

## CONTENTS

---

<i>List of Figures and Tables</i>	viii
<i>List of Abbreviations</i>	ix
<i>Acknowledgments</i>	xii
<i>Series Preface</i>	xiii
<i>Preface</i>	xvii
<b>1 The challenge of identity policies</b>	<b>1</b>
<b>2 A review of national identity policies</b>	<b>22</b>
<b>3 The life cycle of identity policy in the United Kingdom</b>	<b>74</b>
<b>4 The proposed National Identity Scheme for the United Kingdom</b>	<b>96</b>
<b>5 Due process and short-circuiting debate</b>	<b>124</b>
<b>6 Due process and the politics of science and technology</b>	<b>142</b>
<b>7 Intentional ambiguity about technology</b>	<b>154</b>
<b>8 Technological expertise and decision-making</b>	<b>178</b>
<b>9 The Scheme five years on</b>	<b>191</b>
<b>10 The prospects for effective identity policies</b>	<b>209</b>
<i>Methodological appendix</i>	238
<i>Glossary</i>	244
<i>References</i>	247
<i>Index</i>	281

## CHAPTER 1

---

# The challenge of identity policies

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

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

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

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

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

as roadworthy. In this case, the innovative use of technology leverages the process to mitigate the need to present and authenticate various paper documents before paying the tax.

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

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

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

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

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

account,” or “I am old enough to buy alcohol”). The next section examines how identification and authentication raise particular challenges for contemporary life.

## **Identity policies for a modern society**

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

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

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

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

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

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

Ella is 18 and wants to buy some wine from an off-licence to take to a party. Cynthia is a youthful 70 and is keen to claim an “over-65” discount offered at her local garden centre. In each case the retailer could ask for proof of age. As both Ella and Cynthia have an ID card, they do not need to show:

- birth certificate
- pension book
- driving licence
- or any other documents that might be requested to prove identity.

Instead each of them can simply hand over their ID card. In this case the retailers will simply:

- look at both sides of the card checking for the security features, then
- compare Ella or Cynthia with their photograph on the card.

If the retailers are satisfied that the ID cards are genuine and that they each belong to the person using them, they will then check the dates of birth to confirm their ages. It takes just moments for the check to be completed so that Ella can buy the wine and Cynthia can claim her discount.

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

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

At first sight, a solution based on the presentation of an identity card provides a straightforward mechanism for verifying one’s age so that suitable access to age-related services and discounts can be received and prevents

the necessity of carrying multiple identity-related documents that can be easily mislaid or stolen.

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

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

## **Political drivers of identity policies**

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

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

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

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

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

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

knowledge about people, such as their biometrics, is required for an effective identity assurance scheme to operate?

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

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

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

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

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

policy is such a delicate domain that it requires individualized and culturally sensitive solutions.

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

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

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

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

Many governments around the world are now trying to reassess their identity policies in light of technological changes. What used to be simple tasks like opening bank accounts or paying for items over the phone are now threatened by the rise of identity-related fraud. These incidents range from the fraudulent use of an individual's identity to open credit accounts, withdraw cash, or purchase goods to fraudulently using corporate identities and registered details. In extreme cases, individuals may be held in jail

because crimes have been committed by someone matching “their” identity (Whitley and Hosein, 2008). Identity fraud may then turn into a terrorism risk when terrorists are able to get identity documents in the names of other people or travel between countries using multiple identities; into an immigration risk as illegal immigrants can assume the identity of a citizen; into a risk to commerce and e-government as organizations cannot have confidence in the identity of the individuals with whom they are dealing; and into a drop in consumers’ and citizens’ confidence when their identities are at risk of abuse.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

### **Who should be responsible for addressing identity fraud?**

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

#### **Private individuals**

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

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

emphasis added) and “What if it happens *to you*” (Identity Theft, 2009b, emphasis added).

### Private sector companies

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

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

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

### Government and the public sector

As was noted above, there is a general recognition that public policy has an important role to play in addressing issues of identity fraud. This can

range from specifying legislation about identity fraud to encouraging best practice in industry. Moreover, as a holder of significant personal data for most aspects of policy delivery (Dunleavy et al., 2006), the public sector has the opportunity to “lead by example” with respect to the secure handling of personal data.

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

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

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

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

## **A technological policy to address identity fraud**

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

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

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

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

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

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

Another technological policy response to identity fraud might be to introduce a policy of data minimization (Home Affairs Committee, 2008; Sir James Crosby, 2008) whereby “as a matter of principle, the amount of data stored should be minimized.” This means that “in the design of its policies and systems for collecting data, the Government should...collect

only what is essential, to be stored only for as long as is necessary” as data that are not held cannot be breached and cannot lead to problems of identity fraud. Implementing data minimization, however, will require extensive redesign of both systems and work practices and so may be better suited to the design of new systems rather than existing systems.

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

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

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

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

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

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

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

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

are often less secure than data that are known to be sensitive (Verizon Business, 2008).

## Implications

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

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

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

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

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

## Overview of the book

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

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

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

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

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

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

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

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

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

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

## INDEX

Unless otherwise specified, all items relate to issues surrounding the UK Identity Cards Scheme. For identity policies in particular countries, see Identity policies, country name.

- Academic policy engagement 80, 230–6  
*See also* Action Research
- Action research 235–6
- Administrative convergence 7, 97, 110
- Advocacy laundering 219
- Airports, Wave One of implementation 94, 192–4, 200  
*See also* Transportation worker identification credential (TWIC)
- Audit trail 105–6, 146–7, 198  
 Designed into legislation 220
- Authentication  
 Defined 2  
*See also* identification
- Benefits of the Scheme oversold 99
- Burnham, Andy  
 On LSE “Marketing costs” 83–4  
 On what the reported costs of the Scheme include 172–3
- Biographical enrolment  
*See* Enrolment biographical
- Biometric enrolment  
*See* Enrolment biometric  
*See* Front Office Services
- Biometrics  
 Error rates 102  
 Face 6, Chapter 2, 100, 102, 103, 112, Chapter 5, 146, 148, 196, 199, 220, 234  
 Fingerprint 6, Chapter 2, 86, 87, 89, 90, 97, 102, 103, 105, 112, Chapter 5, 148, 150, 154, 165, 196–8, 199, 220, 229, 234  
 Iris 6, 65, 70, 88, 97, 102, 103, 112, 130, 131, 137–8, 139, 148, 152, 196, 199, 220
- Blair, Tony 72, 80, 129, 233
- Blunkett, David 76
- Brown, Gordon 91, 221
- Cameron, David 79, 94–5
- Child Benefit Data  
*See* Her Majesty’s Revenue and Customs
- Chip and PIN 104, 105
- Citizens Information Project (CIP) 115, 116, 202–3
- Clarke, Charles 27, 99, 104, 116–17, 127, 128, 135–6, 137, 163–4, 167, 168, 170, 182, 184  
 On LSE Identity Project 81, 82
- Clarkson, Jeremy 18
- Compulsory and voluntary enrolment Chapter 7
- Constitution Committee (House of Lords)  
 Inquiry into surveillance 93–4
- Contests of experts 149–51
- Costs  
 Home Office estimates 107, 128, 170, Chapter 7, 195, 197  
 LSE estimates 81, Chapter 7  
 Of consultants 1  
 Reporting to Parliament  
*See* s.37 cost reports
- Criminal Records Bureau 90, 114, 117
- Crosby Review 91–3, 221–2
- Data breach  
*See* Her Majesty’s Revenue and Customs (HMRC)
- Data minimization 16–17, 226–7
- Davies, Simon 82, 172, 237
- Davies, Sir Howard 82
- Davis, David 79, 94, 95, 165, 169, 184
- Delivery plan (2008) 92, 93, 186–7, 191–2  
*See also* Strategic Action Plan (2006)
- DNA 139
- Due process  
 Policy laundering Chapter 5  
 Science and technology Chapter 6
- Driver and Vehicle Licensing Agency (DVLA) 77, 117–20

- Enabling legislation 96, 199, 219–22
- Enrolment
- Biographic 82, 89, 100–1, 107, 192, 195, 197, 200, 207, 226
  - Biometric 17, 85, 107, 191, 192, 195, 197, 200, 201, 220, 222, 229
  - Compulsory versus voluntary Chapter 7
  - Centres 101
- Entitlement cards 76–8, 106, 210
- Facts versus values 143–5, 211, 215
- Flash and go 16, 103–4
- Front Office Services 191, 195, 197, 201, 207
- Gateway reviews 77, 94, 115, 120, 138, 183, 203, 213–14, 219
- General Register Office (GRO) 75, 203
- Hall, James 188, 203
- Her Majesty's Revenue and Customs 90–1
- Home Affairs Committee (HAC)
- On draft bill 23–4, 33, 43, 79, 104, 146
  - On surveillance society 93–4, 115, 226
- Home Secretary
- See* David Blunkett, Charles Clarke, John Reid, Jacqui Smith
- Identification
- Defined 2
  - See also* authentication
- Identity and Passport Service (IPS)
- Creation 85
  - See also* Strategic Action Plan, Strategic Supplier Group, Delivery Plan
- Identity card
- Cost in Europe 25
- Identity Cards Scheme compared to National Identity Scheme 85–7
- Identity Commissioner
- See* Scheme Commissioner
- Identity fraud 8–19
- Identity policies
- Austria 24–5
  - Australia 47–51
  - Belgium 25–6
  - Canada 51–4
  - China 60–1
  - Common Travel Area (UK and Ireland) 36–8
  - Estonia 26–7
  - EU initiatives 43–5
  - France 27–32
  - Germany 32–4
  - Greece 34–5
  - Hong Kong 61–2
  - Hungary 35–6
  - India 62
  - Ireland 36–8
  - Italy 38–9
  - Japan 62–3
  - Malaysia 63–4
  - Middle East 64–5
  - The Netherlands 39–42
  - Philippines 65–6
  - Spain 42–3
  - Sweden 43
  - Taiwan 67–8
  - Thailand 68–9
  - United States of America 54–60
- Infrastructure
- Identity infrastructure 109, 120, 123, 185–6, 189
  - Information infrastructure 110–14
- Informed advocate 152, 155, 216–17, 236–7
- Installed base 112–13, 200
- Intentional ambiguity Chapter 7, 216–17
- International Civil Aviation Organization (ICAO) 44–5, 53, 126–40, 154, 198, 204, 206, 214, 227, 233
- Joined up implementation 120–1, 193–4
- KPMG Report on costs 171, 181, 213, 241
- Latour's new division of powers 145
- Leaked plans 90, 91, 192
- LSE Identity Project 79–83
- Mackenzie's uncertainty trough 188
- Manifestos 162–8
- Marketing costs
- See* Andy Burnham on LSE marketing costs
- National Identity Register
- Security risks 81, 146–7
  - Verification against 72, 97, 103, 104, 105, 112, 117, 198, 199, 201, 221
- National Identity Registration Number (NIRNo) 97, 198, 219
- National Identity Scheme compared to Identity Cards Scheme 85–7
- National Institute of Standards and Technology (NIST) 148, 150
- National Insurance Number (NINo) 15, 18, 91, 101, 110

- National Programme for IT (NPfIT) 188  
NO2ID 79, 90, 91, 92, 192, 193
- Overflows 9
- Passports  
70% of the costs of the identity card associated  
with passports 106, 129, 136, 137  
Application form 197, 207  
Roll out with identity cards 93, 106–7, 117,  
126, Chapter 7, 191–3, 200  
Withdrawal 205
- Paying for the Scheme 116–20, 201
- Perplexities Chapter 6
- Ping pong (Parliamentary) 85, 165, 169
- Policy laundering 125–6, 141, 214–15  
*See also* advocacy laundering
- Politics of Nature (Latour) 143, 152
- Procurement  
*See* Strategic Supplier Group
- REAL ID (U.S.) 17, 54–6
- Regulatory impact assessment 155, 170
- Relying party 218, 223, 225–7
- Rigor and relevance 234–5
- s.37 (cost) reports 221, 242
- Salisbury Convention 162
- Schengen Area 44–5, 129, 133–8, 233–4
- Scheme Commissioner 83–6, 192
- Science and Technology Select Committee  
Inquiry 87, 184–5, 189, 199
- Science and technology studies (STS) 144–5, 187
- Smith, Jacqui 1
- Social Security Number (U.S.) 15–16, 34  
For the UK, *see* National Insurance  
Number
- Strategic Action Plan (2006) 87–8, 185–6
- Strategic Supplier Group 88–90
- Sir James Crosby  
*See* Crosby review
- Technology neutral policies 220–2
- Transportation worker identification  
credential 54, 56–7
- Unmatched crime scene prints 92, 115, 199
- US-VISIT 56–60, 127
- USA-PATRIOT ACT 57, 130, 134
- Verification  
Online versus offline 103–4
- Vetting 90, 196, 226
- Values versus facts  
*See* facts versus values
- Voluntary and compulsory enrolment Chapter 7
- Wartime cards 74–6
- Young people 4, 90, 93, 193

PROOF