Global Identity Policies and Technology: Do we Understand the Question?

Edgar A. Whitley and Gus Hosein

London School of Economics and Political Science

Survey Article

Abstract

Why do we get technology policy so wrong, so often? As governments rush to develop new identity policies they fail too often in answering essential questions: are identity policies capable of addressing a diverse range of policy goals? Are the techniques we imagine to be necessary in fact helpful? Instead, policy makers remain fixated on expensive and sexy 'biometrics' and vast new centralised databases to solve problems they do not understand. This survey seeks to resolve why policy makers repeatedly commission identity schemes based on obsolete knowledge of modern technological capabilities. We argue that policy making requires an understanding of technological issues as well as more traditional political and organisational concerns, and a little less bravado. As a result, policy makers can set about developing effective solutions that are citizen friendly and actually address pressing policy goals.

When faced with global migration, terrorism and crime, fraud and the modernisation of public services, governments are nearly unanimous in their silver bullet: identity policy. For example, the Indian government is planning to implement a Unique Identification Number for its billion-plus citizens backed up by biometric authentication in order to regulate access to government services (Unique Identification Authority of India, 2009); in the fight against terrorism, countries as diverse as Greece, Pakistan, South Africa and Spain have introduced requirements on mobile phone providers to ensure that 'prepay' mobile phones are linked to an identification document (Haines, 2009); for the management of borders and the movement of people, the Office of the UN High Commissioner for Refugees (UNHCR) is trialling the use of fingerprint biometrics to manage refugee populations, and recently Rwanda has announced that all refugees will be issued with identity cards (Asiimwe, 2009). Less than a decade ago these policies would have been unthinkable, not least because of a lack of political will and because 'identity technologies' were not as commonplace as they are now. Identity policies now encompass a broad range of policy activity in practically every country in the world.

Without a clear understanding of this complex area, potential benefits of identity policies will be quickly outweighed by the political, social and technological risks (Whitley and Hosein, 2010). As the Australian and British governments have discovered, an ill-thought-out identity policy can become a political and even electoral liability. As other countries have recognised, identity policy can also become a financial and technological albatross. In fact, it remains unclear how policy makers see identity policies: are they imagining identity policy as the traditional issuance of identity cards using new and exciting techniques? Do they see only great opportunities behind new technologies, often without seeing the risks? In our experiences and research, we are worried that policy makers too often believe that there is no limit to what an identity policy can achieve.

As with all modern policy domains an understanding of the technological details is necessary. Reading manuals and scientific articles may not be a politician's idea of preparation for a parliamentary debate but effective deliberation of modern policy issues, particularly identity policy, hinges on a careful understanding of the technologies implicated in making a policy a reality. All too often, however, terms like 'biometrics', 'contactless chips' and 'smart cards' are perceived by politicians and policy makers as panaceas for all the complexities associated with identification when in practice they are a shorthand representation of complex and diverse technological issues. As a result, a government's strategy on identity policy tends to focus on the notion of the state issuing 'biometric identity cards' to its population. We argue that such an approach may actually undermine many of the useful benefits of an effective identity policy.

The purpose of this article is therefore to unpack some of the choices that underlie existing and future policies. The policy challenge, accordingly, is to agree on the requirements of a policy that includes effective consideration of technological issues and choices. We do so by reviewing the key challenges faced by governments and their identity policies in a global environment. The next

section therefore introduces the challenges of implementing an effective identity policy and some of the key concepts underlying identity policies before examining critically some of the most commonly claimed drivers for identity policies and the policy processes that are currently driving identity policy. The article ends with specific recommendations for policy makers in this area.

Key concepts in identity policies

Too often the complexity of implementing an identity policy is concealed through the undefined and indeterminate use of concepts including *identification*, *biometrics*, *enrolment* and *verification*. Despite commonly held beliefs, not all transactions require identification. Aspirations aside, the performance issues relating to biometrics may limit their applicability for some kinds of transactions, environments and populations. Counter to the ambitions of some government departments and vendors, identity schemes do not have to be based on the storage of biometrics on centralised databases. Finally, decisions about how to enrol and verify individual identities directly influence the effectiveness of the policy in addressing particular policy objectives.

The challenge of implementation

Policy implementation is always challenging but identity policies raise particular challenges as they require explicit consideration of scientific and technological issues, the 'missing' elements of much social theory (Latour, 1992). Our political and legal systems of deliberation are set up to consider economic, financial, social and legal issues, but are poorer at considering and evaluating 'things'. When policy makers consider these 'things', they often take a 'thing-centric' approach, which often results in 'identity cards', 'DNA databases' and 'biometrics'. Without an understanding of the inherent complexities of the things as we described above and an equivalent understanding of how these 'things' integrate into existing policies and practices, the policies are, in our experience, very likely to fail.

Sometimes these policies may not be reliant strictly on science and technology, but on equally hard issues like available infrastructure and systems. Common problems of coordinating systems across government departments can result in inconsistent identity policies being applied. For example, an immigration department may wish to limit student visas to those studying on recognised courses but this requires that the education department has proactive oversight of 'registered' institutions which ensures that they are not used as fronts for illegal immigration and that there is an effective network of biometric enrolment centres for prospective students (BBC News, 2009; Manifesto Club, 2010).

Similarly, a decision to base identification on documents that are intended for other purposes might result in unintended consequences. For example, plans for US states to issue enhanced driving licences as an identity card (the 'REAL ID' programme) have been criticised for simply creating an underclass of individuals who are driving without driving licences. Alternatively, issuing 'driving licences' to all would mean that decisions over who is a legitimate citizen are suddenly delegated to the driver's licence authority (Rotenberg, 2006).

Technological implementation decisions also include choices of how and where to store the underlying identity information. For example, the political decision to base an identity policy around a single, centralised database might offer the prospect of being able to focus security protections on the database, but it also means that the database becomes increasingly vulnerable as a natural target for hackers (Fishenden, 2005). A centralised database also raises the risk of catastrophic data breaches, as all the data are held in one place (cf. Perrow, 1984). Finally, a single error in a central database will permeate an entire society as other institutions grow to rely on the data held therein: a failure to register an individual will result in that individual being excluded from society, while a successful but fraudulent registration could result in irrevocable abuse (Berghel, 2006).

Identification and authentication

Although most policies are described in terms of *identification*, in practice many identity transactions are more accurately described in terms of *authentication* (Smith and Clarke, 2000). Identification is taken as 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 authorised to engage in or perform some activity ('I am allowed to withdraw money from this bank machine' or 'I am a citizen and may enter the country' or 'I am allowed to drive a car').

In each case, the 'relying party' in a transaction (which might be a commercial organisation or the 'service' side of government) needs to know that the 'individual' presenting him- or herself is who or what they claim to be. They also need to know the basis of this claim, that is, who is the 'identity service provider' that supports the claim? In the examples above, this could be the individual's bank, passport office and driver's licence authority, respectively. These transactions in turn may depend on the appearance of the individual, the quality of the credential (e.g. the card or passport), the dangers of letting the wrong person gain access, the insurance schemes supporting failures and other considerations that often get enveloped in the concept of *trust*. The decision of whether to rely on the claimed information is therefore an exercise in risk evaluation (Crosby, 2008).

For example, if a prospective employer is presented with a work permit 'credential' such as an identity card which claims that an individual is entitled to work in the country, the employer needs to know the basis for this claim before

employing that person: is the credential a legitimate one? Does it belong to the person presenting it? Has it been issued by a recognised immigration authority? It is an increasingly common requirement in immigration laws around the world for the employer to be able to assure, upon audit or investigation by the relevant authorities, that the employer had diligently assessed the validity of the credential, yet standard methods for this final operation have yet to be developed (Crosby, 2008).

Even in this case the transaction is actually one of authentication rather than identification. As long as the credential is linked to the potential employee, the employer does not necessarily care 'who' the person is (they may claim to be called 'Elvis Presley') just so long as the identity service provider provides the required level of confidence that the individual has the attributes they claim – in this case the right to work in the country. Thus we must keep on questioning the nature of the essential task: identification or authentication? Too often policies focus on identification and this results not only in overly burdensome and complex systems but also systems that are not fit for purpose.

Biometrics

Linking credentials to individuals can be achieved by using something they have (e.g. a token of some form like a card) or something they know (e.g. a secret password or PIN). If the transaction is a high-risk one (cf. Cabinet Office, 2006), a third option that is increasing in popularity is linking the credential to something that the individual 'is', for example their biometrics – literally measures of the body (Kabatoff and Daugman, 2008). Commonly used biometrics include signatures, images of the face, fingerprints and iris scans (Jain et al., 2006). Although biometrics are based on images (of the face, of the fingerprint, of the iris, etc.), in operation they are typically converted into computational representations or templates that can be compared against other representations of the biometric (see, for example, Science and Technology Select Committee, 2006, p. 13). For example, a person may present their (live) fingerprint and the template obtained from it is compared with the template of their fingerprint stored on their identity credential; a match between the two provides increased confidence that the credential is theirs (Mansfield and Rejman-Greene, 2003).

Although biometric systems are often believed to provide perfect matches to a person's identity, in practice each biometric system has a known and measurable operating range. That is, each form of biometric has a measurable, non-zero rate of failing to match when there should be a match, or reporting a match when there is none. Similarly, each form of biometric has a known failure-to-acquire rate (for example, it is difficult to collect fingerprints from someone with no fingers; manual workers and refugees often have less clear fingerprints than other parts of the population). Other biometrics, such as iris, have better performance profiles but these come at increased cost as iris biometric equipment is an expensive, complex technology. Many biometric systems are designed to work under controlled and ideal circumstances, including under controlled lighting conditions. As a result, when these systems are installed, they are fine-tuned for an acceptable error rate for that context, not for perfection. There is also evidence that 'template ageing' affects the performance of the biometric system. For example, Bowyer et al. (2009) report that users of an iris biometric system 'will experience an increase in the false non-match rate with increasing time lapse from enrolment'. Ageing is likely to affect fingerprinting and facial scans even more significantly.

The choice of biometric and the resulting system implementation, therefore, should be based on consideration of the risk level involved. Is the level of risk in the transaction such that biometric matching is required at all? Does the choice of biometric take into consideration characteristics of the population from whom the biometrics will be taken? Is the performance offered by a particular biometric sufficient to warrant the expenditure on biometric readers required to implement it?

Enrolment and verification

Use of identity credentials typically involves two stages: enrolment and verification. Enrolment is the process by which an individual is brought within the identity policy and the resulting systems and is eventually issued with the credential. While this might be done simply by sending credentials to all individuals known to the state, as is common for tax filing numbers for instance, it typically involves some form of application process. Enrolment might be based on consideration of an individual's biographical (or life history) footprint, their biometric footprint or a combination of both (see, for example, UKIPS, 2008).

Verification is the means by which an identity credential presented by an individual is checked. At its simplest, this might simply involve looking at a card and accepting it if it appears genuine. Alternatively, various checks on the validity of the credential may be undertaken. These can include considering specialised security markings on the credential or telephoning a hotline to check that the credential is still valid and has not been listed as stolen or expired. In some cases, the verification process may be against information held on the credential; in others the check may be against data held by the identity service provider. In the context of biometric verification, there is evidence that using different versions of the technology for enrolment and verification can also affect performance markedly (Bowyer et al., 2009).

A decision to identify individuals using particular biometrics requires that identity verification uses those same biometrics. This can mean that verification points need to invest in similar biometric readers to those used in

enrolment and if the verification is intended to compare the biometric data with those held by the identity service provider, fast, secure communications links between the verification location and the service provider are required. Alternatively a failure to require biometric verifications calls into question the very need for biometrics at all, particularly as enrolling an entire nation's biometrics is resource intensive and costly.

The choice of enrolment methods is also not obvious, clear or even intuitive. For example, passports may be applied for by post or in person depending on the state's requirements and yet most passports today are only verified offline by looking out for any signs of tampering. Credit card transactions take place both offline (integrity checks of the card and signature) and online (checking with card provider that it is valid). In contrast, credit cards are often issued without requiring an individual to show up to be registered.

Drivers of identity policies in the modern state

Rather than reviewing specific national identity policies, this section critically examines some common examples of drivers for identity policies. It uses the concepts introduced above to highlight the consequences of some of the technological choices that underpin the policies.

Authentication and managing restricted services

Discerning between individuals and classes of individuals is essential for managing privileges. With a growing diversity of state-related services and service providers, or normative and economic policies that require structuring services (Raab, 2009), states are seeking to categorise individuals and groups who may gain access to specific services.

A common requirement of identity credentials is to provide access to age-restricted services and products. For example, laws may restrict access to nightclubs to individuals over a certain age, or older members of society may be entitled to discounts when they reach a certain age. Age-related transactions are based around authentication rather than identification. Nightclub staff members only need to know if the person before them is old enough to enter the premises. They do not need to know that person's name or even their date of birth. Similarly, the service provider providing discounts to pensioners does not need to know their age but simply whether or not their age means that they are entitled to the discount.

Ensuring uniqueness of citizens

Often seen as the foundation of government management, the ability of a government to recognise its citizens is often perceived as essential in order to endow individuals with rights. The modern welfare state must therefore be able to recognise who may benefit from the privileges of citizenship and through additional information processing the state may actually provide efficient and tailored services. With state-issued identity credentials being seen to drive many identity transactions, it is becoming increasingly important that each citizen has only one official identity (Crosby, 2008). Historically, the task of ensuring uniqueness has been executed by administrative consideration of an individual's 'biographical footprint'. For example, an identity credential might only be issued if a trusted member of society countersigns a citizen's application. The citizen's claimed biographical footprint might be combined with checks made against existing identity documents as well as against government and private sector databases. For example, does the citizen have an existing identity document, are their details stored in the government's health, education and employment records and do financial institutions also have matching records for the citizen?

Such an approach is not without its limitations, not least given the numbers of errors that exist in many official databases. Moreover, decisions about those citizens with 'complex' lifestyles such as the homeless, students or knowledge workers who move around frequently may prove to be difficult to automate. The problems of enrolment are exacerbated when dealing with countries with large populations that have limited public records for biographical checks (cf. Blakely, 2009).

In these circumstances, countries are beginning to consider using biometric checks as a basis for determining uniqueness rather than basing enrolment on the uniqueness of the biographical footprint. Enrolment is therefore predicated on determining that the presented biometric has not already been used to issue an identity credential. The technological challenges here are significant and increase dramatically with the size of the population as the biometric matching is no longer a one-to-one match between the individual and their credential but is instead a one-to-many match between the individual and all previously recorded biometrics. For large populations, the consequences of too many false matches may undermine the proposal to use biometrics to guarantee uniqueness in the population (Spiller, 2007).

Ensuring uniqueness of foreign nationals

Responding to a variety of drivers including concerns around terrorism, global migration, the management of the welfare state and even employment policy, governments have also used identity policies to counteract the trend that globalisation involves the free movement of people around the world. In the case of identity policies for addressing refugees and other foreign nationals, the issue is again one of authentication rather than identification. The relying party (the state) is often unable or unwilling to trust the identity assertions made by the migrant, particularly if they do not have any identity documents from the country they claim to be

coming from (cf. Sadiq, 2009). In such cases the 'identification' decision may be limited to checking whether the person has applied for a visa to enter the country on a previous occasion (perhaps using a different name) and here one-to-many biometric matches are again being used.

The state can then determine the rights that such an individual has: entry into the country, entitlement to work or to claim benefits and health services. The state can then issue its own credentials which can then be relied upon by others in the country (as the identity assertions are now backed by the national government).

Biometrics rather than identity data are also being used by countries such as the US to manage immigration. This is achieved by checking that all foreign nationals who enter a country (and register their fingerprints at immigration) then also leave the country (which is checked by collecting fingerprints on departure). The effectiveness of such a policy is limited by a number of challenges: the consequences that arise if not all departure points are collecting fingerprints and the ease with which departing biometric records are matched to arrival records. In turn, it is still unclear what the implications are for individuals who departed through a non-biometric border point – are they recorded as not having left the country?

Being the first to move on 'biometric' borders with its US-VISIT programme, the US has encountered significant institutional and structural challenges in implementing this policy effectively, for example system failures and logistical problems including airport design and large land and sea borders that make exit checks resource intensive if not infeasible. Yet the fanfare in establishing the laws and showcasing the first 'biometric border' system is never matched by open reviews of the hard work in implementing and auditing the systems that reveal the weaknesses and holes in the policy (e.g. Government Accountability Office, 2008). Regardless of this, officials in dozens of other countries are keen to implement similar VISIT systems, with such systems already in place in Japan and the UAE and under development in the European Union, Iran, Kuwait, Russia and South Korea.

The opportunities for identity policies

Sensing that globalisation poses new challenges for governments, there is a convergence in drivers for identity policy change around the world. Technological developments mean that countries and enterprises have the opportunity to refresh their identity policies to address the particular policy goals that they face. What we are seeing, however, is policy makers reaching out for technologies and systems developers to implement schemes that exist in their imaginations and sales material rather than policies founded upon sound risk assessments and comprehensive technology evaluations.

As governments mimic the actions of others, buy standardised systems from global suppliers (Lyon, 2009, ch. 3) and point to global agreements and international conventions, we are seeing solutions applied to problems that have not yet been identified correctly. Failing to identify the problem that needs to be dealt with may result in a poor consideration of the variety of technology policy alternatives that exist. For instance, although many countries are using the requirements for biometric travel documents to update their identity policies in order to create massive centralised databases of multiple biometrics, there are many other ways in which this can be done. The International Civil Aviation Organisation (ICAO), the UN agency that developed the international standards for biometric travel documents (Stanton, 2008) requires only that states implement face biometrics in new 'e-passports' (cf. LSE Identity Project, 2005, ch. 7). Nation states are not under any 'international obligation' to introduce fingerprint or iris biometrics into their travel documents (ICAO, 2003, 2004). Nor are states under any international obligation to establish biometric databases to implement the ICAO standards; in fact ICAO's standards point out that there are many risks associated with implementing biometric databases. Regardless of this, governments around the world are keen to implement fingerprints in passports and into national databases of biometrics, believing that they are obliged to do so by ICAO (Whitley and Hosein, 2010, ch. 5). It becomes practically impossible to separate out policy objectives from policy argumentation, as technology choices conceal agendas.

If the driver of the identity policy is to address identity fraud, a key design choice might be to minimise the amount of data that is disclosed in an authentication transaction. However, many current credentials used for identity purposes, such as identity cards and driving licences, actually disclose far more personal data than the authentication transaction requires. In many cases, this arises because the credential serves multiple purposes. These other purposes may require these data about the person to be displayed on the face of the credential in human readable form, as is the case with many travel documents and driving licences.

For example, in the case of the age-restricted transactions described above, the nightclub owner only needs to know that the person is old enough to enter the bar and does not need to know the person's name or date or place of birth. An identity credential based around a travel document or driver's licence, however, displays this information on the face of the document. In the UK, knowing someone's full name, place and date of birth is usually sufficient data to obtain a copy of that person's birth certificate. The birth certificate can then be used in the process of opening a bank account and can increase the likelihood of that person's identity being used fraudulently (Birch, 2009b).

Ironically, while policy makers may argue that they are making use of 'cutting edge' technology to overwhelm any opposition to their plans, they are in fact not making full use of the technologies that are available to advance effective identity policies. Technological solutions based around

well-established cryptographic techniques can automatically indicate whether or not a person satisfies the age-related condition being requested without disclosing unnecessary data, for example by displaying a photograph of the individual if they are old enough and not displaying their photograph if they are not (Birch, 2009a). These techniques permit the enhancement of service provision while safeguarding personal information and maintaining high-level security by avoiding centralised databases and disclosing only minimal information.

Innovative identity policies such as these offer intriguing possibilities as they do not rely on carrying a card but can be embedded in technological devices such as mobile phones. It is also possible to ensure that control over what information is disclosed remains with the individual (Information Assurance Advisory Council, 2009). New services may be created and new economies realised, creating systems that are proportionate and relevant to multiple stakeholders, sectors and institutions (Crosby, 2008). We are therefore surprised that the imagination of governments is applied only to the vast amounts of information that may now be made available to them through an identity policy, rather than the new markets and services that are possible through interesting applications of truly innovative techniques.

Policy implications

At one level, identity policies can be seen as an example of a complex policy area where design and implementation choices can have a significant impact on the eventual effectiveness of the policy. As with any policy, a key consideration is a clear statement of what objectives the policy is intended to achieve as this will influence key design choices that underlie the policy: an identity policy that is driven by concerns about identity fraud will have a very different shape from one that is seeking to introduce machine-readable travel documents; a policy that seeks to enhance online access to government services should be quite different from one that is concerned with cross-border security.

What differentiates identity policies from many other policies, however, is the key role that technological issues play in determining the scope and significance of the proposals. Enlightened policy makers can draw upon the opportunities offered by developments in technologies like advanced cryptography and biometrics to provide effective policies that address the particular needs of their citizens. They can do this without compromising the rights of their citizens, without increasing the risk of identity fraud and without spending vast sums of money on high-profile but ineffective initiatives.

Alternatively, national policies can be driven by global technology firms, by misunderstood obligations on travel documents, a 'rear view mirror' understanding of technology and a desire to be doing something – anything – in response to global policy challenges such as terrorism and migration.

Achieving effective policy making therefore requires a process that explicitly includes consideration of technological issues in the decision-making process. Unfortunately, the artificial science/society distinction still drives too much of the policy-making process (Callon et al., 2009). If policy makers do not have sufficient expertise to evaluate technological matters, they need to call upon informed advocates who are able to enumerate the various technological choices that are open to them and advise them of the benefits and risks of each choice (Whitley and Hosein, 2008).

As well as fundamental choices about the kinds of technologies to use, identity policies raise important questions about the role of the private sector and about the relationships between the rights and concerns of the citizen and those of government. For example, if personal information held by the private sector is increasingly used in the enrolment stage for identity credentials, why not take this a step further and allow for a market of private sector authentication providers to exist, offering differing levels of authentication assurance? Those individuals who simply require the ability to confirm that they are able to access age-restricted services do not necessarily need this functionality to be provided by a state-based identification scheme based around the use of biometrics. Instead age verification can be based on details held by a mobile phone company, bank or even education provider (school or university). This pushes the responsibility for confirming the date of birth of the individual, for example, on to these other organisations, but, given the relatively low level of risk associated with age-verification services, this is a manageable risk that these companies might be prepared to take (Whitley, 2009).

Limiting the scope of state-issued credentials can also speed up the rollout of identity credentials. For example, banks could issue basic credentials to their customers fairly quickly and once they are issued citizens could choose to add state-based assertions to the credential as and when required (Crosby, 2008).

We must all open up our minds to new innovations in identity policy. Given the technological challenges these policies raise, policy makers must be informed and imaginative rather than just opportunistic.

References

Asiimwe, B. R. (2009) 'Rwanda: Refugees to Get ID Cards' [online], AllAfrica.com, 18 November. Available from: http://allafrica.com/stories/200911180044.html [Accessed 16 February 2010].

BBC News (2009) 'Bogus Student Checks "Don't Work"', BBC, 1 November. Available from: http://news.bbc.co.uk/1/hi/uk/8332314.stm [Accessed 16 February 2010].

Berghel, H, (2006) 'Fungible Credentials and Next-Generation Fraud', *Communications of the ACM*, 49 (12), pp. 15–19.

Birch, D. G. W. (2009a) 'Psychic ID: A Blueprint for a Modern National Identity Scheme', *Identity in the Information Society Open Access Journal* [online]. Available from: http://dx.doi.org/10.1007/s12394-009-0014-6 [Accessed 16 February 2010].

Birch, D. G. W. (2009b) 'What a Cunning Stunt', 28 October [online]. Available from: http://digitaldebateblogs.typepad.com/digital_identity/2009/10/what-a-cunning-stunt.html [Accessed 16 February 2010].

Blakely, R. (2009) 'India to Issue All 1.2 Billion Citizens with Biometric ID Cards', *The Times*, 15 July [online]. Available from: http://www.timesonline.co.uk/tol/news/world/asia/article6710764.ece [Accessed 16 February 2010].

Bowyer, K. W., Baker, S. E., Hentz, A., Hollingsworth, K., Peters, T. and Flynn, P. J. (2009) 'Factors that Degrade the Match Distribution in Iris Biometrics', *Identity in the Information Society Open Access Journal* [online]. Available from: http://dx.doi.org/10.1007/s12394-009-0037-z [Accessed 16 February 2010].

Cabinet Office (2006) 'Identity Risk Management for E-Government Services' [online]. Available from: http://webarchive.nationalarchives.gov.uk/20070603164510/http://www.cabinetoffice.gov.uk/csia/~/media/assets/www.cabinetoffice.gov.uk/csia/id_risk_mgt061127%20pdf.ashx [Accessed 16 February 2010].

Callon, M., Lascoumes, P. and Barthe, Y. (2009) *Acting in an Uncertain World: An Essay on Technical Democracy*. Cambridge, MA: MIT Press.

Crosby, Sir J. (2008) 'Challenges and Opportunities in Identity Assurance', 6 March [online]. Available from: http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/d/identity_assurance060308.pdf [Accessed 16 February 2010].

Fishenden, J. (2005) 'ID Cards will Lead to "Massive Fraud", *The Scotsman*, 18 October [online]. Available from: http://ntouk.com/archives/2005/Oct/18.10.2005.htm [Accessed 16 February 2010].

Government Accountability Office (2008) 'Strategic Solution for US-VISIT Program Needs to be Better Defined, Justified, and Coordinated', February [online]. Available from: http://www.gao.gov/new.items/d08361.pdf [Accessed 16 February 2010].

Haines, L. (2009) 'Spain Cuts Off 3m Pre-pay Mobiles: Mass Failure to Register Phones', *The Register*, 9 November [online]. Available from: http://www.theregister.co.uk/2009/11/09/spanish_mobiles/ [Accessed 16 February 2010].

ICAO (2003) Technical Advisory Group on Machine Readable Travel Documents. Fourteenth Meeting International Civil Aviation Organisation, 6–9 May [online]. Available from: http://www2.icao.int/en/MRTD/Downloads/TAG-MRTD%20Reports/TAG-MRTD_14%20Report.pdf [Accessed 16 February 2010].

ICAO (2004) 'Biometrics Deployment of Machine Readable Travel Documents', International Civil Aviation Organisation, 21 May, ICAO TAG MRTD/NTWG [online]. Available from: http://www.policylaundering.org/archives/ICAO/Biometrics_Deployment_Version_2.0.pdf [Accessed 16 February 2010].

Information Assurance Advisory Council (2009) Identity Assurance Concluding Report, 7 February [online]. Available from: http://www.iaac.org.uk/Default.aspx?tabid=105 [Accessed 16 February 2010].

Jain, A. K., Ross, A. and Pankanti, S. (2006) 'Biometrics: A Tool for Information Security', *IEEE Transactions on Information Forensics and Security*, 1 (2), pp. 125–143.

Kabatoff, M. and Daugman, J. (2008) 'Pattern Recognition: Biometrics, Identity and the State – An Interview with John Daugman', *Biosocieties*, 3 (1), pp. 81–86.

Latour, B. (1992) 'Where are the Missing Masses? The Sociology of a Few Mundane Artifacts', in W. E Bijker and J. Law (eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge, MA: MIT Press, pp. 225–258.

LSE Identity Project (2005) Main Report, 27 June [online]. Available from: http://identityproject.lse.ac.uk/identityreport.pdf [Accessed 16 February 2010].

Lyon, D. (2009) *Identifying Citizens: ID Cards as Surveillance*. Cambridge: Polity.

Manifesto Club (2010) 'Fortress Academy: The Points-Based Visa System and the Policing of International Students and Academics' [online]. Available from: http://www.manifestoclub.com/files/FortressAcademy.pdf [Accessed 16 February 2010].

Mansfield, T. and Rejman-Greene, M. (2003) Feasibility Study on the Use of Biometrics in an Entitlement Scheme, National Physical Laboratory [online]. Available from: http://dematerialisedid.com/PDFs/feasibility_study031111_v2.pdf [Accessed 16 February 2010].

Perrow, C. (1984) *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Raab, D. (2009) *The Assault on Liberty: What went Wrong with Rights*. London: Fourth Estate.

Rotenberg, M. (2006) 'Real ID, Real Trouble? ', *Communications of the ACM*, 49 (3), p. 128.

Sadiq, K. (2009) *Paper Citizens: How Illegal Immigrants Acquire Citizenship in Developing Countries*. Oxford: Oxford University Press.

Science and Technology Select Committee (2006) 'Identity Card Technologies: Scientific Advice, Risk and Evidence', *House of Commons Sixth Report of Session 2005–06* [online]. Available from: http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf [Accessed 16 February 2010].

Smith, A. and Clarke, R. (2000) 'Identification, Authentication and Anonymity in a Legal Context', *Computer Law and Security Report*, 16 (2), pp. 95–100.

Spiller, S. (2007) 'ID Cards will Give "False" Data', BBC, 31 July [online]. Available from: http://news.bbc.co.uk/1/hi/programmes/file_on_4/6922882.stm [Accessed 16 February 2010].

Stanton, J. M. (2008) 'ICAO and the Biometric RFID Passport: History and Analysis', in C. J. Bennett and D. Lyon (eds.), *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. London: Routledge, pp. 253–267.

UKIPS (2008) 'Introducing the National Identity Scheme: How the Scheme will Work and How it will Benefit You', Identity and Passport Service, 6 November. Available from: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/introducing_the_national_identity_scheme.pdf [Accessed 16 February 2010].

Unique Identification Authority of India (2009) 'Creating a Unique Identity Number for Every Resident in India'. Available from: http://uidai.gov.in/documents/Creating_a_unique_identity_for_every_resident_in_India.pdf [Accessed 16 February 2010].

Whitley, E. A. (2009) 'A New Way Forward for an Effective Identity Policy in the UK', Security-news.tv. Available from: http://identityproject.lse.ac.uk/TheVault2009.pdf [Accessed 16 February 2010].

Whitley, E. A. and Hosein, G. (2010) *Global Challenges for Identity Policies*. Basingstoke: Palgrave Macmillan.

Whitley, E. A. and Hosein, I. R. (2008) 'Doing the Politics of Technological Decision Making: Due Process and the Debate about Identity Cards in the UK', *European Journal of Information Systems*, 17 (6), pp. 668–677.

Author Information

Dr Edgar A. Whitley, Reader in Information Systems, Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science, UK.

Dr Gus Hosein, Visiting Senior Fellow, Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science, UK.