
| Security of biometrics | 14 |
| US-VISIT | 14 |
| Performance | 14 |
| Different types of biometrics | 14 |
| Biometric product | 13 |
| Biometrics as making it "easier" to prove identity | 13 |

|  |  |
|---|---|
| Marketing biometrics | 13 |
| High value transactions | 13 |
| Photograph biometrics | 11 |
| Creating a marketplace for biometric enrollment | 11 |
| US visa waiver program | 11 |
| Taking biometrics | 11 |
| Financial services and biometrics | 11 |
| Biometric enrollment services | 11 |
| Visual check | 11 |
| Public perceptions | 11 |
| Biometrics as preventing identity theft | 11 |
| Biometrics as a link | 11 |
| Biometrics as a physical characteristic | 11 |
| Spoofing biometrics | 10 |
| Biometric chip | 10 |
| Mobile biometric readers | 10 |
| Intrusiveness | 10 |
| Accessibility of biometric stations | 10 |
| Enrollment trial | 10 |
| Biometrics training for staff | 10 |
| False negatives | 10 |
| Technological maturity | 10 |
| Expertise | 10 |
| Privacy | 10 |
| Biodata | 9 |
| Police fingerprint databases | 9 |
| Iris recognition | 9 |
| Biometric checks by police | 9 |
| DNA as a biometric | 9 |
| Learning lessons about biometrics | 9 |
| Criminal connotations | 9 |
| Arguments against biometrics | 9 |
| Biometric e-Passport | 9 |

| | |
|---|---|
| Allow himself to be photographed | 9 |
| Biometric cards | 9 |
| Effectiveness of biometrics | 8 |
| Iris photograph | 8 |
| Vision | 8 |
| Iris scanning | 8 |
| Iris recognition immigration system (IRIS) | 8 |
| Expectations of biometrics | 8 |
| Biometrics as securing identity | 8 |
| Fingerprint scan | 8 |
| Risks of biometrics | 8 |
| Government data sharing of biometric data | 8 |
| Fingerprint images | 8 |
| False positives | 8 |
| Principles | 8 |
| Finger scans | 8 |
| Crime scene matching of NIS fingerprints | 7 |
| Cultural objections | 7 |
| Comfortability of biometrics | 7 |
| Biometrics as "personal" info | 7 |
| Elderly's problems with fingerprinting | 7 |
| Uses of biometrics | 7 |
| Biometrics as protecting identity | 7 |
| Exception handling | 7 |
| Facial photograph | 7 |
| Procurement | 7 |
| Iris biometrics as a *possibility* | 7 |
| Biometrics as inevitable | 7 |
| Biometrics as individuating | 7 |
| Accessibility of biometric data by employers or other agencies | 7 |
| Biometric ID | 6 |
| Biometric procedure | 6 |
| Mobile units | 6 |

| | |
|---|---|
| Biometric fingerprints | 6 |
| Privacy advocates' views | 6 |
| Biometric pilot | 6 |
| How biometrics work | 6 |
| Schengen area | 6 |
| Biometric travel documents | 6 |
| Biometric identity documents | 6 |
| Irises | 6 |
| Impermanence (mutability?) of biometrics | 6 |
| Biometric records | 6 |
| Accuracy | 6 |
| Biometrics as "identifying information" | 6 |
| Biometrics as increasing degree of assurance when proving identity | 6 |
| Offline check | 6 |
| Biometrics as personalised identifiers | 6 |
| Biometric driving licenses | 6 |
| Biometrics enabling Government to deal w/ threats to national security | 6 |
| Biometrics as a *possibility*, not a certainty | 6 |
| Operational aspects | 6 |
| One-to-one | 6 |
| Biometric capture | 6 |
| Complexity of recording biometrics | 6 |
| Interviews | 5 |
| Perceived effectiveness of biometrics | 5 |
| Accountability | 5 |
| Eye biometrics ("any other part of the eye") | 5 |
| Resistance to biometrics | 5 |
| Biometrics as securing link between document and holder | 5 |
| Secondary biometric (for travel docs) | 5 |
| Biometric image | 5 |
| Vulnerable groups | 5 |
| Biometrics as personal information | 5 |
| Primary biometric (for travel docs) | 5 |

| | |
|---|---|
| HMRC | 5 |
| Biometrics as making crime more difficult | 5 |
| Biometrics as linking people to a single identity | 5 |
| Photos as 'old' biometric | 5 |
| False identities | 5 |
| Biometrics as preventing duplicate identities | 5 |
| Fingerprint data | 5 |
| Biometrics as physical characteristics | 5 |
| Feasibility of doing biometrics | 5 |
| Biometrically-enabled | 5 |
| LSE | 5 |
| Biometric documents | 5 |
| Limitations of FRT | 5 |
| Encryption | 5 |
| Biometrically-challenged | 5 |
| Robustness | 5 |
| Biometrics as a "new" technology | 5 |
| Biometrics as "specific" identifiers | 5 |
| DNA as not an option | 5 |
| Definition of iris | 5 |
| Collecting biometrics | 5 |
| Level of assurance | 5 |
| One-to-many | 5 |
| "Plain" biometric identity cards | 5 |
| Ethnic differences in biometrics acceptance | 5 |
| Usability | 4 |
| Forgeability of biometrics | 4 |
| Biometric residence cards | 4 |
| System failure | 4 |
| Civil rights | 4 |
| Forensic applications of fingerprints | 4 |
| Biometrics as securing identity information | 4 |
| Biometric photographs | 4 |

| | |
|---|---|
| Biometrics as a "lock" | 4 |
| Biometric registration certificates | 4 |
| Biometrics as tackling illegal immigration | 4 |
| The "public" | 4 |
| Transsexuals | 4 |
| Biometrics as preventing false identities | 4 |
| Eye, the use of | 4 |
| Biometrics as identifying information | 4 |
| Biometrics as preventing fraudulent use of public services | 4 |
| Biometric systems | 4 |
| Facial recognition technology | 4 |
| Public approval | 4 |
| Fingerprint reader | 4 |
| Voice biometrics | 4 |
| Biometrics as unable to prevent terrorism | 4 |
| Biometrics as preventing illegal working | 4 |
| Expert opinion | 4 |
| Biometric capability | 4 |
| Iris scans | 4 |
| Biometric identity | 4 |
| National biometric identity service | 4 |
| Human rights | 4 |
| Relationship between the card, NIR and biometrics | 4 |
| Safety of iris scanning | 4 |
| How FRT works | 4 |
| Medical conditions | 4 |
| Biometric partners | 4 |
| Physical contact as problem with fingerprint systems | 4 |
| Able-bodied people | 3 |
| Biometric-based | 3 |
| Secondary usage | 3 |
| Environmental factors | 3 |
| Iris features | 3 |

| | |
|---|---|
| Biometric technology demonstration | 3 |
| Failure to acquire rates | 3 |
| Outsourcing biometrics | 3 |
| Biometrics as helping fight terrorism | 3 |
| Biometrics as relating to external characteristics | 3 |
| Restricting access to biometric data | 3 |
| Face recognition as unreliable | 3 |
| Retina | 3 |
| International sharing of biometric data | 3 |
| Interoperability | 3 |
| Digital facial image | 3 |
| Usefulness | 3 |
| Digital fingerprints | 3 |
| Consent | 3 |
| Uncertainty about biometrics | 3 |
| Definition of "fingerprint" | 3 |
| Biometrics as "data about his external characteristics" | 3 |
| Demand | 3 |
| Creating a market for biometrics | 3 |
| Quality of biometrics | 3 |
| National fingerprint register | 3 |
| Public communication | 3 |
| Efficiency | 3 |
| Biometrics as a safeguard of identity | 3 |
| Non-unique digital representations of biometrics (Crosby) | 3 |
| Legal dimensions of fingerprint analysis | 3 |
| UK Borders Act | 3 |
| Safety of biometrics | 3 |
| DNA profile | 3 |
| Children's biometrics | 3 |
| e-Borders | 3 |
| Problems with the pilot | 3 |
| Health risks of biometrics | 3 |

| | |
|---|---|
| Photograph of his head and shoulders | 3 |
| Suppliers | 3 |
| Biometric scanners | 3 |
| Hygiene | 3 |
| Information comprised in a fingerprint | 3 |
| Biometrics as possibly making identity theft worse | 3 |
| Biometric sensors | 3 |
| Human resources | 3 |
| Biometrics as linking card holder and identity owner | 3 |
| Biometrics as making it easier to check the age of customers | 3 |
| Availability of biometric stations | 3 |
| How iris works | 3 |
| Biometrics as making identity checks faster | 3 |
| Biometrics as helping reduce abuse of public funds | 3 |
| Reading biometrics | 3 |
| Age-related differences in biometrics acceptance | 3 |
| Biometrics as helping to prevent crime | 3 |
| Familiarity with biometrics | 3 |
| Biometrics as key to accessing personal record on register | 3 |
| Penalties | 3 |
| Biometrics as overkill (or not) | 3 |
| How fingerprint biometrics work | 3 |
| Fingerprint checks | 3 |
| Forensic v. civil systems | 3 |
| Biometric characteristics | 3 |
| NBIS contract | 2 |
| Biometrics as a "tie" | 2 |
| NIS SSF | 2 |
| Biometrics as not foolproof | 2 |
| Biometrics as link between your name and your NIR entry | 2 |
| Biometric enabled passport | 2 |
| Biometrics as not a new technology | 2 |
| Biometrics as "protecting" identity | 2 |

| | |
|---|---|
| Biometric ID as part of transformational government | 2 |
| When to use biometrics, or not | 2 |
| Misidentification | 2 |
| Biometrics as making financial fraud more difficult | 2 |
| Data ownership | 2 |
| Customers | 2 |
| Safeguarding biometric data | 2 |
| Biometrics as "strange" | 2 |
| Contracts | 2 |
| Potential of biometrics | 2 |
| Compulsion | 2 |
| Cost of biometric checks against a database | 2 |
| Public service delivery | 2 |
| Biometrics as making it more difficult to register false identities | 2 |
| Biometrics as making it easier to detect attempts to record duplicate identities | 2 |
| Biometric element | 2 |
| Public reaction | 2 |
| Biometrics as difficult to lose | 2 |
| Requirements | 2 |
| Biometrics as difficult to steal | 2 |
| Attitudes towards biometrics | 2 |
| Number of fingerprints taken (4) | 2 |
| Photograph (as identifying information) | 2 |
| Biometrics as difficult to forge | 2 |
| Biometrics as fixing a person to a single identity | 2 |
| Biometrics as preventing people attempting to "defraud the system" | 2 |
| Ownership of biometric data | 2 |
| Biometrics as fixing identity | 2 |
| Biometrics as discriminatory | 2 |
| Biometrics as strengthening verification procedures | 2 |
| Biometrics as enhancing the integrity of ID docs | 2 |
| Organizational experience | 2 |

| | |
|---|---|
| Regulating biometrics | 2 |
| Biometrics staff | 2 |
| Biometrics requiring face-to-face transactions? | 2 |
| Biometric checks as acceptable when doing "applications" | 2 |
| Biometrics as a replacement to PINs | 2 |
| Card-not-present biometric check | 2 |
| Refugee biometric ID | 2 |
| Blind people (and their problems w/ iris biometrics) | 2 |
| Biometrics as attributes | 2 |
| Biometrics as increasing confidence of identity checks | 2 |
| Biometrics Centre of Expertise | 2 |
| Number of fingerprints stored on passport (2) | 2 |
| Biometrics precluding online applications | 2 |
| Biometrics as an element of identity | 2 |
| Biometrics make it easier to detect attempts to record duplicate identities | 2 |
| Biometrics making it easier to re-document and deport people | 2 |
| Data Protection Act | 2 |
| Local authorities to do biometric recording | 2 |
| Long-term uses of biometrics | 2 |
| Facial digital photograph | 2 |
| Facial data | 2 |
| Specialist expertise required for biometrics | 2 |
| Technology refresh | 2 |
| (In)convenience of fingerprinting | 2 |
| Fingerprints as *optional*? | 2 |
| Strength of biometrics | 2 |
| Discrimination | 2 |
| Biometric support | 2 |
| Fingerprint visa | 2 |
| Malfunctions with biometrics | 2 |
| Ease | 2 |
| Immigration and Asylum Fingerprint System | 2 |

| | |
|---|---|
| Biometric identity systems | 2 |
| Eye scans | 2 |
| Exclusion | 2 |
| Biometric measures | 2 |
| Integrating biometrics | 2 |
| Fingerprint biometrics for asylum seekers | 2 |
| Second class (i.e. non-biometric) passports | 2 |
| Ethnicity as a biometric detail? | 2 |
| Approach to trialing biometrics | 2 |
| Biometric identities | 2 |
| Providing biometrics | 2 |
| Fingerprint identifiers | 2 |
| Biometric solution | 2 |
| Fingerprint pattern | 2 |
| Facial measurements | 2 |
| How iris biometrics are enrolled by computers | 2 |
| Unfamiliarity | 2 |
| Heat radiation | 2 |
| Facial recognition image biometric | 2 |
| Something you are | 2 |
| State-of-the-art | 2 |
| Differences in performance for different biometrics | 2 |
| Design specifications | 2 |
| Biometrics as "certain" | 2 |
| Mastering biometric technology | 2 |
| Differences in enrollment for different biometrics | 2 |
| Designer contact lenses interfering w/ iris | 2 |
| Hand geometry | 2 |
| Statistical probability | 2 |
| Digitized facial image | 2 |
| Identification | 2 |
| Biometrics (in ID cards) as helping to deter crime | 2 |
| Uniqueness | 2 |

| | |
|---|---|
| (Im)maturity of biometric technology | 2 |
| Digitized photograph | 2 |
| STORK | 2 |
| Digital representations of biometrics (Crosby) | 2 |
| Facial structure | 2 |
| Dead people's biometrics | 2 |
| Digitalized photograph | 2 |
| Administrative support required for biometrics | 2 |
| Biometrics as facilitating the passage of legitimate passengers and trade | 1 |
| Biometric marker | 1 |
| Biometrics as helping catch and deport foreign criminals | 1 |
| Biometrics as guarding identity | 1 |
| Biometrics as helping prevent multiple identity records | 1 |
| Biometrics as helping lower risk | 1 |
| Biometric as "a digital record" | 1 |
| Airside workers | 1 |
| Biometrics as linking an individual and his/her biographic information | 1 |
| AFIS | 1 |
| Biometrics as increasing security | 1 |
| Biometric scans | 1 |
| Awkwardness | 1 |
| Biometric passport chip malfunctions | 1 |
| Biometric pods | 1 |
| Biometric assets | 1 |
| Biometric recording equipment | 1 |
| Biometrics as identity data | 1 |
| Biometric passport cards | 1 |
| Algorithms | 1 |
| Biometrics as helping verify the identity of the holder against the document | 1 |
| Biometric data as "sensitive" | 1 |
| Biometric security | 1 |

| | |
|---|---|
| Biometric search | 1 |
| Audit trail | 1 |
| Biometric software | 1 |
| Biometrics as improving integrity of enrollment process | 1 |
| Biometrics as facilitating aliases for those in abusive relationships | 1 |
| Biometrics (in ID cards) as helping to detect crime | 1 |
| Biometrics as a form of protection | 1 |
| Biometrics 'stay with us continually' | 1 |
| Arguments against the use of fingerprints | 1 |
| Biometrics as a characteristic | 1 |
| Biometrics as a feature | 1 |
| Biometric ID register | 1 |
| Biometrics as a service | 1 |
| Biometric upgrade test | 1 |
| Biometrically verified | 1 |
| Biometric ID management | 1 |
| Biometrics as a physical process | 1 |
| Biometric functionality | 1 |
| Biometric features | 1 |
| Biometrics as "carried" by ID cards | 1 |
| Biometrics as "concept" | 1 |
| "Some form of recorded biometrics" | 1 |
| Biometrics as "locking down" identity | 1 |
| Biometric feasibility study | 1 |
| Biometrics as a "bind" | 1 |
| Biometric EU travel documents | 1 |
| "Reducing" biometrics to a barcode | 1 |
| Biometrics as 'added protection' | 1 |
| Biometrics are 'always with us' | 1 |
| "A third biometric" (iris) | 1 |
| Biometric lock | 1 |
| Biometrics as electronic records | 1 |
| Biometric-only check | 1 |

| | |
|---|---|
| Biometrics as detecting illegal immigrants | 1 |
| Biometrics as difficult to forget | 1 |
| Biometrics as external identifiers | 1 |
| Best practice (and what it means) | 1 |
| Biometric database as central to NIS | 1 |
| Biometrics as essential | 1 |
| Biometrics as excessive | 1 |
| Achievements | 1 |
| Biometrics as an unnecessary complication | 1 |
| Biometric identity register | 1 |
| Biometrics as barcoding | 1 |
| Biometric identification | 1 |
| Biometric testing (i.e., enrollment) | 1 |
| Biometrics as an emerging technology | 1 |
| Biometrics as countering identity fraud | 1 |
| Biometrics as creating efficiencies in public service delivery | 1 |
| "Customer experience" of biometrics | 1 |
| Biometrics as binding personal info to its owner | 1 |
| Atos Origin trial | 1 |
| Biometrics as clean | 1 |
| Media reportage | 1 |
| Mandating biometrics | 1 |
| Making biometrics work | 1 |
| Modern v. ink fingerprinting systems | 1 |
| Minimal disclosure | 1 |
| Merits of biometrics (in the context of fingerprinting 6 year olds) | 1 |
| Justification for collecting biometrics | 1 |
| Joining-up biometric systems | 1 |
| Irrevocability | 1 |
| Iris imaging | 1 |
| Large scale v. specialised biometric systems | 1 |
| Large-scale systems | 1 |
| Non-biometric details | 1 |

| | |
|---|---|
| Non-biometric cards | 1 |
| Need to test biometrics before system is given final approval | 1 |
| Objectives of biometrics pilot | 1 |
| Number for fingerprints to be recorded on the ID card (2) | 1 |
| NPL Feasibility Study | 1 |
| National biometric identification service | 1 |
| Multiple biometrics | 1 |
| Morality of biometrics | 1 |
| Need for universal biometrics | 1 |
| Necessity of a "definitive" database | 1 |
| National biometric identity scheme | 1 |
| Irreplaceability of compromised biometric images | 1 |
| Guarantees about biometrics | 1 |
| Gordon Brown | 1 |
| Giving biometrics | 1 |
| High volume transactions (making DNA an inappropriate biometric) | 1 |
| Hand biometrics | 1 |
| Gun crime | 1 |
| Front-end biometric services | 1 |
| Fingers | 1 |
| Fingerprints not mandatory (ICAO) | 1 |
| Geographical issues | 1 |
| Gender aspects | 1 |
| Future-proof | 1 |
| Iris picture | 1 |
| Iris digital photograph | 1 |
| Iris camera | 1 |
| Iris scan data | 1 |
| Iris recognition data | 1 |
| Iris readers | 1 |
| Inclusivity | 1 |
| Hospitals | 1 |
| Homeless | 1 |

| | |
|---|---|
| Intelligence services | 1 |
| Integrity (of the application process) | 1 |
| Innovations in iris biometrics | 1 |
| Strategic Action Plan | 1 |
| Stability of biometrics | 1 |
| Specific identifiers | 1 |
| Technology tests | 1 |
| Technological development | 1 |
| Technical challenges | 1 |
| Screening biometrics | 1 |
| Royal Mail | 1 |
| Risks | 1 |
| Sophistication of biometric databases | 1 |
| Service innovation | 1 |
| Security of biometric technology | 1 |
| Vagueness of legislative language | 1 |
| Use of biometrics limited in early stages of the scheme | 1 |
| Unique confirmation of identity | 1 |
| Volume | 1 |
| Video conferencing for remote communities | 1 |
| Validating biometrics | 1 |
| The process will be quick, easy and safe | 1 |
| Test population | 1 |
| Terrorism | 1 |
| Uncertainty | 1 |
| Thumbprint | 1 |
| The technology "works" | 1 |
| Retrieving biometrics | 1 |
| Portable fingerprint readers | 1 |
| Police biometric "services" | 1 |
| Plain fingerprint biometrics | 1 |
| Private sector organizations | 1 |
| Potential for fraud during enrollment | 1 |

| | |
|---|---|
| Potential for costs of biometrics to increase | 1 |
| People with "complex lives" | 1 |
| Passport Agency Support System (PASS) | 1 |
| Overconfidence in biometrics | 1 |
| Picture (biometric) | 1 |
| Physical process | 1 |
| Physical appearance as a biometric | 1 |
| Reducing fraud | 1 |
| Real-time biometric verification | 1 |
| Public understanding of science | 1 |
| Retinal patterns | 1 |
| Relationship between biometric passport and biometric ID | 1 |
| Regional offices | 1 |
| Proportionality | 1 |
| Probabilistic biometric matching technologies | 1 |
| Private sector use of biometrics | 1 |
| Public interest | 1 |
| Public engagement | 1 |
| Psychological effects | 1 |
| Biometrics as stronger proof of identity | 1 |
| Biometrics as strengthening integrity of passports | 1 |
| Biometrics as strengthening authentication processes | 1 |
| Biometrics as the real step change | 1 |
| Biometrics as the most secure way to fix an individual to a unique identity | 1 |
| Biometrics as the best proof of identity | 1 |
| Biometrics as securing identity records | 1 |
| Biometrics as securing financial transactions | 1 |
| Biometrics as saving police administrative costs | 1 |
| Biometrics as something the government must do "a duty" | 1 |
| Biometrics as simplifying verification | 1 |
| Biometrics as securing online transactions | 1 |
| Biometrics permitting automation of immigration controls | 1 |

| | |
|---|---|
| Biometrics of dead people | 1 |
| Biometrics learning curve | 1 |
| Border control philosophy | 1 |
| Biometrics support | 1 |
| Biometrics reducing the social and economic costs of crime | 1 |
| Biometrics as what secures an identity system | 1 |
| Biometrics as untried | 1 |
| Biometrics as the riskiest part of the scheme | 1 |
| Biometrics industry | 1 |
| Biometrics in other HO systems | 1 |
| Biometrics can only be registered to one identity | 1 |
| Biometrics as required to establish a person's "core identity" | 1 |
| Biometrics as permitting physical identification | 1 |
| Biometrics as part of a "triple ring" of border security | 1 |
| Biometrics as one of multiple modes | 1 |
| Biometrics as physical evidence | 1 |
| Biometrics as personal features | 1 |
| Biometrics as personal behavioral traits | 1 |
| Biometrics as non-sensitive | 1 |
| Biometrics as measurable | 1 |
| Biometrics as making it incredibly difficult to steal someone's identity | 1 |
| Biometrics as offshoring borders | 1 |
| Biometrics as nothing new | 1 |
| Biometrics as not preventing illegal immigration | 1 |
| Biometrics as proven technology | 1 |
| Biometrics as protecting personal information | 1 |
| Biometrics as protecting legal migrants | 1 |
| Biometrics as relating to physical features | 1 |
| Biometrics as quick | 1 |
| Biometrics as proving one's "bona fides" | 1 |
| Biometrics as preventing illegal migration | 1 |
| Biometrics as preventing identity exploitation | 1 |
| Biometrics as possibly replacing a password | 1 |

| | |
|---|---|
| Biometrics as protecting against identity theft | 1 |
| Biometrics as preventing asylum grantees from creating additional identities | 1 |
| Biometrics as preventing others from using one's ID card | 1 |
| Enhanced passports | 1 |
| Empowerment | 1 |
| Embarrassment | 1 |
| Ethical issues | 1 |
| Establishing identity with biometrics | 1 |
| Enrollment pilot | 1 |
| DNA analysis requires specialised skills | 1 |
| Digitally enlarged photograph appearing on a computer screen | 1 |
| Digital photographic image | 1 |
| Do biometrics work? | 1 |
| DNA as invasive | 1 |
| DNA as better than other biometrics | 1 |
| Eurodac | 1 |
| Fingerprint scanner | 1 |
| Fingerprint records | 1 |
| Fingerprint recognition | 1 |
| Fingerprinting by video conference | 1 |
| Fingerprint templates | 1 |
| Fingerprint technology | 1 |
| Facial characteristics | 1 |
| Face biometric as the only one required for biometric passport | 1 |
| Face (biometrics) | 1 |
| False matches | 1 |
| Failure to enroll | 1 |
| Facial hair | 1 |
| Competition (among biometric service providers) | 1 |
| Comparing biometrics | 1 |
| Commercial viability of biometric enrollment services | 1 |
| Consultation | 1 |

| | |
|---|---|
| Conflicting evidence | 1 |
| Complexity of biometric checks against a database | 1 |
| Capturing | 1 |
| Business volumes | 1 |
| Brandon Mayfield (?) | 1 |
| Complexity of multiple biometric databases | 1 |
| Claims of biased biometrics expertise (Mansfield) | 1 |
| Civil liberties | 1 |
| Database size | 1 |
| Data minimization | 1 |
| Data integrity | 1 |
| Difficulty of explaining biometric systems | 1 |
| Different types of fingerprint readers | 1 |
| Delays | 1 |
| Customer satisfaction | 1 |
| Continuity of biometric services | 1 |
| Contest of experts | 1 |
| CRB checks | 1 |
| Customer experience | 1 |
| Criteria for using biometrics | 1 |

# Appendix 7

Raw codes from the analyzed media communications about biometrics in the National Identity Scheme (listed in order of frequency[29], starting with the most frequently used)[30]

| | |
|---|---|
| Fingerprints | 108 |
| No mention of biometrics | 81 |
| Biometric passports | 51 |
| Biometric data | 46 |
| Iris scans | 37 |
| Costs | 36 |
| Biometric details | 27 |
| Storing biometrics | 27 |
| HMRC and NIS | 26 |
| National Identity Register | 26 |
| Biometric information | 21 |
| Biometrics and the HMRC data breach | 20 |
| Security | 16 |
| FNIDs | 16 |
| Reliability | 14 |
| Biometric technology | 13 |
| Biometric ID cards | 13 |
| Facial scans | 13 |
| Temporal aspects | 12 |
| DNA | 12 |

[29] As this part of the analysis was focused around certain critical events in the Scheme's history, the frequency of particular codes cannot be said to represent all newspaper coverage of the NIS.

[30] I list these codes as documentation of my analysis, which is a quality criterion for qualitative research (Flick 2008; Bauer & Gaskell 2000, p.346)

| | |
|---|---|
| Taking biometrics | 11 |
| Iris | 11 |
| Number of fingerprints (10) | 11 |
| Photograph | 11 |
| Royal Mail | 10 |
| NIS SSF | 10 |
| Ethnic differences in biometrics performance | 9 |
| Biometric pilot | 9 |
| Number of biometrics | 9 |
| Biometric database | 9 |
| Fingerprinted | 9 |
| Face scans | 8 |
| Failure rates | 8 |
| Enrollment | 8 |
| Enrollment centers | 8 |
| Biometric scans | 8 |
| Biometrics trial | 8 |
| International obligations | 8 |
| Readers | 8 |
| Re-enrolling biometrics | 7 |
| Biometric identifiers | 7 |
| Performance | 7 |
| Scanners | 7 |
| Fallibility of biometrics | 7 |
| Facial features | 7 |
| Terrorism | 7 |
| Fingerprinting | 7 |
| Data security | 7 |
| Accuracy | 7 |
| Uniqueness | 7 |
| Face | 7 |
| Biometrics | 7 |

| | |
|---|---|
| Iris pattern | 7 |
| Spoofing | 7 |
| Biometrics in schools | 7 |
| Effectiveness of biometrics | 7 |
| Surveillance | 7 |
| Electronic fingerprints | 6 |
| Elderly | 6 |
| Disabled people's biometrics | 6 |
| Recording biometrics | 6 |
| Irises as optional | 6 |
| Irrevocability of biometrics | 6 |
| Biometrics in other countries | 6 |
| Private sector | 6 |
| Compulsion | 6 |
| Failure | 5 |
| Fingerprint scans | 5 |
| Biometric identity cards | 5 |
| LSE | 5 |
| High street shops | 5 |
| Taking fingerprints | 5 |
| Photos | 5 |
| Biometric pilot NOT a technology pilot | 5 |
| Outsourcing biometrics | 5 |
| Examples of biometrics | 5 |
| Digital photograph | 5 |
| Verification | 5 |
| Biometric card | 5 |
| US | 5 |
| Biometric technology as new | 4 |
| Biometric register | 4 |
| Iris print | 4 |
| Identity theft | 4 |

| | |
|---|---|
| Age-related differences | 4 |
| Criminal connotations | 4 |
| Do biometrics work? | 4 |
| Accenture | 4 |
| Facial images | 4 |
| Forging biometrics | 4 |
| How FRT works | 4 |
| Facial recognition | 4 |
| The term 'biometric' | 4 |
| Quote by Blair re: biometrics | 4 |
| Problems with trial | 4 |
| Public resistance | 4 |
| Permanence of biometrics | 4 |
| Biometric enrollment services | 3 |
| Unions | 3 |
| Signatures | 3 |
| Iris technology | 3 |
| Fat fingers | 3 |
| STORK | 3 |
| Commercial confidentiality | 3 |
| Boots | 3 |
| Andy Burnham | 3 |
| Photographed | 3 |
| Creating a market | 3 |
| Biometric visas | 3 |
| False matches | 3 |
| Biometrics as securing identity (or not) | 3 |
| Errors | 3 |
| EU | 3 |
| Digital scan of the face | 3 |
| Fingerprint recognition | 3 |
| Visions | 3 |

| | |
|---|---|
| Biometrics companies | 3 |
| IBM | 3 |
| Number of fingerprints (2) | 3 |
| Iris scanning technology | 3 |
| Half-baked technology | 3 |
| Iris recognition | 3 |
| No2ID | 3 |
| BT | 3 |
| Biometric checks | 3 |
| Experts | 3 |
| Brown eyes (and problems with iris biometrics) | 2 |
| Biometric indicators | 2 |
| Fingerprint verification | 2 |
| Gordon Brown | 2 |
| Biometrics industry | 2 |
| Giving biometrics | 2 |
| Police state | 2 |
| Technical uncertainties | 2 |
| High-tech | 2 |
| Flaws with biometrics | 2 |
| Atos Origin | 2 |
| Tony Blair | 2 |
| Fujitsu Services | 2 |
| Fraud | 2 |
| Privacy | 2 |
| Purpose of biometrics | 2 |
| Advances in biometrics | 2 |
| Facial biometrics | 2 |
| Crime | 2 |
| Facial details | 2 |
| Eyes | 2 |
| David Blunkett (writing in the Times) | 2 |

| | |
|---|---|
| Registering biometrics | 2 |
| Electronic facial images | 2 |
| Eye scans | 2 |
| Experience | 2 |
| Airside workers | 2 |
| Collecting fingerprints | 2 |
| Comfortability | 2 |
| Children | 2 |
| Fingerprint device | 2 |
| Fingerprint details | 2 |
| Faking biometrics | 2 |
| Transsexuals | 2 |
| Contact lenses | 2 |
| Facial verification | 2 |
| Fake fingerprints | 2 |
| Resistance within the Labour party | 2 |
| Humor | 2 |
| Iris verification | 2 |
| Biometric security | 2 |
| IPS | 2 |
| Online biometric checks | 2 |
| Biometric testing | 2 |
| Big Brother | 2 |
| Multiple biometrics | 2 |
| Biometric certainty | 2 |
| Photo-style booth | 2 |
| Biometric systems | 2 |
| Success rate | 2 |
| Surveillance society | 2 |
| mylifemyid | 2 |
| Scanning biometrics | 2 |
| Scan of the iris | 2 |

| | |
|---|---|
| L-1 Identity Solutions | 2 |
| Photo-Me kiosk | 2 |
| Linking national DNA database to NIR | 2 |
| Standards | 2 |
| Illegal immigration | 2 |
| Identity fraud | 2 |
| Biometrics as securing identity documents | 2 |
| Biometric tech as "unstable" | 1 |
| Cross Match | 1 |
| Concerns about multi-modal biometrics in the NIS | 1 |
| Biometric tech as "experimental" | 1 |
| Biometric 'checks' | 1 |
| Biometric verification data | 1 |
| Biometric authentication | 1 |
| Biometric tracking | 1 |
| Biometric images | 1 |
| Crime-scene matching | 1 |
| Convenience | 1 |
| Biometrically excluded | 1 |
| Corrupting biometrics | 1 |
| Dermalog | 1 |
| Digital face scans | 1 |
| Biometric identity card system | 1 |
| 10 fingerprints as the "Rolls Royce" solution | 1 |
| Biometric residence permits | 1 |
| Biometric identity base | 1 |
| Digital scan of the iris | 1 |
| 'Sexing up' the system | 1 |
| Biometric enrollment fees | 1 |
| 'Unproven technology' | 1 |
| Biometric registration | 1 |
| Biometric security technology | 1 |

| | |
|---|---|
| Data sharing | 1 |
| Biometric services | 1 |
| CSC | 1 |
| Daon | 1 |
| Biometric identities | 1 |
| Daugman | 1 |
| David Blunkett (writing in the Sun) | 1 |
| A 'dialogue' about biometrics | 1 |
| Biometric identity | 1 |
| A scan of the (passport) holder's photo | 1 |
| Biometric fingerprint checks | 1 |
| BAG | 1 |
| Biometrics as markers of individual identity | 1 |
| Biometrics as personal data | 1 |
| Biometrics malarkey | 1 |
| Biometrics as making it difficult to misuse identity (but not impossible) | 1 |
| Blind people | 1 |
| Biometrics as genetic data | 1 |
| Biometrics as innovation | 1 |
| Bad Science article | 1 |
| Biometric frou-frou | 1 |
| Biometrics makes people feel confident | 1 |
| Biometrics in airports | 1 |
| Banks | 1 |
| Biometrics going "too far" | 1 |
| Biometrics as untested | 1 |
| Biometric photographs | 1 |
| Biometric fingerprints | 1 |
| Biometrics as process | 1 |
| Biometrics as physical details | 1 |
| Biometrics as sensitive | 1 |

| | |
|---|---|
| Biometrics as underpinning the ID card | 1 |
| Bald heads | 1 |
| Commercial actors | 1 |
| Biometrics as a 'ring-fence' | 1 |
| Biometrics as a recognition method | 1 |
| Cogent | 1 |
| Biometrics as a safeguard | 1 |
| Asylum seekers' biometrics | 1 |
| Biometrics about 'reading' people | 1 |
| Ambitiousness | 1 |
| Biometrics as 'global' | 1 |
| Biometrics as 'imperative' | 1 |
| Complexity | 1 |
| Civil liberties arguments (as phoney) | 1 |
| Builders | 1 |
| Biometrics as electronic data | 1 |
| Biometrics as foolproof | 1 |
| Benefits | 1 |
| Biometric recognition technology | 1 |
| Biometrics as certain | 1 |
| Chip-and-PIN as an alternative to biometrics | 1 |
| CISx | 1 |
| Celebrities' biometrics | 1 |
| Biometrics as a technical challenge | 1 |
| Capturing biometrics | 1 |
| Digitized facial scan | 1 |
| Picture | 1 |
| Photographing | 1 |
| Police | 1 |
| Pictures of their irises | 1 |
| Orwellian | 1 |
| Organizational change | 1 |

| | |
|---|---|
| People with dark eyes | 1 |
| Passing data | 1 |
| Politicians' (lack of) understanding about biometrics | 1 |
| Record of their face | 1 |
| Reasons for biometrics | 1 |
| Relationships between biometrics and national identity | 1 |
| Relationship between cards, databases, and biometrics | 1 |
| Privacy International | 1 |
| Privacy during enrollment | 1 |
| Public acceptance | 1 |
| Providing biometrics | 1 |
| miSense | 1 |
| Microsoft | 1 |
| Mobile enrollment centers | 1 |
| Misunderstanding | 1 |
| Limitations of fingerprints (Daugman) | 1 |
| Liberty | 1 |
| Meg Hillier | 1 |
| Managing biometrics | 1 |
| Morality | 1 |
| Nose-to-chin distance | 1 |
| Nick Clegg | 1 |
| Online authentication | 1 |
| Nothing to hide | 1 |
| Multiple identities | 1 |
| Motorola | 1 |
| NEC | 1 |
| NAO e-passport report | 1 |
| Totalitarian state | 1 |
| Tony Blair, against ID cards (1996) | 1 |
| UKPS | 1 |
| Triple check (?) | 1 |

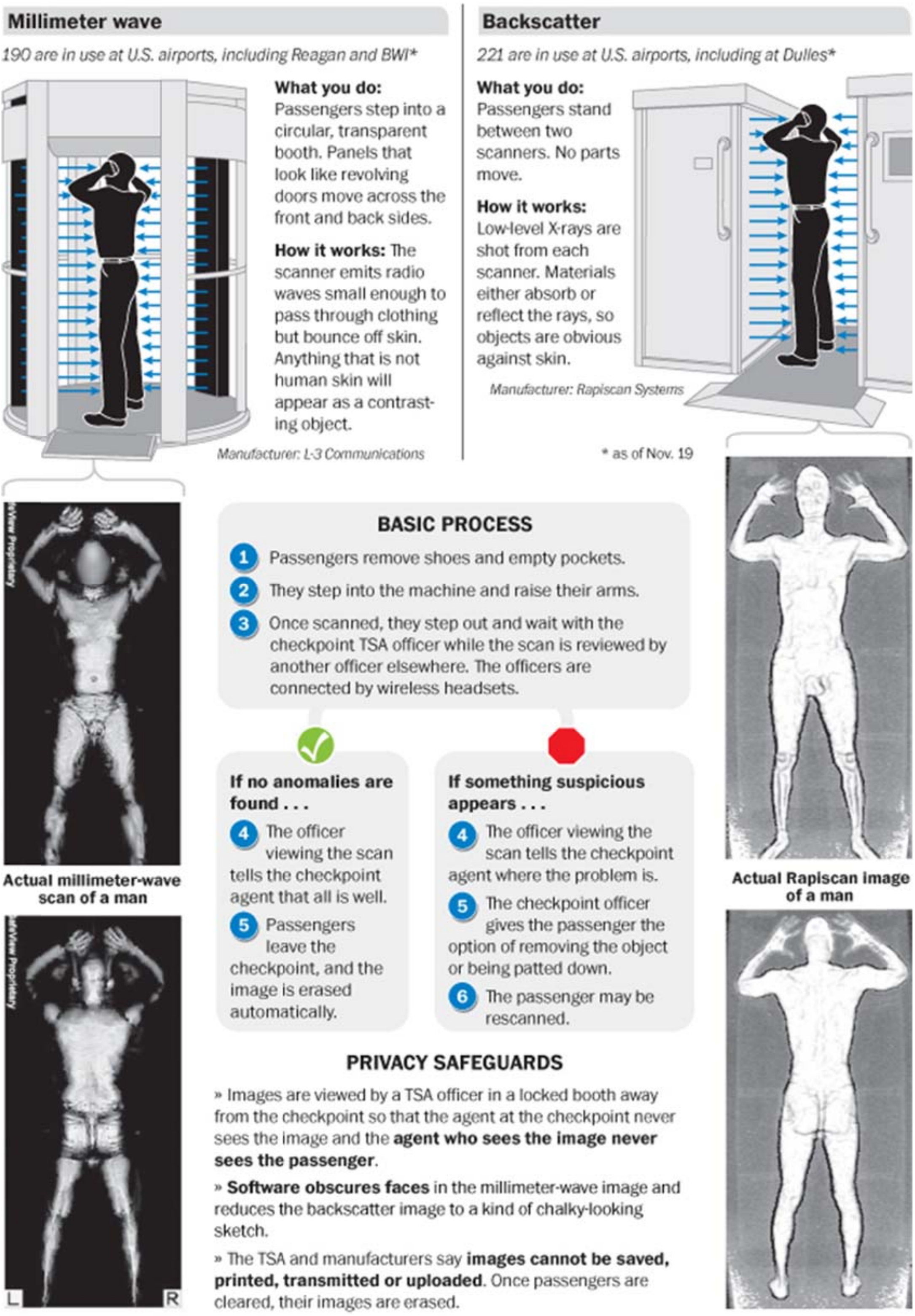
| | |
|---|---|
| The eye | 1 |
| Teething problems | 1 |
| Three parts of the body | 1 |
| The public | 1 |
| Unpopularity of fingerprinting | 1 |
| Values | 1 |
| Value for money | 1 |
| Voluntariness | 1 |
| Visual check | 1 |
| US-VISIT | 1 |
| Untried technology (iris) | 1 |
| Using biometrics | 1 |
| US visa waiver program | 1 |
| Sarcasm | 1 |
| Sagem | 1 |
| Scanning machines | 1 |
| Scan of the eye | 1 |
| Replicating biometrics | 1 |
| Replacing fingerprints (because of an accident) | 1 |
| Robustness | 1 |
| Retina | 1 |
| Schengen | 1 |
| Stealing biometric data | 1 |
| So-called "biometrics" | 1 |
| Tamper resistance | 1 |
| Supermarkets | 1 |
| Separating design and implementation | 1 |
| Science | 1 |
| Sir Ian Blair | 1 |
| Siemens | 1 |
| Lack of justification | 1 |
| Facial technology | 1 |

| | |
|---|---|
| Facial recognition systems | 1 |
| False fingerprints | 1 |
| False enrollment | 1 |
| Facial recognition maps | 1 |
| Facial readings | 1 |
| Facial recognition software | 1 |
| Facial recognition scan | 1 |
| Fingerless people | 1 |
| Financial fraud | 1 |
| Fingerprint booths | 1 |
| Fingerprint biometrics | 1 |
| False non-matches | 1 |
| False identities (and how biometrics can't prevent them) | 1 |
| Fears about biometrics | 1 |
| False positives | 1 |
| Facial measurements | 1 |
| Electronic biometrics | 1 |
| EDS | 1 |
| Encoding biometrics | 1 |
| Electronically scanned facial image | 1 |
| Distance from your nose to your chin | 1 |
| Discrimination | 1 |
| E-government failure | 1 |
| Distances between facial features | 1 |
| Facial biometric technology | 1 |
| Face maps | 1 |
| Facial imaging | 1 |
| Facial data | 1 |
| Expertise | 1 |
| Expectations | 1 |
| Face-shape | 1 |
| Eye recognition | 1 |

| | |
|---|---|
| Fingerprint data | 1 |
| Insecurity | 1 |
| Imprint of your irises | 1 |
| Integrity | 1 |
| Inside leg measurement as a biometric | 1 |
| Implementation | 1 |
| Images of irises | 1 |
| Impressions of the their (the terrorists') irises | 1 |
| Impression of the iris of your eye | 1 |
| Interoperability problems | 1 |
| Irises scanned | 1 |
| Iris scanners | 1 |
| John Reid 'answers' questions about the NIS | 1 |
| Jacqui Smith | 1 |
| Iris recognition immigration system (IRIS) | 1 |
| Iris biometrics | 1 |
| Iris scanned | 1 |
| Iris scan technology | 1 |
| Human rights | 1 |
| Fingerprint scanning technology | 1 |
| Gathering biometrics | 1 |
| Glasses | 1 |
| Fingerprint scans at borders | 1 |
| Fingerprint technology | 1 |
| Fingers | 1 |
| Fraudulent use of public services | 1 |
| How biometrics trial worked | 1 |
| Fingerprint recording database | 1 |
| How iris biometrics works | 1 |
| House of Lords | 1 |
| Hands | 1 |
| Fingerprint records | 1 |

# Appendix 8

Basic overview of full-body imaging technologies (Washington Post 2010)



**Millimeter wave**

*190 are in use at U.S. airports, including Reagan and BWI**

**What you do:** Passengers step into a circular, transparent booth. Panels that look like revolving doors move across the front and back sides.

**How it works:** The scanner emits radio waves small enough to pass through clothing but bounce off skin. Anything that is not human skin will appear as a contrasting object.

*Manufacturer: L-3 Communications*

**Backscatter**

*221 are in use at U.S. airports, including at Dulles**

**What you do:** Passengers stand between two scanners. No parts move.

**How it works:** Low-level X-rays are shot from each scanner. Materials either absorb or reflect the rays, so objects are obvious against skin.

*Manufacturer: Rapiscan Systems*

* as of Nov. 19

**Actual millimeter-wave scan of a man**

**Actual Rapiscan image of a man**

**BASIC PROCESS**

1. Passengers remove shoes and empty pockets.
2. They step into the machine and raise their arms.
3. Once scanned, they step out and wait with the checkpoint TSA officer while the scan is reviewed by another officer elsewhere. The officers are connected by wireless headsets.

**If no anomalies are found . . .**

4. The officer viewing the scan tells the checkpoint agent that all is well.
5. Passengers leave the checkpoint, and the image is erased automatically.

**If something suspicious appears . . .**

4. The officer viewing the scan tells the checkpoint agent where the problem is.
5. The checkpoint officer gives the passenger the option of removing the object or being patted down.
6. The passenger may be rescanned.

**PRIVACY SAFEGUARDS**

» Images are viewed by a TSA officer in a locked booth away from the checkpoint so that the agent at the checkpoint never sees the image and the **agent who sees the image never sees the passenger**.

» **Software obscures faces** in the millimeter-wave image and reduces the backscatter image to a kind of chalky-looking sketch.

» The TSA and manufacturers say **images cannot be saved, printed, transmitted or uploaded**. Once passengers are cleared, their images are erased.