

PERSONAL IDENTIFICATION IN THE INFORMATION AGE: THE CASE OF THE NATIONAL IDENTITY CARD IN THE UK

Paul Beynon-Davies, European Business Management School, University of Wales Swansea,
Singleton Park, Swansea, UK, p.beynon-davies@swansea.ac.uk

Abstract

The informatics infrastructure supporting the Information Society requires the aggregation of data about individuals in electronic records. Such data structures demand that individuals be uniquely identified and this is critical to the necessary processes of authentication, identification and enrolment associated with the use of e-Business, e-Government and potentially e-Democracy systems. It is also necessary to the representation of human interactions as data transactions supporting various forms of governance structure: hierarchies, markets and networks.

In this paper we use the agenda surrounding the proposed introduction of a national identity card in the UK as an empirical backbone for considering the issue of identity management. Currently, the UK government is attempting to relate the rights and entitlements of citizenship in the UK with a standard electronic identifier for British citizens and its instantiation in an 'entitlements card'. This attempt to define legitimising identity seems to us a potentially fruitful empirical source for examining the conceptual and pragmatic issues associated with identity management in the information age. Such a card offers numerous potential benefits for individuals and organisations but its introduction raises major challenges to data protection, data privacy and public trust in the information governance of the UK.

Keywords: electronic government, identity management, electronic service delivery

1. INTRODUCTION

The informatics infrastructure supporting the e-Society requires the aggregation of data about individuals in electronic records. Such data structures demand that individuals be uniquely identified and this is critical to the necessary processes of authentication, identification and enrolment associated with the use of e-Business, e-Government and potentially e-Democracy systems ((Beynon-Davies, 2004). It is also necessary to the representation of human interactions as data transactions supporting various forms of governance structure: hierarchies, markets and networks (Thompson, 2003).

In the Information Society an individual may take on a number of different identities – one for each electronic service in the public, private and voluntary sectors with which the individual engages. Associated with these identities an individual may accumulate a vast array of personal identifiers for such ‘services’ and is also likely to accrue a range of physical representations of such multiple identification: credit card, debit card, driving licence, passport, library card, parking permit etc.

The key example we wish to discuss in-depth in this paper is the way in which personal identifiers are used as a symbolic representation of national identity. Recently in the UK, the government is attempting to relate the rights and entitlements of citizenship with a standard electronic identifier for British citizens and its instantiation in an ‘entitlements card’. This attempt to define what Castells (Castells, 1996) has referred to as legitimising identity seems to us a potentially fruitful empirical source for examining the conceptual and pragmatic issues associated with identity management in the information age.

The structure of the paper is as follows. First we make some important distinctions relating to the issue of identity management. Second we consider the proposed introduction of an ‘entitlements’ card in the UK. Third, we examine the introduction of ID cards in other countries. Fourth, we conduct a strategic evaluation of the UK national identifier and associated card.

2. IDENTITY MANAGEMENT

2.1 Authentication, Identification and Enrolment

We would argue that identity management comprises three inter-related processes which are illustrated in Figure 1 in terms of the classic meaning triangle (Ogden and Richards, 1923). In a semiotic sense (Stamper, 1973), personal identifiers can be seen as symbols relating to the referents of the multiple identities that individuals may experience in the Information Society. Hence, the issue of personal identification is distinct from and reliant upon a precursor process of authentication. In turn, identification is a necessary pre-condition for enrolment in many activities in contemporary life.

The identifier is a symbol or set of symbols (a designation) that can be used to authenticate a person (an extension). Authentication is a process that involves answering the question - *Am I who I claim to be?* It involves validating the association between the identifier and the person (Zorkadis and Donos, 2004). For example, possession of a valid passport is taken as an authentication token in travel situations between countries.

Identification is the process of using an identifier to connect to a stream of information constituting a person’s identity (an intension). Identification in the large involves answering the question *Who am I?* Identifiers are used to assign identities to individuals – for example, legitimating somebody as a legal resident, credit-worthy customer or taxpayer.

A third process is illustrated on figure 1 – that of enrolment. Here a validated identity serves to enrol the individual in some defined human activity system (Checkland, 1999). Enrolment involves answering the question – *What am I expected to do.* Hence, a validated identity such as that of a taxpayer will enrol the individual in a whole range of rights, responsibilities and expected actions in the activity system associated with fiscal matters.

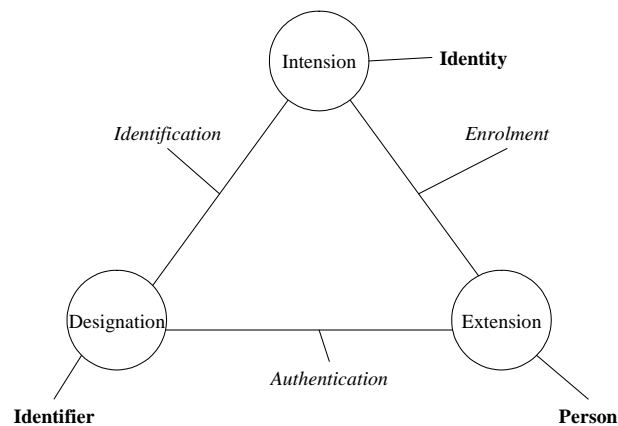


Figure 1: Authentication, Identification and Enrolment

2.1 Identification Methods

A number of methods are available for identifying a person, in order to associate data with them (Clarke, 1994). These methods include:

- **Appearance.** How the person looks including features such as gender, skin colour, hair colour, colour of eyes, facial hair or distinguishable markings such as a birth-mark.
- **Social Behaviour.** How the person interacts with others including style of speech and accent.
- **Names.** What the person is called by other people including personal name(s), surname, maiden names, nicknames and also-known-as (AKA) names.
- **Codes.** What the person is called by an organisation such as a series of numbers or letters which can be human-readable, machine-readable or both.
- **Knowledge.** What the person knows such as the use of user names, personal identity numbers (PINs) and passwords.
- **Tokens.** What the person has in his or her possession, such as a birth or marriage certificate, passport, drivers licence and credit card. More recently such tokens may include digital certificates or signatures.
- **Bio-dynamics.** What the person does, such as the way in which someone's signature is written, statistically analysed voice characteristics or keystroke dynamics in relation to login-identifier and password.
- **Natural Physiography.** What the person is in terms of features such as skull measurements, teeth and skeletal injuries, thumbprint, fingerprint sets and handprints, retinal scans, earlobe capillary patterns, hand geometry and DNA patterns. If such characteristics are readable by machine then they are referred to as bio-metric identifiers.

In essence this typology may be collapsed into identifiers of two forms - natural identifiers and surrogate identifiers. Natural identifiers are the conventional identifiers used in well-established interactions in society. They begin with the physical characteristics of the person such as appearance and range across the social conventions of names and knowledge. Generally speaking, such natural identifiers are deficient in producing the characteristic of uniqueness demanded by organisations and their information systems. For this reason, surrogate identifiers are used, which constitute additional features such as codes and tokens used to uniquely identify individuals. We include in this latter category those features of the individual such as bio-metrics and bio-dynamics which are amenable to capture by new technologies.

2.2 Features of Good Identification Systems

Identification systems are essential to the effective operation of any organisational information systems that utilise personal data. In terms of this informatics context, there are a number of characteristics of good identification systems, which include (Prabhakar, Pankanti et al., 2003):

- Universality of coverage. Every relevant person for the domain or situation in question should have an identifier.
- Uniqueness. Each relevant person should have only one identifier and no two people should have the same identifier.
- Permanence. The identifier should not change, nor be changeable without authority. This implies that the identifier should be non-mnemonic since if any meaningful association is built into an identifier such an association may change over time.
- Indispensability. The identifier should be available for use at all times.
- Exclusivity. No other form of identification should be necessary or used.

2.3 Identification and e-Government

It is important to distinguish between the issue of personal identification and its implementation in terms of some smartcard. These two concepts are frequently confused and conflated in the political debate surrounding national identity cards. The introduction of a national identifier is a pre-condition to the introduction of a technology such as a smartcard and is potentially more interesting because it would enable private and public sector organisations to integrate data about the individual far more easily. A national identity smartcard would allow the government to store a lot more information about an individual than simply an identifier.

Personal identifiers are much used by public and private sector organisations. There is probably at least one identifier for each organisation a person interacts with. The reason for this lies in the need for organisation information systems to relate data to some notion of object identity.

There is clearly an option as to whether to display or not the identifier on a smartcard. Explicit identifiers are probably required to enable entry to on-line services unless card readers are provided ubiquitously. In the short term, mappings would need to be made between the national identifier and organisation identifiers. Over the longer term organisations could migrate to use of a national identifier and this it is claimed would make easier the introduction of new electronic services.

A common and standard identifier for citizens would undoubtedly have numerous benefits for the implementation of 'joined-up' government (the integration and inter-operability of government processes) generally and e-Government (the integration and inter-operability of ICT systems in the e-government infrastructure) in particular. It is also seen as critical to certain e-Democracy initiatives such as the introduction of e-Voting. For such activity a national electronic electoral register is a pre-requisite.

Particular benefits arise from the use of biometric information. Biometric data, such as an iris scan, will ensure that an individual's identity cannot be copied, that a person cannot establish more than one identity for public and private sector schemes, and most importantly, help to verify that the person presenting the card is the person that it was issued to.

However, some of the key concerns seem to surround the relationship between personal identification and other data properties held about the individual including transactional data (Burnham, 1983) gathered about the behaviour of the individual— what has been referred to as data creep (Travis, 2002). Generally, there appears less public trust in the potential use of integrated information by government than by business (Perri6 and Briscoe, 1996).

3. THE UK 'ENTITLEMENTS' CARD

In this section we examine the case of a national identity card, which is built on the basis of a documentary analysis of published material. The case is interesting because it highlights many

of issues of identity management in the information age discussed above but also raises them to a higher plane of discourse in what Taylor and Williams have referred to as the Information Polity (Taylor and Williams, 1991).

Recently, the Home Secretary has resurrected the idea of introducing a national identity card, which existed in the UK during the First and Second world Wars. Successive Home Secretaries (including Michael Howard in the 1980s) have proposed the re-introduction of such a card. However, the introduction of this ‘identification technology’ has met with continuous opposition from a range of different stakeholder groups. This is interesting in the face of acceptance of such technologies in mainland Europe and the growing use of ‘identification technology’ amongst the private and public sectors in the UK.

The first ‘identity card’ was introduced in the UK in 1915 by the National Registration Act, which set up a population register for England, Wales and Scotland covering all persons between 15 and 65. The primary purpose of this population register was to aid military conscription and workforce planning during the First World War. All persons between these ages were issued with a certificate of registration. An amendment to the act in 1918 required persons to produce the certificate on demand to a police officer or authorised person on request. Registration was withdrawn after the First World War but planning for a revised system took place during the 1930s.

At the outbreak of the Second World War a national registration scheme was introduced. Members of the armed forces were issued with their own cards while civilians were issued with cards that they had to carry at all times. A process akin to the census was used to register persons. Enumerators visited every house in the country and issued identity cards on their return visits a week later. The national registration number used on this card eventually became the National Health Service (NHS) number after the war.

The National Identity Card was heavily associated with rationing which continued for some time after the War. Calls were made to repeal rationing and other emergency measures. The card was repealed by Winston Churchill’s Conservative government after the case of Muckle Vs Wilcocks in 1950.

Table 1: Key Events in the UK Experience of National Identification

Date	Event
1915	The National Registration Act established a population register for England, Wales and Scotland.
1920s	Sir Bernard Mallet, Registrar General, proposed a population register with a linked ID card.
1940	National Registration Scheme with associated card introduced.
1950	National Identity Card withdrawn after the case of Muckle vs. Wilcocks.
1978	The Lindhop Committee on Data Protection proposed a UPI (Universal Personal Identifier) for all data users on all occasions, but this was considered to be a ‘considerable threat to privacy, and perhaps the freedom of the private citizen’.
1988	Tony Favell tried to introduce a Bill under the Ten Minute Rule to introduce a British ID card, which would ‘help in the fight against football hooligans’ and ‘crime in general’. The Bill was defeated by 172 votes to 114. The Home Affairs Select Committee briefly considered and rejected the idea of ID cards.
1989	Ralph Howell MP introduced the National Identity Bill as a private member’s bill for a compulsory identity system. It failed due to lack of time. Jaques Arnold MP attempted to introduce a Ten Minute Bill for a personal ID number for all those born after 1.1.90.
1990	The Association of Chief Police Officers (ACPO), declared themselves no longer against machine readable ID cards. The Home Affairs Committee published its report, <i>Practical Police Co-operation in the European Community</i> , which favoured voluntary ID cards. In reply, the government considered that voluntary ID cards would not ‘benefit either the individual or the state’.

1992	The government considered that a compulsory scheme would be too costly.
1993	David Amess MP tried to introduce the Voluntary Personal Security Cards Bill, under the Ten Minute Rule, to combat fraud, illegal immigration and terrorism.
1994	Harold Elletson MP's Bill to introduce national ID cards failed by 113 votes to 89.
1999	A report <i>Wired Whitehall</i> anticipated that every individual would carry a citizen card permitting the individual to carry out a wide-range of transactions with government services.
2002	David Blunkett issues a consultation document on the introduction of a National Entitlements card.
Jan 2004	A six-month trial of a bio-metric smartcard started.

Much of the debate surrounding this issue relates to the purposes of this 'technology' in its social context. In the consultation document (Home-Office, 2002) the universal entitlement card is described as having four main purposes:

- To provide people who are lawfully resident in the UK with a means of confirming their identity to a high degree of assurance. This is fundamentally proposing its use as a form of authentication. There are also echoes of legitimising identity. In other words, associating possession of this token with rights of citizenship.
- To establish for official purposes a person's identity so that there is one definitive record of an identity which all government departments can use if they wish. Here the card is being proposed as a way of integrating identity data about the individual. It is also implied that the card will be used to integrate identification processes across government.
- To help people gain entitlement to products and services provided by both the public and private sectors, particularly those who might find it difficult to so do at present. Here the card is proposed as a mechanism of enrolment in the use of government services. It also raises the possibility of its extension into the use of private sector services.
- To help public and private sector organisations to validate a person's identity, entitlement to products and services and eligibility to work in the UK. Here the card is being proposed as the major source of identification for use with public and private ICT systems.

The current consultation document proposes that as an interim measure the photo-card driving licence and new passport card would both be equally acceptable forms of entitlement card. Around 13 million photo driving licences have been issued and approximately 44 million passports are currently in issue. Both of these forms of identification have to be paid for by the public and this would continue, presumably with two different identifiers; perhaps with an increased cost to cover free production of cards for the disadvantaged. Checks would have to be tightened in passport and driving licence applications to ensure greater protection against identity fraud. The government wishes to include certain biometric information such as an image of the person and a thumbprint or perhaps an iris scan on the card. It is likely it would be a smartcard to enable it to store a range of portable personal information.

The key to the power of biometrics as an identification technology is the amount of randomness and complexity that the biometric contains. In terms of three forms of biometric identification iris scanning offers the strongest form of authentication followed by fingerprints and facial recognition. This is because different degrees of freedom (independent dimensions of variation) are associated with different aspects of physiography. Irises have about 249 degrees-of-freedom; fingerprints have approximately 35 degrees-of-freedom whereas faces have only about 20 degrees-of-freedom.

The card is really one particularly sensitive instance of a wider e-Government agenda. Implementing a national identity card would involve:

- Establishing the first national register of legal residents in the UK (some 67.5 Million people) – a population register. The aim is to have one definitive record for each person on this register that would hold core data about the individual such as name, residential address, date of birth, place of

birth, sex and nationality. This will also involve assigning and storing a unique personal identifier for each legal resident in the UK.

- Establishing procedures for maintaining the register - adding new entries to the register and for updating existing entries. Procedures would have to be developed to ensure that the information gathered was accurate and that the data was secure from unauthorised access. A PIN might be issued with a card to ensure a further level of security in the case of remote access to services.
- Linking the register to other service provider information systems. It is claimed that keeping data in separate databases, linked to entitlement to specific services, will increase levels of data protection and data security. The central register can be seen as an attempt to expand the government gateway concept – a unified citizen portal to government services. For this clearer data sharing policy needs to be established. This would involve determining the data that can be shared between providers without and with the consent of the individual.
- A card would then need to be issued to each person on the central database.

4. ID CARDS IN OTHER COUNTRIES

Identity cards are widely used across Europe. Many countries have already introduced such cards in order to benefit government services and to protect individual identities (MapleLeafWeb, 2003). Some schemes are voluntary; some are compulsory. Compulsory ID cards exist in Germany and Spain. Such cards must be carried at all times and can be checked by the police at any time. In Greece information on the card includes a person's religion and also a person's thumbprint. Identity cards in the form of various smart cards are also widely used by UK individuals. The identity card has become the consumer and citizen's portal to the information economy and to key basic public services.

This tension between widespread resistance to a national form of identification in the face of widespread adoption of electronic identification for key activities in the Information Society has led some to propose that our information politics remains firmly in the industrial society, while our problems are becoming those of an information society (Perri6 and Briscoe, 1996). This tension is evident in recent policy. Up until 2013 the card will not be universal although it is expected that 80% of the UK population will be enrolled by that time and the Government will then have the option of deciding on legislating for compulsory ownership of such a card. Therefore, at such a time, like the wartime card, the entitlements card would be universal. However, unlike the wartime card the new card will apparently not need to be carried at all times and the Police will not be given any new powers to ask a citizen to produce their identity card.

Some of the international experience of ID cards is summarised in table 2.

Table 2: International Experience of National Identity Cards

Country	ID	Attribute Data	Compulsion	Uses
Australia	No ID.			
Belgium	ID Card (1919).	Photograph, nationality, place of birth, date of birth, sex, address, issuing authority, digital signature.	Compulsory.	Access to government services.
Finland	ID Card (1999).	Identifier, Photograph, signature.	Voluntary - widely held.	Online banking, and travel throughout Europe.
France	ID card.	Photograph, name, sex, place of birth, date of birth, nationality, height, signature.	Voluntary - widely held.	Access health, education, voting, bank transactions, European travel.
Germany	ID Card.	Photograph, name, place of birth, date of birth, nationality, parent's names, height, eye colour, address, expiry date.	Compulsory (over 15)	European travel.

Greece	ID Card.	Photograph name, place of birth, date of birth, nationality, parent's names, physical description, address, occupation, religion, image of right thumb print.	Compulsory (over 14)	Passports, driving licence applications, entrance to public buildings, access to some local government services, European travel.
Hong Kong	ID card (2003)	Embedded microchip holds an individuals name, birth date, photograph, thumb prints.	Voluntary	Immigration, travel.
Italy	ID Card	Name, photo, serial number, stamp and a signature.	Voluntary (over 15)	Access public sector services, European travel.
Netherlands	ID Card (1996)	Name, photograph, hologram, social security and tax numbers.	Voluntary	Access public services, European Travel.
Malaysia	MyKad, (1999)	Biometric information is included in the form of thumbprints.	Compulsory	Combined driver's license, passport, health card, ATM bankcard.
Portugal	ID card.	Photograph, fingerprint, signature, name, details of parents, place and date of birth, marital status, height.	Voluntary	Access passports, driving/marriage licences, employment, education.
Spain	ID card.	Photograph, name, nationality sex, signature, details of parents, place and date of birth, address.	Compulsory	Dealings with government and commerce, European travel.
US	No ID Card			Photographic driving licenses universal.

5. A STRATEGIC EVALUATION OF A NATIONAL IDENTITY CARD

It is possible to conduct a strategic evaluation (in terms of cost and benefits) of the introduction of a national identifier and associated smartcard. Such an evaluation usefully summarises many sides of the debate surrounding the introduction of a universal form of personal identification in the UK. Benefits include stronger authentication, more convenient access to services, support for greater integration and inter-operability of government systems, combating identity fraud and other forms of criminal behaviour.

5.1 Authentication

Authentication assumes greater significance with increasing use of on-line delivery of services and products and increased security risks that this entails. 90% of people in the UK currently hold some form of card identification, particularly for financial purposes. There are clear benefits from having one form of identification for individuals rather than the vast range of identification, which individuals hold currently such as a passport, National Health Service card, National Insurance Card, Tax Reference.

5.2 Citizen Benefits

Such forms of identification are used to authenticate access to a vast range of services. There is nearly an identification number for each form of government service with which the government interacts with the citizen. A common identifier would avoid the need for an individual to provide the same personal information to different government departments time and again. When an individual engages in a major life-event such as moving house, the process of updating information across diverse departmental systems would be made easier. An identity card could be used by citizens for a range of purposes, such as a travel document, proof of age, and authentication of right to vote, work etc.

5.3 Data Administration

Benefits will arise for service providers in reducing the administrative burden of entering the same data a number of times into different systems. However, universality of coverage would have to be ensured for these benefits to be realised.

5.4 Integration and inter-operability of Government Information Systems

A key element of the e-Government agenda (Cabinet_Office, 2000) is so-called 'joined-up' service delivery. Such joined-up service delivery demands joined-up government information systems. Joined-up in this latter sense means greater integration and inter-operability of systems. A common identifier would facilitate the integration of data across systems and improve the inter-operability of systems. Key benefits would also arise in the simpler processing of systems and reductions in error rates. A national population register would eventually remove the need for an electoral register organised on local lines or make easier the collection of such data.

5.5 Identity Fraud

Identity fraud, sometimes referred to as identity theft, occurs when someone takes over a totally fictitious identity or adopts the identity of another person with or without their consent (Cabinet_Office, 2002). The UK government believes that an identity card would prove a significant weapon against identity fraud in both the public and private sectors (over 50% of identity fraud occurs in the private sector). It is also seen as a major way of tackling identity fraud, particularly in relation to the benefits system. Identity fraud estimated to cost the UK £1.3 billion per annum.

5.6 Illegal Immigration

Illegal immigration can be seen as one potent example of identity fraud. The UK government believes that an identity card would prove a significant weapon in the fight against illegal immigration. It believes that the UK's lack of an identity card acts as a magnet to illegal immigrants who believe that they can work and access benefits with impunity. An identity card would make it more difficult for employers to claim evidence of entitlement to work from a vast range of documentation currently used for this purpose.

5.7 Monitoring Criminals and Criminal Behaviour

Recently two police forces in the UK (Humberside and Cambridgeshire) have come under criticism in relation to the conviction of the Soham murderer Ian Huntley. Huntley was able to obtain a job as a school caretaker despite a number of recorded allegations of molestation of under-age girls. These records were apparently deleted by Humberside police for fear of infringing data protection legislation. Cambridgeshire police also failed to access a previous criminal history of Ian Huntley because a search was not conducted on his previous aliases.

Although a national identifier would not solve such problems of data sharing it would make it easier for police forces, and the new Criminal Records Bureau, to maintain accurate records of criminal activity and to share this data between police forces. It would also make it more difficult for people to gain employment using an alias.

As well as clear benefits there are a number of associated costs with the introduction of a national identifier and card. The issue of costs is larger than purely the financial cost of introducing and maintaining a national identity register. Costs include risks to data privacy and protection, the potential misuse of data and the possibility of increased fraudulent activity.

5.8 Data Privacy and Protection

Data privacy is seen to be a key citizen right in most Western countries. Data protection corresponds to the legislative means for ensuring data privacy. There is concern over the data contained on the proposed card and also over the data sharing implications of a central record (Cabinet_Office, 2002).

The government already holds a vast amount of personal information about citizens, whether it is health records, tax returns, welfare benefit forms, criminal records, local authority records or driving licence data. But the underlying principle remains that personal information supplied for one purpose is not used for another.

To comply with the 1998 data protection act the government aims to distinguish between personal data and sensitive personal data. The intention is to include on the identity register personal information including name, date and place of birth, home address, unique personal number, national insurance number, passport and driving licence numbers, nationality, sex, photograph, digitised signature, employment status, the card's validity dates and by whom it was issued. Data protection legislation would rule out the inclusion of 'sensitive personal data' such as details of ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life or past life of crime.

The Home Office says a more expensive form of identity card scheme, one that would involve the use of a two-dimensional bar code or a memory chip, could be used to store a lot more information - it suggests that some people might want to include details of a medical condition, such as epilepsy or diabetes, that would be helpful to an ambulance crew, or the details of their public transport season ticket. The government stresses that any such extra information on the new identity card would only be included with the consent of the individual themselves.

However, the concern is for the potential for 'data creep' that this entails. What starts as an identity management infrastructure ends up as an all-purpose database for controlling citizenry.

5.9 Data Misuse

The existence of a national identifier and the integrated government information systems that may be built around it, raise fears that potential future authoritarian governments in the UK may use it as a weapon of mass control (Guardian, 2003). UK citizens are the most monitored in the world, particularly via CCTV. Such monitoring combined with integrated government databases provides the technological means for enabling dystopias such as Huxley's Brave New World and Orwell's 1984.

5.10 Denial of Service

If the entitlements card is the only way of accessing a wide range of services, people might be denied services while they waited for a replacement for a lost or stolen card.

5.11 Increased Fraudulent Activity

There is concern also that if a card scheme was not secure then it could actually lead to increased levels of fraudulent activity, as counterfeiting of cards would have greater potential benefits for criminals. This is because of the wider scope of use of such a card – opening up at one stroke the possibility of multiple false identities.

5.12 Development Issues

In the consultation document the introduction of an identity card is seen as needing three years to develop and implement the systems. It will demand a large and complex ICT system project with all the associated risks. Such large-scale government ICT projects are normally subject to high rates of risk and also of failure.

5.13 Financial Cost

The cards would be valid for ten years and the total cost of the scheme is estimated at £1.5 billion. Proposals are that money be recouped by increasing passport and driving licence fees (by around £14 – £18) and by charging a fee for a non-driving licence/passport card. Disadvantaged groups would apparently be able to obtain a card free of charge.

6. CONCLUSION

Personal identification is the process of associating data with a particular human being. This process assumes greater significance in the Information Society because of the increasing use of remote interaction between individuals and organisations. Hence, in such situations it is not possible to identify persons through their physical presence. As a growing range of services in the public and private sectors are provided via electronic channels, authentication of individuals assumes greater significance, coupled with the increased security risks this entails.

Personal identification is distinct from but a necessary pre-condition of personal identity. In the information age identification involves the use of common attributes or features of the individual to access a vast range of other data expressions of the individual. This is distinct from authentication (validating the association between some identifier and the person it stands for) and enrolment (assigning an individual rights, responsibilities and actions in some human activity system).

Personal identification in the information age is characterised by a movement from natural to surrogate identifiers. Natural identifiers are the conventional identifiers used in well-established interactions in society but which are deficient in producing the characteristic of uniqueness demanded by organisations and their information systems. For this reason, surrogate identifiers are used, which constitute additional features such as codes and tokens used to uniquely identify individuals. We include in this latter category those features of the individual, which are amenable to capture by new technologies such as bio-metrics and bio-dynamics.

The aim of this paper has been to reflect the issue of identity management against an important recent case. A clear relationship is being made in the UK between citizenship, national identity and the possession of an identifier embodied in a national identity token. Turner (Turner, 1993) defines citizenship ‘as that set of practices (juridical, political, economic and cultural) which define a person as a competent member of society, and which as a consequence shape the flow of resources to persons and social groups’. In the UK national identity card debate possession of such a token (authentication) is proposed as evidence of citizenship (identification), which in turn will confer a range of rights and obligations on the individual (enrolment) – rights to healthcare, obligations to pay tax etc. Since the distribution of rights and obligations is increasingly moving on-line there may be a move implicit in this agenda to equate citizenship purely with rights and obligations associated with such services.

The debate surrounding the introduction of the ‘entitlements card’ in the UK is useful in highlighting the importance of a common, universal identifier for persons in the nation state. Proposed benefits for the citizen include the introduction of a simpler and more convenient token of identity for authentication purposes. Benefits for government lie in clearer authentication protocols for service delivery and easier integration and inter-operability of information systems. Such infrastructure benefits, it is claimed, will lead to more efficient and effective human activity systems in government, particularly by those agencies tasked with law enforcement of various kinds. These are direct consequences of a national identifier potentially satisfying the features of a good identification system since it would be universal, unique, permanent, indispensable and exclusive.

However, the existence of such an identifier and its associated token raises a vast range of issues and concerns. Most such concern centres around the potential such technology poses to the citizen’s right to personal privacy in general and data privacy in particular. Opponents of this introduction also argue that the considerable financial cost expended on the introduction of an identity management

infrastructure could not be justified in terms of the claimed rationale of tackling identity fraud in areas such as illegal immigration and terrorist activity. Indeed, many on this side of the debate point to the experience of countries such as Spain with an established identity card system but with comparable levels of illegal immigration and terrorist activity to the UK.

It is interesting that the issue of identity management appears to have been largely ignored by Information Systems academy. Perhaps some of the reasons for this are contained in the attitude that the introduction of national identification is 'throwing technology at complex social problems' (Clarke, 1988). Without denying the truth of elements of this attitude we would argue that the increasing rise of the e-Government agenda, as an important facet of the larger Information Society, has provided a new vigour to debates surrounding personal identification. The issue of identity management also offers a useful framing for a whole range of informatics issues surrounding individual-organisation interaction in the Information Society – data administration, data protection and privacy, information security, system integration and inter-operability – to name but a few.

REFERENCES

- Beynon-Davies, P. (2004). e-Business. Houndmills, Basingstoke, Palgrave.
- Burnham, D. (1983). The Rise of the Computer State. New York, Random House.
- Cabinet_Office (2000). e-Government - a strategic framework for the public services in the information age. London, Cabinet Office.
- Cabinet_Office (2002). Identity Fraud: a study. London, HMSO.
- Cabinet_Office (2002). Privacy and Data Sharing: the way forward for public services. London, Performance and Innovation Unit.
- Castells, M. (1996). The Rise of the Network Society. Mass., Blackwell.
- Checkland, P. (1999). Soft Systems Methodology: a thirty year retrospective. Chichester, John Wiley.
- Clarke, R. (1988). "Just Another Piece of Plastic in your Wallet: the 'Australian Card' scheme." Computers and Society **18**(1): 7-21.
- Clarke, R. (1994). "Human Identification in Information Systems: management challenges and public policy issues." Information Technology and People **7**(4).
- Guardian (2003). Explained: ID Cards, Guardian Unlimited.
- Home-Office (2002). Entitlement Cards and Identity Fraud: a consultation paper. London, HMSO.
- MapleLeafWeb (2003). National ID Cards: an international perspective, Maple Leaf Web.
- Ogden, C. K. and I. A. Richards (1923). The Meaning of Meaning. London, Routledge and Kegan Paul.
- Perri6 and I. Briscoe (1996). On the Cards: privacy, identity and trust in the age of smart technologies. London, Demos.
- Prabhakar, S., S. Pankanti, et al. (2003). "Biometric Recognition: security and privacy concerns." IEEE Security and Privacy: 33-42.
- Stamper, R. K. (1973). Information in Business and Administrative Systems. London, Batsford.
- Taylor, J. A. and H. Williams (1991). "Public Administration and the Information Polity." Public Administration **69**: 171-190.
- Thompson, G. F. (2003). Between Hierarchies and Markets: the logic and limits of network forms of organization. Oxford, Oxford University Press.
- Travis, A. (2002). National Card Games. The Guardian.
- Turner, B. S. (1993). Contemporary Problems in the Theory of Citizenship. Citizenship and Social Theory. B. S. Turner. London, Sage: 1-18.
- Zorkadis, V. and P. Donos (2004). "On Biometric-Based Authentication and Identification from a Privacy-Protection Perspective: deriving privacy-enhancing requirements." Information Management and Computer Security **12**(1): 125-137.