Human Identification in Information Systems: Management Challenges and Public Policy Issues

Roger Clarke

Principal, Xamax Consultancy Pty Ltd, Canberra

Visiting Fellow, Department of Computer Science, Australian National University

Published in Information Technology & People 7,4 (December 1994) 6-37

This document is at http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Abstract

Many information systems involve data about people. In order to reliably associate data with particular individuals, it is necessary that an effective and efficient identification scheme be established and maintained. There is remarkably little in the information technology literature concerning human identification. This paper seeks to overcome that deficiency, by undertaking a survey of human identity and human identification. The techniques discussed include names, codes, knowledge-based and token-based id, and biometrics.

The key challenge to management is identified as being to devise a scheme which is practicable and economic, and of sufficiently high integrity to address the risks the organisation confronts in its dealings with people. It is proposed that much greater use be made of schemes which are designed to afford people anonymity, or enable them to use multiple identities or pseudonyms, while at the same time protecting the organisation's own interests.

Multi-purpose and inhabitant registration schemes are described, and the recurrence of proposals to implement and extent them is noted. Public policy issues are identified. Of especial concern is the threat to personal privacy that the general-purpose use of an inhabitant registrant scheme represents. It is speculated that, where such schemes are pursued energetically, the reaction may be strong enough to threaten the social fabric.

Contents

- Introduction
- Human Identity and Human Identification
  - Human Identity
  - Human Identification
- Organisational Needs For Formal Identification
- Bases for Formal Identification
  - Names
  - Codes
  - Knowledge-Based Identification
  - Token-Based Identification
  - Biometrics
- Management Challenges
  - Desirable Characteristics of a Human Identifier
  - Effectiveness of the Available Identification Bases
  - Identification Schemes in Organisational Information Systems
  - The Scope for Anonymous and Pseudonymous Transactions
  - Conclusion
- Multi-Purpose Identification Schemes
  - The Concept
  - Inhabitant Registration Schemes in Continental Europe
  - Countries with British Legal Backgrounds
  - Current Developments
- Public Policy Issues
  - Inherent Objections to Identification
  - Risks in Multi-Purpose Identification Schemes
- Conclusions

Introduction

Introduction

Human identity is a delicate notion which requires consideration at the levels of philosophy and psychology. Human identification, on the other hand, is a practical matter. In a variety of contexts, each of us needs to identify other individuals, in order to conduct a conversation or transact business. Organisations also seek to identify the individuals with whom they deal, variously to provide better service to them, and to protect their own interests.

The use of human identification in the personal data systems used by organisations is remarkably little-discussed in the information systems literature. The purpose of this paper is to make good that gap, by undertaking a survey of the topic, and identifying matters of concern to managers and policy-makers.

The survey is based on 25 years of professional experience in information systems, literature searches, and 20 years of research and advocacy in the areas of data surveillance and information privacy, which has necessarily involved considerable work in relation to the question of human identification. The paper focusses on the identification of humans. The following related matters arise, but are not the focal point of discussion:

- the identification of products and packaging;
- the identification of vehicles;
- the identification of animals;
- forms of identification which show a category to which a person belongs, rather than specifying the individual;
- the gathering and use of information about identified individuals; and
- restrictions on individuals' movements, actions and behaviour.

The paper commences by outlining the concepts of human identity and human identification, and examining the reasons why organisations need to identify people. The various forms of identification are then presented. This includes discussion of names, codes, knowledge-based and token-based identification, and various kinds of physical characteristics which are encompassed by the term 'biometrics'. On that basis, the nature of the challenge to management is able to be drawn out. Finally, a discussion of multi-purpose identification schemes leads into an assessment of public policy issues arising in relation to human identification.

Human Identity and Human Identification

* Human Identity

In the context under discussion, identity is used to mean "the condition of being a specified person" (Oxford, 1976, p.533), or "the condition of being oneself ... and not another" (Macquarie Dictionary, 1981, p.879, definition 3 of 9). It clusters with the terms 'personality', 'individuality' and 'individualism', and, less fashionably, 'soul'. It implies the existence for each person of private space or personal *lebensraum* , in which one's attitudes and actions can define one's self.

Since the Renaissance, individuality and human identity have become central to our modern conception of mankind. The later stages of the industrial age have enabled the majority of the population to become concerned far less with survival, and far more with 'the higher things in life', such as 'self-fulfilment'.

The integrity of the individual has become central to western civilisation. It is the justification for our horror at the Nazi persecution of the Jews, at terrorist treatment of hostages, and at totalitarian regimes' arbitrary imprisonment and torture of dissidents. It is the reason for careful expression of human rights in documents like the U.S. Constitution, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

The dictionary definitions miss a vital aspect. The origin of the term implies equality or 'one-ness', but identities are no longer rationed to one per physiological specimen. A person may adopt different identities at various times during a life-span, and some individuals maintain several at once. Nor are such multiple roles illegal, or even used primarily for illegal purposes. Typical instances include women working in the professions, artists and novellists, and people working in positions which involve security exposure (such as prison warders and psychiatric superintendents).

* Human Identification

The term 'identification' means the act or process of "establishing the identity of, [or] recognising", or "the treating of a thing as identical with another" (Concise Oxford Dictionary, 1976, p.533), or "the act [or process] of recognising or establishing as being a particular person", but also "the act [or process] of making, representing to be, or regarding or treating as the same or identical" (Macquarie Dictionary, 1981, p.879).

For the purposes of record systems, these definitions are rather abstract and unhelpful. Information Technology Dictionaries are of little or no assistance; for example, the Penguin Dictionary of Computers (1985, p.221) provides no definition for human identity or identification, and the definitions for 'file identification' and 'file identifier' both depend on the meaning of the word 'identify', which is not defined.

In the context of information systems, the purpose of identification is more concrete: it is used to link a stream of data with a

In the context of information systems, the purpose of identification is more concrete: it is used to link a stream of data with a person. Hence this paper adopts as its operational definition:

> *human identification is the association of data with a particular human being*

Identification is applicable to data stored in structured, tangible and manageable form, as in corporate databases and documentary filing schemes; but also to data stored in less formal ways, as in private notes; and in incorporeal form, as in ballads and human memory.

The original needs for identification were social rather than economic. The social dimension of human culture is reflected by the idea of a person 'identifying' with a group. Indeed, group-membership ('one of us' or 'one of them') was probably a far more important matter than individual identity ('I', 'you' or 'he') throughout pre-historic times and most of the historic era.

Relatives, friends and acquaintances recognise a person on a contextual basis, in which physical appearance, voice characteristics, knowledge of private information, location and espoused name all play a part. These features are not individually reliable, they only work when the people involved are in close proximity, and they depend upon human memory, with all its vagaries. They are, however, sufficient for most social purposes.

As the complexity of economic transactions developed, the need arose for parties to know with whom they were dealing. It became normal for parties to provide one another with information about themselves, appropriate to the nature of the transaction. This may have been an explicit identifier (e.g. of the property the person owned, such as 'the Dalkeith', or perhaps of the person himself, e.g. 'Arthur, King of the Britons'). Alternatively, a number of pieces of information might together identify the person ('meet me at the bar on the corner in ten minutes; I'll be wearing a red carnation in my lapel'; or 'you'll always find me in this corner of the market on Tuesdays. Ask Beowulf at the next stall - he'll vouch for that').

The purposes of the interchange of identification include to provide a gesture of goodwill, to develop mutual confidence, and to reduce the scope for dishonesty; to enable either person to initiate the next round of communications; and to enable either person to associate transactions and information with the other person.

If identification is to be more than casual and unreliable, it must have an adequate basis. There are several types of evidence which could be used. Some depend on intrinsic or physiological characteristics of the person, others on more abstract information. In practice a person is accepted as being the person to whom a record relates because they represent themselves as being that person, they know things that in the normal course of events only that person would be expected to know, they do things (like paying money) that would only be in the interests of that person to do, or they are in possession of a document or token which it is reasonable to expect that, and preferably only that, person to have. In practice, it is common to use various techniques in combination.

Literatures of many ages and cultures have taken advantage of the scope for mistaken identity, with Shakespeare and Gilbert & Sullivan providing manifold examples. All identification mechanisms are fraught with difficulties, and hence the vast majority of transactions involve risk. They also cost money. A primary purpose of this paper is to provide a basis whereby individual organisations on the one hand, and policy-makers on the other, can use rational processes to implement schemes which balance the costs, the benefits and the risks involved.

Organisational Needs For Formal Identification

Identity and identification are vague and ambiguous. They continue to be treated with considerable looseness by most legal systems, particularly those whose origins can be traced to Britain. For social purposes, informal, contextual identification is sufficient. There are also many circumstances in which informal identification, or even none at all, suffices for economic transactions. This is generally the case for transactions which are completed in a single step, as is the case with both barter and sales for cash, and in other circumstances, where the costs of errors are negligible, or the party bearing the risk of an identification error does so willingly.

In some situations, however, organisations have a need for reliable identification of the individuals they deal with. The reason may be to protect the individual; for example, a record of any allergies the individual may have to drugs and particularly anaesthetics, and of drugs which the person is currently taking. More commonly, the purpose is to protect the organisation; for example, to ensure that the person can be contacted and located in the future in the event that he or she does not fulfil an obligation such as payment of a debt; or to guard against a person misrepresenting their status, e.g. their educational qualifications, age, income or medical condition.

The twentieth century has seen a vast growth in organisational size, and in distance between organisations and people. Organisations have increasingly assumed that there is a need for large quantities of identified data about people. This 'information-richness' has assumed the dimensions of an imperative, to the extent that individuals who demur when asked for evidence of identity are frequently presumed to 'have something to hide'.

Organisations often assume that a one-to-one relationship exists between persons and identities, no matter how many different

Organisations often assume that a one-to-one relationship exists between persons and identities, no matter how many different roles he or she may play, or choose to adopt. There are exceptions, however, in a variety of contexts; for example, many banks and insurance companies have only recently adopted 'client-oriented' approaches (whereby all accounts or policies which each individual has with the company are recorded against a single identifier, rather than being scattered around the company's divisions and branches); and employees who are also customers of their employer frequently have distinct employee and customer codes.

Implicit within many of the issues discussed in this paper are the questions as to when anonymity is unacceptable and identification necessary; and in what circumstances the restriction of a person to a single identity is appropriate.

Bases for Formal Identification

A variety of means is available for identifying a person, in order to associate data with them. These include:

- appearance - or how the person looks;
- social behaviour - or how the person interacts with others;
- names - or what the person is called by other people;
- codes - or what the person is called by an organisation;
- knowledge - or what the person knows;
- tokens - or what the person has;
- bio-dynamics - or what the person does;
- natural physiography - or what the person is; and
- imposed physical characteristics - or what the person is now.

This section of the paper commences by examining identification using names and codes. Identification based on knowledge and tokens is then discussed. Finally, it considers the cluster of 'biometric' techniques that depend on appearance, social behaviour, bio-dynamics, physiography and imposed physical characteristics.

* Names

The nature of names is tightly bound up with the cultural and legal environment. The discussion in this section is oriented towards those countries whose traditions originate in Great Britain. The situation may be quite different in other countries, such as those in continental Europe, in other areas influenced by the Code Napoléon, and in Arabic and East Asian nations. The primary references used were Fox-Davies & Carlyon-Britton (1906), Josling (1980), Halsbury (1981) and Robinson (1986).

In english-language cultures, names generally comprise one or more Christian, first, given or fore-names, and a one-word (sometimes two-word or hyphenated) surname. In Britain, a 'Christian name' was and is that provided at the time of baptism. If the child was not baptised, or no name was given at baptism, then a name is gained by 'repute', i.e. by usage. Whether or not a person has a Christian name, and whether or not he or she uses it, alternative and additional names may be used, without restraint by the law. In short, there is nothing illegal about the use of an alias or 'aka' (also-known-as), although acts which involve the use of an alias may be.

Surnames are of more recent origin than given names. They were originally written above the Christian name, and the term 'surname' derives from the French 'surnom' implying 'above'. There is no evidence of surnames being used in Britain before the Norman Conquest in 1066. They were initially descriptions, and related to the land the person owned, as in Simon 'de Montfort'. By about 1200, it had become normal for the small minority of land-owners to use surnames, and for them to be hereditary family names, i.e. passed from parent to child, generally (although never quite exclusively) through the male line.

In 1465, Edward IV created what appears to have been the first statute law relating to names, by requiring that every Irishman take to himself an English surname. One of the key steps in entrenching the use of surnames was the requirement enacted in 1538, in the reign of Henry VIII, that (Anglican) parish priests keep registers of births, deaths and marriages. Birth entries were to include the surnames of the parents.

Registers remained the responsibility of the clergy until 1837, when the Births and Deaths Registration Act made it a civil matter. In many jurisdictions, the surname of the child was implicitly assumed to be that of the father, if born in wedlock (children born out of wedlock technically did not have a surname, although they commonly gained their mother's or adoptive parents' surname by repute). In New South Wales, for example, it was only in 1966 that the surname of the child began to be recorded on the Register.

Over a period of centuries, the need for and use of surnames worked its way down through the classes. For people who did not own land, the primary sources of surnames were:

- locality or territory (e.g. Bywater, Styles, Ashurst, Attwood, Heath, Kent);
- offices, and later occupations and trades (e.g. Butler, Clark, Smith, Cook, Fletcher, Thatcher, Mason, Slater, Miller, Foster);

Foster);
- parentage, predominantly in the male line (e.g. -son, Mac-, O'-); and
- nicknames (e.g. Black, Fox, Wise, Hardman, Russell).

In most english-speaking countries, there has never been any legal compulsion for a married woman to adopt her husband's surname. However it has been traditional to do so, and this was reinforced by the (until quite recently) almost universal application to children born in wedlock of their fathers' surname. A small proportion of women continue using their name after marriage, although some do so only in the workplace, and choose to be known socially by their husband's surname. There is nothing to prevent a woman from adopting the name of a *de facto* spouse, and for convenience some do, at least for some purposes.

The contemporary concern with gender equality is not the only demonstration of the flexibility of names, and of the many-to-one relationship between names and individuals. People in security-sensitive positions (such as staff in prisons and psychiatric hospitals, and operatives and managers for espionage and counter-espionage agencies) use multiple identities as a means of protecting themselves and their families. Actors, authors and playwrights use multiple identities in order to more readily take advantage of artistic licence.

It is important to appreciate that the name is distinct from the person; for example, the validity or criminality of any act is unaffected by the use of a name: " ... (provided always that no question of deception or fraud enters into the matter) an act done in any name holds for good or bad equally with an act done in a genuine name" (Fox-Davies & Carlyon-Britton, 1906, pp. 41, 51, 8).

Under the common law, anyone may take on whatever surname, and as many surnames, as he or she pleases. In various jurisdictions, exceptions to that rule have been created by statute. For example, the Australian Aliens Act at s.11 prohibits residents of Australia who are not citizens from changing their names without first obtaining written permission from the Minister of Immigration; and the Change of Name Regulation Act 1923 of the State of Western Australia requires that changes of name be evidenced by executing and registering a Deed Poll. It does not appear that such requirements are widely known, honoured, or enforced.

It is curious that, despite all the complexities of law regarding the registered name-at-birth, in few jurisdictions is there any compulsion to ever use it, and it has very limited official force. In general, a person is free to establish any name 'by reputation', that is to say, by using it consistently, if only within some particular context. Legal mechanisms are available whereby a person may evidence that he has changed his name, or that he consistently uses a name, in particular the deed poll.

The effect is that, with minor exceptions, there may be such a thing as 'the legal name of a person', but there is no compulsion to use it, and no prohibition on using any other name or names instead, or as well. Examples of this are seen when the press reports that a person has been arrested and charged with a variety of offences in a variety of States under a variety of names. A person may, in general, use any name he or she wishes to, provided he or she does not thereby attempt to defraud.

As a basis for identification, names lack constancy and reliability. Moreover, many other difficulties arise. The legal and administrative systems of many countries in which anglo-saxon-celtic traditions dominate continue to have difficulty with non-European names, which may, for example:

- have different sequences (e.g. <family name> may appear first);
- have additional components in the name (e.g. a name of religious rather than identificatory significance);
- be incomplete (e.g. there may be no <family name>);
- be assigned in unfamiliar ways (e.g. the surname may come from the matriarchal rather than patriarchal line, or by leap-frogging generations);
- change in ways or at times foreign to local traditions (e.g. at puberty); and
- be variable depending on the context (e.g. by omitting the religious component).

In some cultures, a relatively small number of first-names are prevalent (e.g. John and James in Anglo-Saxon communities), and in others a small number of surnames may dominate (e.g. Kim in Korea, Ng and Nguyen in Vietnam, and Singh universally among Sikhs). As a result, many duplications of name arise.

A further challenge arises from mis-spellings and variations. In some cases these are initiated or enforced by organisations with whom the person deals, which may have difficulties with transliteration from a non-Roman script, or from a Roman script which uses diacritics such as ç, ü and ø, or in handling long series of consonants (such as "...wrysczwicz"). The unilateral actions of immigration officers at Ellis Island off Manhattan are reputed to have contributed greatly to the enormous richness of surnames in the U.S.A. Various techniques are used by organisations to cope with these difficulties, such as 'phonex' algorithms to deal with homophone (like-sounding) names. Specialised software packages combine these techniques to assist large organisations in matching new transactions with existing data.

In order to cope with these uncertainties, it is common to use further data as additional elements of the identification, or as confirmatory data. Most common among these are data of birth (which suffers from being, for some people, particularly

confirmatory data. Most common among these are date-of-birth (which suffers from being, for some people, particularly sensitive), and address. Address is also sensitive for some people, and is volatile. In developed countries, it is not uncommon for 10-15% of the population to be at a different address from where they were one year earlier.

In short, names are a challenging and risky foundation on which to build an organisation's id system.

* Codes

To cope with the vagaries of name-based identification, it is common for organisations to create coding schemes. These are commonly based on a set of digits, but may incorporate alphabetic characters.

A major reason why identification codes are of value to organisations is that their issue can be controlled, and hence the uniqueness of the code assured. It is common to not only assign a code to each person with whom the organisation deals, but also to request them to remember it (see the following section on knowledge-based identification), and to issue them with a token bearing the code, and request them to have the token with them when they conduct transactions with the organisation (see the subsequent section on token-based identification).

It is possible to build some degree of internal and external validity checking into an id code. For example, it can carry a check-digit, such that, at the point of data capture, a simple computation will (generally) detect a invalid code; or it may include, in clear or in hidden form, some characteristic of the person, such as their year of birth, gender, location of residence, or pension status, enabling alert counter-staff to detect possible errors, or fraudulent or criminal behaviour.

Codes may be devised in such a manner as to be readily human-readable, machine-readable, or both. Bar-coding is a currently popular means of recording codes on products and packages in such a way that devices can read the code, and card-borne magnetic stripes and memory-chips can also contain identification codes.

* Knowledge-Based Identification

People may be recognised by demonstrating that they are in possession of information which only that person would be expected to know. Examples of data used for this purpose are one's family and given names, prior names, father's name, mother's name, mother's and grandmothers' maiden names, date and place of birth, address, marital status, religion, and occupation. There have even been proposals to apply astrology, in the form of the person's spouse's zodiac sign. Identification on the basis of such information suffers from the problems that some people just do not know (e.g. orphans and refugees), some forget, and any such information is or can be known by other people. It results in many errors, of commission and omission, and of false-inclusion and false-exclusion.

Passwords are a very common application of knowledge-based identification. Another is the Personal Identification Number (PIN) used in conjunction with Automatic Teller Machines and merchants' EFT/POS terminals. Imposed passwords and PINs are not easily memorised and are easily forgotten. As a result, a significant proportion of the population records them on or near the card whose unauthorised use it is supposed to prevent, reducing the effectiveness of the identification scheme. User-nominated passwords and PINs may be more readily guessed by an imposter, but less likely to be stored adjacent to the card or terminal.

Knowledge-based approaches to personal identification seldom provide organisations with an adequate basis for the operation of their information systems. They can have some value as a means of secondary, correlative confirmation of identity, particularly in relatively low-security contexts.

* Token-Based Identification

A 'token' is some 'thing' which a person has in his or her possession, in particular documentary evidence. Commonly used documents are birth and marriage certificate, passport, driver's licence (or in most states of the U.S., non-driver's licence), employer-issued building security card, credit card, club membership card, statutory declaration, affidavit, or letter of introduction.

The passport is a particular token which is popularly regarded as being especially reliable, and this section commences by considering it as an example of documentary evidence. Important sources used included Ehrlich (1966), Thornberry (1974) and Stewart (1982), but see also Turack (1972).

A passport was originally a document, provided by a sovereign to an individual, which requested officials at borders and in seaports to permit the bearer to enter. The notion was known to English law at least as early as 1300. At the end of the nineteenth century, passports were issued on request, by the governments of various countries. Their purpose was to provide evidence of nationality, and, by implication, of identity; but there were few circumstances in which it was actually necessary to have one, even when crossing national borders. After World War I, in a climate of mass movements of displaced persons, it became increasingly common for governments to demand documents which evidenced a person's nationality. An international conference in 1920 established the present passport system.

During the inter-war period, the passport became a near-universal requirement for international travel. It has remained so, even though many aspects of the system are inadequate or inappropriate for contemporary use. Measures are in train to overcome some of its deficiencies. Meanwhile, within some communities of nations, and especially within the European Union, it is being progressively supplanted by alternative forms of identification.

The issue of passports, and indeed of all forms of documentary evidence of identity, depend on some 'seed' or 'breeder' document such as birth, naturalisation, residence, or immigration papers. It is therefore important to appreciate the nature of the most fundamental of these, the birth certificate.

In Britain, from the Middle Ages, the church recorded events of significance in ecclesiastic law, and in particular birth, baptism, marriage and death. In 1538, both the recording of the event and the maintenance of the register were made a civil responsibility of the parish (the lowest level of ecclesiastic organisation). The coverage of events was highly variable, both between parishes, and, over time, within each parish.

These events came to take on various kinds of secular significance. For example, they are now used in establishing entitlements (e.g. patriality, retirement age, age for insurance purposes); and in determining freedom to marry (based on age and previous marriage). In 1837, the function of maintaining the registers was assumed by the State. The data collection functions are generally performed by doctors, hospitals and marriage celebrants, but also to some extent by individuals.

There are very limited protections against a person, other than the person to whom the facts relate, acquiring a copy of a birth certificate. The law and practice relating to the issue of certificates is fairly consistent across most common law countries, for example:

> *An application for a copy of or an extract from a Birth Certificate shall be: in writing signed by the applicant; contain sufficient particulars to enable the search to be made; and specify the reason for which the search is required. Where the Registrar is of the opinion that a ... copy or extract is required for an improper reason ... , he may refuse to ... issue the copy or extract after Sections 51(2) and (4), A.C.T. Registration of Births, Deaths and Marriages Ordinance 1963. All Australian State and Territory laws are very similar to this.*

Thus, although Registrars may have the authority to refuse to issue a Birth Certificate, there is no onus on them to satisfy themselves about the person's identity or reasons for wanting it. Moreover, if Registrars were given any greater responsibility than they already have, many individuals would suffer great inconvenience in getting copies of certificates.

The position has been summarised as follows: " ... a tendency has developed in the community to regard a birth certificate as evidence of identity. It clearly is not evidence of identity. Without evidence to connect a person with the person named in the birth certificate, the certificate establishes nothing about that person. It is easy to obtain from any of the registries ... a birth certificate relating to another person without that person's knowledge. It matters not whether the other person is living or dead" (Stewart, 1982, p.56).

A variety of more specific problems arise. For example, in respect of the approximately 20% of Australia's population born outside the country, it is necessary to use a seed document other than an Australian Birth Certificate or Register entry. Some 7.5% of the population is British-born, and British Birth Certificates suffice. The remainder come from many different countries with many different traditions of birth registration. For many of them, birth certificates are unavailable, or their form is unacceptable to Australian authorities. There are some 2 million such people, including the majority of the estimated 60-100,000 illegal immigrants. For those whose Birth Certificate cannot be used as a seed document, it is therefore necessary to interpolate the use of various of the Department of Immigration and Ethnic Affairs' documents or data systems. These include the Citizenship Register (for those already naturalised), and arrival cards and visa register entries.

Another consideration in Australia is that multiple Registers of Births, Deaths and Marriages operate, and are functionally and geographically independent. There has generally been no contact among the 8 State and Territory Registrars in relation to particular individuals, and no attempt to correlate death certificates back to the corresponding birth certificates. In any case, later events could be directly related back to births only where the event occurred in the same state as the person's birth, and the name was recorded in the same manner as at birth. The situation is similar in many other countries.

The difficulties of associating death certificates with the corresponding birth entries are exacerbated by the transient nature of names. As was discussed earlier, there is no obligation for a person to ever use the name in which his or her birth was registered. It is generally not obligatory for change of name to be registered with anyone, let alone Registrars of Births. It is not uncommon for a person's death to be recorded under a name different from that on their birth certificate. There are therefore severe impediments to cross-relating deaths back to birth entries.

Another class of document which is much-used in some countries as evidence of identity is the driving licence. It is commonly sought in many countries as a supporting document, and in some cases even the primary document, despite the absence of any obligation on the part of the licence-issuing authority to undertake any substantial integrity assurance measures. In recent years, photographs have joined signatures as a means of enabling people to whom the document is produced to satisfy themselves that the person presenting the token is probably the same person as that to whom it was issued.

the person presenting the token is probably the same person as that to whom it was issued.

In summary, seed documents attest only to the facts concerning some event. Nothing intrinsic to them associates them with any particular person. Any reliability they may offer in identifying a person must therefore come from some other source. In most cases, it is not even practicable to prevent the same seed document from being used to create several different identities. This could only be achieved if each data system contained some control mechanism which ensured that each document was used only once as a basis for the creation of an entry. I use the term 'the entry-point paradox' to refer to the problem of low integrity being propagated from seed documents onwards to derivative documents.

Stories about 'false identities', how they are used, and how they are constructed, are stock-in-trade for journalists, and re-surface continually in various guises. A particularly lucid explanation of how identities are built by exploiting the entry-point paradox was provided in a 'Sydney Morning Herald' (9 April 1993) report on a District Court judgement against a pensioner who had defrauded the Department of Social Security of $400,000. The defendant had claimed he was born overseas, obviating the need for a birth certificate. He adopted multiple names. For each name, he entered himself on the Electoral Roll, obtained a Tax File Number and submitted a tax return (for amounts which did not incur the payment of tax), nominated on various application forms the names of various companies as previous employers, visited doctors and acquired various certificates from them, and using these obtained membership of a roadside assistance association, insurance policies, union membership, Medicare and government concession cards. An Appendix to FACFI (1976) and Hibbert (1992) also provide insights into the twilight world of 'false identities'.

Generalising, a relatively high-integrity identity is constructed by accumulating a collection of low-integrity evidence. Even people who are responsible for nominally high-integrity schemes accept accumulations of data as being sufficient evidence, especially for people whose (apparent) background suggests that they will have difficulty producing 'harder' evidence; these organisations know that ultimately they would have to anyway.

Token-based schemes are of value in tightly controlled environments, as a variant on the 'turnaround document' approach: the person first presents at a counter, then must wait in a large, anonymous area prior to visiting the counter a second time. If an identifier is issued on the first occasion, and interchange or theft of the identifier is unlikely, then its presentation on the second occasion will be fairly reliable 'proof of identity' within that limited context. Generally, however, schemes based on tokens alone are of limited integrity. To overcome the deficiencies, it is necessary to have adequate means of associating the token with the person to whom it relates, and of detecting attempts by others to use it.

* Biometrics

The term 'biometrics' is used to refer to any and all of a variety of identification techniques which are based on some physical and difficult-to-alienate characteristic. They are sometimes referred to as 'positive identification', because they are claimed to provide greater confidence that the identification is accurate.

Among many other instances in the animal world, mice and penguins are capable of using their olfactory senses, aided to some extent by other cues, to very reliably recognise their parents and their progeny, even among large populations packed into a small space. Humans with such capabilities appear to be limited to those whose other senses are severely impaired, such as the blind and deaf Helen Keller (Young 1988). Hence biometric techniques involve 'metrics' or measurements of some kind, rather than depending merely on informal or subliminal methods. Exhibit 1 presents a classification scheme and examples of biometric techniques.

The natural physiological characteristics traditionally employed by the international passport system are fairly gross, and are seldom sufficient to reliably identify a person. Teeth and skeletal injuries and repairs are used in forensic applications, although they are of little use for routine identification. Anyone who has played the various party-games involving blindfolded recognition of their partner's knees (or other body-parts) will attest to the difficulty of recognising even close friends by means other than facial appearance, voice, and above all the correlation of appearance and behavioural characteristics.

Exhibit 1: A Taxonomy of Biometric Techniques

- **appearance** (e.g. the familiar passport descriptions of height, weight, colour of skin, hair and eyes, visible physical markings; gender; race; facial hair, wearing of glasses; supported by photographs);
- **social behaviour** (e.g. habituated body-signals; general voice characteristics; style of speech; visible handicaps; supported by video-film);
- **bio-dynamics** (e.g. the manner in which one's signature is written; statistically-analysed voice characteristics; keystroke dynamics, particularly in relation to login-id and password);
- **natural physiography** (e.g. skull measurements; teeth and skeletal injuries; thumbprint, fingerprint sets and handprints; retinal scans; earlobe capillary patterns; hand geometry; DNA-patterns); and
- **imposed physical characteristics** (e.g. dog-tags, collars, bracelets and anklets; brands and bar-codes; embedded micro-chips and transponders).

Some of these features change naturally over time, such as hair colour, height and weight. Natural changes can be enhanced or retarded by such means as tinting, platform shoes and dieting. Some are fairly readily changed, whether for personal whim, or as an explicit attempt to change appearance; for example, contact lenses change eye-colour, the shape of glass-frames has the effect of changing the shape of the face, and changed facial hair styles (including beard, moustache, sideburns, eyebrows and eyelashes) make physical identification quite difficult. Gross devices like wigs, body-padding and cosmetic surgery can be of assistance in the endeavour to deceive, but frequently the pattern adopted by the scores of facial muscles is more effective.

Most such attempts to change appearance are an endeavour to communicate, perhaps even to achieve, change in some aspects of identity. Although intentionally 'deceptive', only a very small proportion would be regarded as 'acts of deceipt', or are undertaken in order to effect criminal fraud.

Photographs, although not originally intended for the purpose, can be used as evidence of identity. Photographs provide a gross representation of part of a person's physiognomy or facial features, at a particular point in time, and under particular lighting conditions. Depending on their size, the fineness of grain, and the precision of the reproduction media, and on whether it is in monochrome or colour, a photograph may be a more or less faithful representation, in two dimensions, of a historical three dimensional reality. It may therefore be a more or less fair guide to the past appearance of a person from a particular perspective, under particular conditions. For the reasons discussed in the previous paragraphs, a photograph is a highly unreliable means of recognising a person at a later time, particularly if the person is seeking to avoid being recognised. The internal passport scheme in the U.S.S.R. attempted to surmount this obstacle by containing three photographs taken at three different ages.

All such relatively informal appearance- and behaviour-based schemes can assist in detecting an imposter, but are not reliable for that purpose. They are of limited use in confirming that the person presenting is the right one.

In addition to gross features, others of a far finer nature enable more precise identification. Thumbprints, individual fingerprints and sets of fingerprints have been used since the end of the nineteenth century in matters of a criminal nature (Wilton 1938, Moenssens 1969, Vic CCPPI 1987). In relatively free countries, the situation generally is that there is no authority for the compulsory provision of fingerprints, unless they are being charged with a criminal offence; and there is no authority for the prints to be retained unless the charge is pursued and the offence proven. A few countries, however, including the U.S.A., apply fingerprinting in other areas such as immigration matters.

Linear measurements of parts of the body (anthropometrics) are also feasible, but have proven difficult and have seldom been used until recently. Early examples were the use of cranial measurements in attempts to correlate head-shape with race and with psychological measures. These were interests of various German scientists during the last two centuries, under the influence of liberal interpretations of Hegel and Nietzsche. More recently, hand measurements and three-dimensional optical scans of the index finger have been used as the basis for commercial products.

For many years, forensic scientists have used genetic testing of various kinds as aids to identification, but because, for example, blood-groups are shared by many people, none of them represented a precise identifier. A small portion of the human genome is believed to be all but unique in all cases except identical twins. Based on this assumption, a method of identification based on patterns of DNA has been developed. It is variously referred to as DNA 'prints', 'typing' or 'profiling'. It was first used in 1983 in a United Kingdom case (Wambaugh 1989), has since been applied in many jursidictions, and has been generally accepted by the scientific community, the courts and the public as a very-high-integrity identification method. In at least the United States, this has led very quickly to proposals that national databases of DNA prints be established as the basis for a national personal data system, and applied to all manner of purposes (OTA 1990).

There are also imposed physical identifiers. Branding and tattooing have been employed at many times in history, usually in the context of slavery, racial subjugation or harsh criminal systems. Some schemes, on the other hand, have general community acceptance, such as the wearing of dog-tags by soldiers on active duty, and of id-cards by employees and visitors within secure premises. Even with these, however, concerns can arise regarding the uses to which they are put, such as the tracking of employees' movements throughout a working day.

Tags of various kinds are commonly used with manufactured goods, with packaging and containers, and with animals. There has been an increasing tendency in recent years to apply similar technologies to the design of collars, anklets and bracelets for institutionalised persons, including patients, particularly new-born babies and those who are comatose or suffering senile dementia), and prisoners in gaol, on day-release schemes, and on bail. There were proposals to use them for prisoners-of-war during the Gulf War.

Tags are passive, and need to be inspected. Some devices are designed to respond when queried using a radio signal, and others are active in the sense that under pre-programmed conditions they can transmit a message.

It has been technically feasible for some time, and is increasingly economically practicable, to implant micro-chips into animals for the purpose of identification and data-gathering. Examples of applications are to pets which may be stolen or lost, breeding stock, valuable stock like cattle, and endangered species like the wandering albatross. As the technology develops, there will doubtless be calls for it to be applied to humans as well. In order to discourage uncooperative subjects from removing or

doubtless be calls for it to be applied to humans as well. In order to discourage uncooperative subjects from removing or disabling them, it may be necessary for them to be installed in some delicate location, such as beside the heart or inside the gums.

Management Challenges

Many organisations no longer rely on their employees to recognise individual clients. They seek a means whereby individual humans can be recognised reliably, at a distance, over a period of time, without reliance on human memory, and (in some cases) despite the preference by the person not to be recognised. As Rule put it, " ... the problem of linking the client with his number, and hence with his data, remains a very difficult one" (1973, p.294).

Information systems have tended to use codes rather than names as the primary identification mechanism. As information technology develops, there are signs that artificial codes may be beginning to give way to natural names again. This is because processing capabilities with textual data are improving; so too are the handling of non-unique identifiers, of partial data and of partially incorrect data like mis-spellings; and key-based data management is being supplemented by, and may progressively be supplanted by, text-string-based and contextual access techniques.

In establishing their id schemes, organisations apply variants and combinations of the techniques described in the preceding section, in manners appropriate to the circumstances. It is vital that, in doing so, they appreciate the difficulties involved. Of especial importance is the need to achieve an appropriate balance between the harm arising from false-inclusions (i.e. the acceptance of imposters and mistaken matching), and from false-exclusions (i.e. rejecting or failing to recognise correct matches). This section highlights some of the considerations.

* Desirable Characteristics of a Human Identifier

It is remarkable in how few places in the literature criteria for assessing the quality of huamn identification have been seriously discussed (see, however, IBM 1969, NZCS 1972 and HEW 1973). In Exhibit 2, a set of criteria is proposed, whereby an organisation can assess alternative means of identifying people with whom it deals. Inevitably, these objectives exhibit internal conflict.

Exhibit 2: Desirable Characteristics of a Human Identifier

- universality of coverage
  - every relevant person should have an identifier
- uniqueness
  - each relevant person should have only one identifier
  - no two people should have the same identifier
- permanence
  - the identifier should not change, nor be changeable
- indispensability
  - the identifier should be one or more natural characteristics, which each person has and retains. If artificial, the identifier should be enforcedly available at all times
- collectibility
  - the identifier should be collectible by anyone on any occasion
- storability
  - the identifier should be storable in manual and in automated systems
- exclusivity
  - no other form of identification should be necessary or used
- precision
  - every identifier should be sufficiently different from every other identifier that mistakes are unlikely
- simplicity
  - recording and transmission should be easy and not error-prone
- cost
  - measuring and storing the identifier should not be unduly costly
- convenience
  - measuring and storing the identifier should not be unduly inconvenient or time-consuming
- acceptability
  - its use should conform to contemporary social standards

The term 'universal' has two distinct usages. In this paper, it means 'completeness of coverage of the relevant population'. In some documents, it means 'used by all agencies for all purposes', but for that purpose this paper uses the term 'general-purpose identifier'. There are also a number of writers, particularly in the press, who use the term in both senses, sometimes in the same sentence. The confusion is deepened because in some acronyms 'U' stands for 'universal', while in others it stands for 'unique'.

* Effectiveness of the Available Identification Bases

When assessed against the desirable characteristics, most natural physiological identifiers are universal and indispensable, but many are not unique, including facial appearance, height and weight, colour of eyes and skin. Many are not permanent, including marks and scars and handicaps, as well as height and weight. Gender is not unique, (in recent times at least) it is not necessarily permanent, and its collection may also conflict with social standards. Teeth and skeletel injuries and repairs are often distinctive, but are not unique, may be only semi-permanent, and are available only with intrusive examination. Although appropriate and accepted in post-mortems, they are otherwise not very practicable.

Measuring, collecting and processing natural characteristics involve serious problems. For example, tissue testing requires intrusive surgery, if only of a minor kind, and are only possible when the person presents themselves. Some techniques are feasible remotely, using high-quality video-transmission. Despite the great strides it is currently making, contemporary video technology cannot record and transmit copies of fingerprints sufficiently quickly and cheaply to enable their routine use. And despite the sophistication of satellite-image processing in military intelligence work and now land information systems, application of image-processing, codification and storage in personal data systems has made slow progress.

Fingerprints are associated with criminality, and in many countries would not appear to be currently acceptable for general usage. The feasibility of applying other forms of biometrics are also subject to technical, economic and social limitations. DNA-testing is expensive and slow, and involves the provision of tissue or specimens, which many people find demeaning, and which create logistics and security problems. Branding, tattooing and micro-chip implantation fulfil many of the prime requirements, but would not seem to be socially acceptable, at least at this stage.

Non-physiological information suffers worse problems. Names are not unique (although duplicates are sufficiently uncommon that cases of mistaken identity occasionally - and sometimes damagingly - arise because most people most of the time presume uniqueness). Names are also not permanent, and many errors are made in their recording and transmission. Date and place of birth are not unique, but are universal and permanent. For some people they are sensitive data. They are widely used as the prime means of distinguishing between duplicate names.

Race is amongst the most sensitive of all data, and anyway is not clearly defined. Address, marital status, religion and occupation are non-unique, non-permanent, ambiguously-defined, and in some cases, sensitive. Codes may be contrived to satisfy universality, uniqueness and storability, but they are very difficult to make indispensable, reliably collectible, and exclusive.

There is no basis for identification that fulfils all desirable characteristics.

* Identification Schemes in Organisational Information Systems

Organisations vary enormously in the care with which they apply human identification techniques to their needs. At one extreme, some organisations have no interest whatsoever, as in retail cash sales and public advisory bodies like tourist offices. At the other, a small number of organisations, mainly in criminal investigation and national security, depend upon the collection of fine-grained physical characteristics, traditionally fingerprints, but increasingly DNA-prints.

Many organisations depend upon documentary evidence when they establish a relationship with an individual. Thereafter they usually depend on the person's knowledge (e.g. of his name, his birth-date or his client-code), or on his ability to present a token issued by the organisation itself (e.g. a motor club card, or an automatic teller machine card), or on a combination of both.

Documentary evidence is treated by many administrators as though it were the, or even the only, authoritative basis for identification. In fact, as discussed earlier, all documents are dependent on a seed document, and the integrity of an identification scheme also depends on a provable relationship between the person and the document.

A common approach taken by many organisations is to seek a variety of information about a person, from a variety of sources, and, in the absence of inconsistencies or 'bad' references, accept the person as being identified by that loose set of data. For the majority of the population, and the majority of purposes, document-based identification schemes, supported by limited cross-checking, provides sufficiently reliable evidence of identity. Most people have no inclination to establish multiple identities, and for many of those who are interested in doing so, the effort, difficulty and cost outweigh the potential benefits; but for those with an axe to grind, a serious prank to play, or criminal intent, the effort is frequently perceived to be worthwhile.

The lack of integrity of most identification schemes is mirrored by the lack of regard paid to identification cards. No matter what care and expense is invested in the design and issue of cards, their potential for ensuring accurate identification of individuals is dependent on the assiduousness of gatemen and doormen. Anecdotes abound of the swapping of cards between bearded black-haired giants and petite blonde women; and of cards carrying the bearer's dog's photograph going undetected for long periods. Even in ostensibly medium-security environments, cards seldom contribute much to the accuracy of identification.

* The Scope for Anonymous and Pseudonymous Transactions

The contemporary organisational habit of requiring an identity appears to be of late-nineteenth and early-twentieth century origin, and to be derived from an increase in the size of the institutions, a decrease in the degree of trust between organisations and

and to be derived from an increase in the size of the institutions, a decrease in the degree of trust between organisations and individuals, and an increase in the incidence of long-term economic relationships.

In some circumstances, there are clear functional needs for the identification of individuals; for example when entering into loans and making repayments; and investing funds, and seeking interest payments and return of capital. There is also a fiduciary need for organisations providing income-support payments to individuals to know to whom it is being paid.

Corporations which actively market goods and services to consumers avidly gather information about them. During the last two decades, they have applied developments in information technology to sustain customer loyalty, encouraging them to buy more from them more often, by providing volume-based incentives. These 'frequent-buyer' and 'loyalty' schemes presume that the clients identify themselves to the company.

These mainstream activities have led to a presumption on the part of many organisations that they need to have identity in order to conduct almost any kind of transaction. There remain many circumstances, however, in which the identity of the person with whom an organisation performs transactions is of no consequence. In fact, the majority of the transactions undertaken between individuals, and between individuals and corporations, are still conducted anonymously. This includes most cash payment and barter transactions, and many legitimate transactions which have some sensitivity about them, ranging from the booking and the payment for services of prostitutes, and treatment at venereal disease clinics, to the purchase of gifts for one's spouse.

There are many additional circumstances in which identification is commonly assumed to be necessary, but may not be; for example, whether taxation authorities need the parties involved in every significant economic transaction to be identified depends entirely on the taxation mechanism used: a tax levied at a rate which depends on a cumulation of transactions (i.e. a progressive or regressive rate) may require identification of the parties; but one levied at a flat rate on each transaction does not.

With the dramatic increase in electronically facilitated transactions recently and in the coming decade, an increasing amount of effort is being invested in transaction techniques which protect the identity of one or all participants (e.g. Chaum 1985). One approach is 'anonymity', whereby none of the parties are aware of the identity of the others (e.g. in many stock exchanges, buyer and seller are never aware of who they sell to and buy from; and nor do they need to be). Another is 'pseudonymity', whereby the parties are aware of an identification code for the other party, and may be able to initiate contact with them using that code, but cannot associate that identity with any particular person. In effect, that person has multiple identities that correspond with particular roles he, she or it plays, and it is not possible to correlate the identities without the person's active cooperation.

Using such schemes, it is possible for a corporation which runs a loyalty scheme to achieve its ends without actually having details of its clients' identities. It is also feasible to implement schemes in which the parties are unaware of one another's identities, yet are secure in the knowledge that the goods or services, and the funds, have been transferred as agreed. For example, each party to the transaction may have to identify itself to the others while the transaction is conducted, but all parties may be precluded from recording the other's identity. Alternatively, schemes may be used that authenticate each party's eligibility to conduct the transaction (e.g. is a member of an appropriate class, or has a particular characteristic) without disclosing the party's actual identity.

* Conclusion

Organisations are confronted by enormous difficulties in devising high-integrity identification schemes. In practice, the difficulties do not prevent organisations from dealing successfully with their clientele. The dictum that most of the population is fairly honest most of the time, enables even organisations highly prone to cheating to operate successfully. For example, credit companies budget in advance for bad debts, and still make a profit. The challenge confronting each organisation, in respect of each information system it operates which involves people, is to devise an identification scheme appropriate to the particular set of circumstances. The design criteria are to enable information to be associated with, and/or action to be taken in respect of, the right person, with a degree of accuracy commensurate with the gravity of the information or the action.

In order to rationally decide on an identification scheme, an organisation should identify the alternatives, and apply an appropriate form of financial analysis or cost/benefit analysis (e.g. Thompson 1980, Gramlich 1981, Sugden & Williams 1985). Corporations have a financial incentive to do so, where the costs and/or benefits associated with the various alternatives are perceived to differ significantly. For public sector organisations, however, the incentives are often much less direct, and much less effective (Clarke 1994c).

Given that identification schemes are costly, and generally of only moderate integrity, organisations in both the public and private sectors need to familiarise themselves with anonymous and pseudonymous transaction techniques, and assess their applicability to their operations.

Multi-Purpose Identification Schemes

* The Concept

The analysis undertaken in the first half of this paper has been kept relatively simple by sustaining an implicit assumption that

The analysis undertaken in the first half of this paper has been kept relatively simple by sustaining an implicit assumption that each organisation operates its own, separate identification scheme. In fact, there may be significant advantages in multiple organisations using the same basis for identifying the individuals with whom they deal.

One apparent reason is cost. A single organisation can take responsibility for establishing the scheme (e.g. validating the credentials offered, establishing a code, issuing a token, maintaining the registers of codes and tokens, and performing integrity checks such as recording attempts to use credentials which have already been accounted for, and reflecting in the register such events as deaths, emigration and temporary 'non-person' status through, for example, imprisonment). All organisations might contribute to the costs of the id issuer, or the organisation might absorb them as costs of its own operation or a service to the community. Economies of scale can be gained if the equipment and software needed to check the tokens and capture the code are common.

An additional advantage of a multi-purpose scheme is that organisations which perform related functions can have an easy means of inter-relating the data they hold and collect about each individual. Moreover, the overall costs of that kind of operation would be lower, and hence it would become economic for more pairs and sets of organisations to share data about their clients. In the extreme case, a single, general-purpose scheme could be used by all organisations for all purposes, facilitating general-purpose use of personal data. Instances exist of both 'centralised' schemes, in which the register is held in a single location, and 'dispersed' schemes, in which the data is held regionally or locally.

Many multi-purpose schemes exist. Some of these are operated by the private sector, especially in relation to credit reporting schemes and insurance claim and claimant information systems, such as the U.S. Medical Information Bureau. The remainder of this section examines multi-purpose identification schemes operating primarily in the public sectors of various countries. A few of them make incidental use of a physiological characteristic (e.g. schemes in Singapore, Hong Kong, Malaysia and Spain have been claimed to store a replica of the thumb-print on the card). Some include a photograph, displayed on the card and/or stored in digital form in the register. Some cards carry the person's signature. To date, however, none appears to use a biometric as the major identifying feature; instead all depend on some other means of confirming that the person presenting a token is probably the person to whom it was issued.

* Inhabitant Registration Schemes in Continental Europe

Most countries in Western Europe operate a particular kind of multi-purpose system referred to in this paper as an 'inhabitant registration scheme'. Such a scheme provides all, or most, people in the country with a unique code, and a token (generally a card) containing the code. In most countries, the schemes are used for the administration of taxation, national superannuation and health insurance. In some, they are used to ensure that additional rights are exercised only by people entitled to them, such as the right of residence (especially the control of illegal immigration), and the right to work (especially to prevent unauthorised work by visitors). In Scandinavian countries, they are used for even more purposes, such as the administration of social welfare, banking, the enrolment of electors and the exercise of voting rights.

The first inhabitant registration scheme is generally understood to have been attempted by the French, after the revolution of 1789 (Walker 1986). The use of such schemes accelerated during the first half of the twentieth century. In some countries in 1939-40, especially the Netherlands, the existence of a detailed register was of considerable assistance to the Nazi invader, and resulted in the easy identification and location of many people targeted for the most extreme form of racial discrimination. Such experiences generated or reinforced distrust of efficient registration schemes in some European countries; for example, censuses in The Netherlands were abandoned in the 1980s, due to public opposition and the consequent low quality of data; and the inhabitant registration schemes in Austria, France and Italy are officially non-compulsory (despite which, or perhaps in part because of which, they are close to universal in coverage).

The misgivings are less apparent in Scandinavian countries. Widespread use of a single personal identity number in Sweden began in 1947, in the context of a census. Norway followed suit in the 1960s, and a similar arrangement was introduced in Denmark in 1968 (Blume 1990). One of the advantages claimed for it is that a periodic census is unnecessary, because statistics can be extracted from the national personal data system at the time they are needed.

In some countries, including The Netherlands, Switzerland and (at least at present) West Germany, the Register is stored in a dispersed manner, at the level of the municipality. All events deemed relevant by the authorities must be registered with the municipality. When the person moves across municipal boundaries, both the old and new municipalities must be informed, to enable data transfer to take place. In at least The Netherlands, passport issue is recorded against the munipical register (Stewart, 1982, p.60).

In general, there is not, or not yet, a requirement that individuals carry at all times a token evidencing their right to use a particular code. One exception in Western Europe is Belgium, where members of the police force have the power to arbitrarily require proof of identity from any person at any time. Under the most repressive regimes, such as those in Communist Eastern Europe, inhabitant registration schemes were instrumental in the prevention of unauthorised movement both within the country and out of it. Systems in post-communist eastern Europe appear likely to retain at least some similar characteristics (Clarke 1994b).

The absence of the power to demand evidence of identity weakens the integrity of a general-purpose identification scheme. It is only to be expected that various pressure-groups will seek to increase the impositions as time goes by, in response to such problems as illegal immigration, perceived worsening of law and order, epidemics, natural disasters, national security emergencies, etc.

The European Union (EU) continues to make efforts to 'harmonise' the various inhabitant registration schemes of its member-states sufficiently to enable each country's internal passport / identification card to be used for transit across EU borders, and perhaps even for residence and employment in other EU countries. The cultural and systemic differences are such that progress has not been easy.

* Countries With British Legal Backgrounds

In the United States, the Social Security Number (SSN) is operated by the Social Security Administration (SSA), for its own purposes. Many other agencies use the number and card for additional purposes, and there has been considerable use in business and in education. The SSN has a very substantial coverage of the population, but the integrity is very low (FACFI 1976, CG 1980, OTA 1981).

The history of the Social Security Number is instructive. As in most countries, there was a gradual increase in the reliability of birth registry information during the nineteenth and early twentieth century. By 1933, it was estimated that at least 90% of all births and deaths were recorded (Rule et al., 1980, p.31). This laid the foundation for an id scheme. Following the original Social Security Act of 1935, which imposed a tax on both employees and employers, an identifying number was established in late 1936, and employees were required to provide that number to their employers. The card that was issued bore the legend 'Not For Identification' (HEW, 1973, pp.114-122).

In 1943, the decision was taken to extend the use of the SSN to all Federal Government employees, and "An Executive Order [9397] by President Roosevelt ... required that, as a means of avoiding costly duplication, any Federal agency establishing a new system for personal identification must use the Social Security number. That order is still in effect" (Westin & Baker, 1972, p.41).

However, those decisions had very little impact until 1961, when the Internal Revenue Service (IRS) began to use the SSN for identifying taxpayers. In turn, IRS imposed on corporations which pay interest to individuals the responsibility to collect and report the SSNs of individuals they deal with.

The SSN is of low integrity. It is very easy to nominate a number which has surface validity, and relatively few organisations which use them have the ability to confirm or deny whether the number was issued by SSA to the person who is supplying them the number. The 9 digit (nnn-nn-nnnn) code permits 1,000 million combinations, or only about four times the country's living population. In addition, several blocks of codes, totalling close to 200 million, are not used. The proportion of possible codes which are currently assigned to a living person is therefore approaching 40%. As a result, a large proportion of wrong codes (whether they are wrong through accident or intent) are syntactically valid, in the sense that they are assigned to someone, or are within a range that is in use. A highly-used bogus number is 078-05-1120, which was printed on 'sample cards' inserted in thousands of wallets sold in the 1940s and 1950s.

Despite these serious weaknesses, many federal government agencies have used the number as the basis for identification of their own clients, and corporations make the provision of the number a condition of doing business, and use it for their own purposes, despite the absence of any authority for them to do so (Hibbert 1992). The Lotus Marketplace service, which was intended to sell vast quantities of data about consumers (but was withdrawn due to the furore its announcement stimulated), used the SSN as the primary identifying mechanism.

In Canada, a similar scheme to the U.S. SSN exists, called the Social Insurance Number (SIN). The Canadian Privacy Commissioner expressed serious concern about the threats to personal privacy involved in any expansion of the use of the SIN (1981), and subsequently the extent of its use was rolled back by an Act of Parliament.

The United Kingdom, Australia and New Zealand generally claim to share a strong tradition of personal freedoms, and do not have inhabitant registration systems. At least Britain and Australia had schemes during World War II, however. They were justified by the threat of invasion, and made possible by the resulting economic deprivation. They were abandoned when the threat was removed, because they were regarded as unsustainable and inappropriate:

> *"Britain had ... the identity card system used during the Second World War and up until 1951. Food was so scarce as to be unavailable without rations, and rations were available only to persons registered in their area of residence and provided with an identity card. Registration was all but universal, and the continual need for rations forced people to keep the authorities apprised of their current addresses, so that they could present a valid identity card. The cards were nationally indexed, so that the police could immediately find the address of any person throughout the country. As long as food remained virtually impossible to obtain without rations, the inducements to keep contact with the authorities remained highly persuasive ... the system in its old form would have quickly*

become unworkable without the inducement of rationing to keep addresses current" (Rule, 1973, pp.314-315).

* Current Developments

It is in the self-interest of executives of government agencies to establish tighter social control, and proposals for inhabitant registration schemes are being continually brought forward (Westin & Baker 1972, OTA 1981, Eaton 1986). During the last decade, the march of identification, data-processing and communication technologies have excited a particularly enthusiastic surge of attempts by governments to introduce general-purpose, national schemes (PI Bulletin 1993-). In Australia, for example, there was a concerted effort in the mid-1980s to establish a national identification scheme to attack tax evasion, welfare fraud and illegal immigration. It foundered on the rocks of public opinion (Clarke 1987). Subsequently, use of the Tax File Number has become a great deal more widespread. Despite nominal promises and legislative provisions, it is being developed as a proxy for the failed Australia Card proposal (Clarke 1991, 1992).

Other initiatives have included the United Kingdom (where the control of unruly soccer fans was the stated motivation), Singapore (to enable cross-enforcement of laws by various agencies), and Iran. There are two current political initiatives in the United States, one in relation to the proposed national health scheme, and the other to verify employment eligibility and facilitate cross-matching between agencies.

Even a national inhabitant registration scheme would not solve international problems. A general-purpose scheme would be at its most effective if it were world-wide, with all people registered at birth. The scope for people to undertake illegal activities would be constrained. In principle at least, it would be very difficult for anyone to have any other than their own official identity; it would be scarcely possible to live entirely out of contact with the national government of the country in which they were resident; and similarly difficult to move between countries without being intercepted by border officials.

Improving the integrity of these schemes, however, involves enormous difficulties, including establishing and maintaining standards across more than 200 nation-states (including, at any given time, a modest number of maverick governments and endemically corrupt administrations); the fundamental problems of ensuring a scheme of sufficient integrity in the first place; the prevention of forgery; and ongoing quality assurance. Periodic attempts are made to harmonise the identification procedures among associated countries (notably within the European Union, but also among other sets of close neighbours such as Australia and New Zealand). There is, however, little (publicly-perceived) momentum toward a world-wide identification scheme.

Public Policy Issues

* Inherent Objections to Identification

In considering the design of identification schemes, many interests need to be balanced. Powerful institutions and individuals seek to sustain their influence over individuals, variously as customers, suppliers, employees, students, patients, critics and opponents. There is also a collective interest in social control, primarily in order to sustain law and order and thereby protect life, health and property, but also to ensure that equity is achieved in terms of tax payment and receipt of government benefits (or, more realistically, that the inequities are planned, rather than accidental).

Against these motivations for tight social control, and an efficient identification scheme to support it, it is necessary to balance the interests of individuals in the various aspects of civil liberty. Private spaces in which people can behave free from intrusions are being rapidly invaded by data surveillance technologies. In this paper it is not appropriate to enter into a lengthy analysis of the impact of information technology on civil liberties, but see Rule (1973), Rule et al. (1980), Clarke (1988, 1994a), Davies (1992, 1994), Wigan (1994) and Agre & Harbs (1994).

The need to identify oneself may be intrinsically distateful to some people. For example, they may regard it as demeaning, or implicit recognition that the organisation with whom they are dealing exercises power over them. Many people accept that, at least in particular contexts, an organisation with which they are dealing needs to have their name. Some, however, feel it is an insult to human dignity to require them to use a number or code instead of a name. Some feel demeaned by demands, as part of the identification process, that they reveal information about themselves or their family, or embarrassed at having to memorise a password or PIN.

Some people are unwilling to submit to the regimen of carrying tokens, or unprepared to produce them, on the grounds that this reeks of a totalitarian regime, reflects and perpetuates a power relationship that they despise (such as the South African pass laws during the period of apartheid), or carries with it the seeds of discrimination (as reflected by the content of the token).

Another factor which forces compromise between the interests of accountability and law and order on the one hand, and civil liberties on the other, is the importance of multiple identities as a means of avoiding physical harm and death at the hands of violent opponents.

All forms of identification may attract opposition in different circumstances. The greatest degree of public distrust, however, is generally associated with biometric identifiers. Their use is in some cases invasive, and in all cases seems that way. In many

generally associated with biometric identifiers. Their use is in some cases invasive, and in all cases seems that way. In many countries whose law and traditions derive from the United Kingdom, fingerprints continue to be associated with the exercise of power by the State over people, especially in relation to criminal law enforcement. As a result, the compulsory provision of fingerprints is seen in such countries as an invasion of privacy, an indignity and an embarrassment (e.g. Vic CCPPI 1987). The situation is rather different in the U.S.A., where a wide range of organisations require the provision of fingerprints, and "near the end of 1968, the FBI's collection of civilian fingerprints exceeded 150 million sets" (Moenssens 1969, pp.143, 238). This author also claimed that the courts "have recognised that fingerprinting has come into general use as a means of identification, and that it can no longer be maintained that the taking of fingerprints of a person stigmatizes him as a criminal" (p.72). DNA-printing is especially intrusive, because it requires not just moral submission to authority, but also physical submission, in the form of body tissue or fluids.

Imposed physiographic identifiers, such as embedded chips, represent a yet greater exercise of power over the individual, to the extent that the person is treated in a manner similar to inanimate goods on a production-line. It is reasonable to anticipate that the public of some countries would at least resent, and may take political action to limit, the imposition of many forms of biometric identification.

As the sophistication of identification technologies increases, the identification schemes operated by individual corporations and government agencies require regulation, in order to achieve appropriate balance between personal, corporate and social needs. The need for equity makes this particularly important in the case of organisations which exercise effective monopoly, and where the multiple organisations which offer a particular product or service apply similar conditions, e.g. as a result of co-operation through an industry association.

The regulation of organisations' practices represents de facto approval of their aims, and of the social valuations implicit in their operations. There are many dealings among people, and between people and organisations, in which the parties' interests can be satisfied even though they are unaware of one another's identities. In these circumstances, any requirement that the parties identify themselves is extraneous to the business itself, and the regulatory regime should extend to requiring justification for the use of any identification scheme.

* Risks in Multi-Purpose Identification Schemes

People's dealings with individual corporations and government agencies involve significant issues, but the level of public concern becomes much more acute once identification schemes are used for multiple purposes. Accordingly, the question of what transactions can reasonably be conducted anonymously or pseudonymously requires even more careful consideration.

There is a common presumption that, when required to do so by an appropriate authority, people must identify themselves. In many jurisdictions, however, that presumption is largely unjustified. In many countries, a policeman only has the power to demand that a person identify themselves in particular contexts or locations. He may be empowered to demand the driver's licence of a person driving a vehicle, when dealing with a traffic offence. In some countries, this power may exist even in the absence of an offence. In many instances, however, the power does not extend to, for example, demanding the identification of passengers in the vehicle, or the identification of a driver who has passed a random breathalyser test.

There are countries, such as Belgium, in which a policeman has arbitrary power to stop any individual and demand their identity. Generally, however, (and leaving aside traffic matters), policemen, and even magistrates and judges, may not have the power to demand the identity of individuals, even if they are charged with criminal offences. In some States of Australia, for example, it is an offence not to provide one's identity (e.g. in Queensland and South Australia); whereas in others it is not (e.g. in Victoria). One may have to compromise other rights by exercising the right to remain unidentified (e.g. bail might be refused); but the right exists, and some people in some circumstances will wish to exercise it.

Public concerns about multi-purpose identification schemes have been well-documented in the United States. That country has considerable problems with illegal immigration and citizen dishonesty. There have been continual proposals by government agencies to upgrade the integrity of the SSN with the intention that it become an efficient multi-purpose identification scheme.

In 1969, the American National Standards Institute (ANSI) proposed a standard national identifier which incorporated the Social Security Number. Westin & Baker, after completing a major study of 'databanks' were of the opinion that "Given the cleavages in the nation today, the levels of distrust in government already present, and the fears that a national administration might take repressive actions in response to disorders or political crises, we should join nations such as Great Britain, Canada and France that are not moving to change historic policies against the establishment of a citizen numbering system at this time" (1972, p.41). The draft standard was withdrawn.

In 1973, an Advisory Committee to the U.S. Department of Health, Education and Welfare took the position that "a standard universal identifier (SUI) should not be established in the United States now or in the foreseeable future ... We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems. What is needed is a halt to the drift toward a [Standard Universal Identifier]" (HEW,

supported automated personal data systems. What is needed is a halt to the drift toward a [Standard Universal Identifier]" (HEW, 1973, pp.xxxii, 122).

The U.S. Privacy Act of 1974 (Public Law 93-579) recognised the concerns. It does not go so far as to require agencies using the SSN to change to some other identifier, nor does it prevent agencies from using the SSN for new purposes; however, it does make it unlawful for any Federal, State or local government agency to deny to any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. This can of course be overridden by statute, but it does ensure that an agency is in practice unable to use the SSN as the major identifying key for its clients (since some clients would decline to provide their numbers), until it has gone through the formality of gaining legislative approval for compulsory collection.

After (yet another) government agency assessment of the scope for the SSN to provide the basis for a national identification scheme, FACFI (1976) concluded that any attempt to improve on or replace the highly unreliable SSN scheme would not be worth the money. Subsequently, the Comptroller-General also recognised the unreliability of any documentary identification scheme, and especially the SSN, noting the estimate of about 4.2 million Americans with more than one Social Security Number (CG 1980). The title of this Government Report is itself quite informative: 'Re-issuing Tamper Resistant Cards Will Not Eliminate Misuse of Social Security Numbers'.

Reviewing developments during the 1970's, Rule concluded that " ... federal authorities have avoided any overt move in the direction of identification cards per se. There has recently been discussion of devising a tamperproof Social Security card, mainly to counteract the hiring of illegal aliens, but federal officials have apparently judged that a full-scale system of federally required, rigorous personal identification would be politically unacceptable. Their judgment is prudent" (Rule et al., 1980, p.161).

In the early 1980s, an Australian Royal Commission examined the manner in which international drug traffickers established and maintained sufficient identities that they could escape detection. Despite the security inadequacies which the looseness of birth certificate, citizenship certificate and passport issue entail, the Commission recognised that a free society like Australia's would not be prepared to accept tight controls, and decided not to recommend major changes, nor any form of national identification scheme (Stewart 1982).

Despite this catalogue of findings against the SSN in particular, and the idea of an inhabitant register and code in general, proposals keep coming forward from government agencies desperate for a 'magic bullet' to address their concern-of-the-moment. Meanwhile, arguments have been presented to Congressional Committees in favour of the prohibition of the use of the SSN for purposes other than its mainstream and controlled uses in social security administration (Rotenberg 1991). Similar arguments have been mounted in many other countries, including Australia (Clarke 1987) and Germany (Taeger 1984).

Most people are cowed by the power of large institutions, and resent at least some aspects of the surveillance society. The imposition of social control mechanisms, including the enforced use of intrusive identification, could stimulate an increased degree of conscious non-acceptance of authority. This could in turn bring on the collapse of that twentieth century phenomenon, the nation-state, and with it the disappearance of regional enforcement of law and order. The cyberpunk genre of science fiction (e.g. Gibson 1984, Sterling 1986) works on the assumption that the social surveillance and control movement contains the seeds of its own self-destruction. If this premonition has validity, it is vital that the public policy aspects of identification schemes be subjected to much more serious consideration than they have been in the past.

Conclusions

Identification is an important design consideration in information systems which deal with people. Management faces challenges in devising cost-effective schemes which fit their particular circumstances. The more effective biometrics-based identification schemes all involve serious social implications, and can be expected to excite considerable public suspicion and even hostility. It is remarkable how poorly understood the topic is. This paper has set out to fill a void in the literature. It points to a need for research into the origins for, and justification of, identification of individuals.

It was concluded that organisations should consider whether the nature of their relationships with individuals really requires identification, or whether appropriate design can enable transactions to be undertaken anonymously, or using pseudonyms. Organisations must appreciate that, in many cases, it is entirely feasible for them to protect their interests without knowing their clients' identities.

Inhabitant registration schemes, in countries with appropriate social control infrastructure, and designed appropriately, can be important elements in the exercise of control over the majority of the public, who are relatively straightforward in their life-styles, respectful of authority, honest, and politically weak. The inevitable deficiencies in any scheme leave ample scope for the seriously dishonest to manipulate it. Hence multi-purpose identification schemes assist in the enforcement of social control over the weak; but they do little to influence the powerful, clever and dishonest. Societies which seek to implement or sustain inhabitant registration schemes may do so at the risk of their social fabric.

Any high-integrity identifier represents a threat to civil liberties, because it represents the basis for a ubiquitous identification

Any high-integrity identifier represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behaviour would become transparent to the State, and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-utopian novellists. The highest-integrity schemes combine physically intrusive data-collection with a potentially ubiquitous instrument of power. As a result, the kinds of multi-purpose identification schemes, or inhabitant registration systems, which would appear capable of exciting the greatest degree of concern are those based on DNA-printing and implanted chips.

Government agencies, and some corporations, are seeking to exercise tighter control over individuals using various forms of data surveillance, underpinned by effective identification schemes. Parliaments throughout the world may passively process bills put before them to facilitate such schemes. Alternatively, they may choose to actively seek a balance between the organisational and collective interests on the one hand, and the individual interests on the other. If they adopt this course, then they must proscribe unjustifiably intrusive schemes, promote the use of anonymous and pseudonymous transactions wherever practicable, and, except in carefully justified and regulated cases, deny the multiple use of identification schemes.

References

Agre P.E. & Harbs C.A. (1994) 'Social Choice About Privacy: Intelligent Vehicle-Highway Systems in the United States' Information Technology & People 7,4 (December 1994)

Blume P. (1990) 'The Personal Identity Number in Danish Law' Comp. L. & Security Rep. 5,3 (1989-90) 10-13

CG (1980) 'Re-Issuing Tamper Resistant Cards Will Not Eliminate Misuse of Social Security Numbers' U.S. Comptroller-General, 1980

Chaum D. (1985) 'Security Without Identification: Card Computer to Make Big Brother Obsolete' Comun. ACM 28,10 (October 1985) 1030-44

Clarke R.A. (1987) 'Just Another Piece of Plastic for Your Wallet: The Australia Card' Prometheus 5,1 June 1987. Republished in Computers & Society 18,1 (January 1988), with an Addendum in Computers & Society 18,3 (July 1988)

Clarke R.A. (1988) 'Information Technology and Dataveillance' Commun. ACM 31,5 (May 1988). Re-published in C. Dunlop and R. Kling (Eds.) 'Controversies in Computing', Academic Press, 1991

Clarke R.A. (1991) 'The Tax File Number Scheme: A Case Study of Political Assurances and Function Creep' Policy 7,4 (Summer 1991)

Clarke R.A. (1992) 'The Resistible Rise of the Australian National Personal Data System' Software L. J. 5,1 (January 1992)

Clarke R.A. (1994a) 'Dataveillance by Governments: The Technique of Computer Matching' Information Technology & People 7,2 (June 1994)

Clarke R.A. (1994b) 'Information Technology: Weapon of Authoritarianism or Tool of Democracy?' Proc. World Congress, Int'l Fed. of Info. Processing, Hamburg, September 1994

Clarke R.A. (1994c) 'Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism' Forthcoming, Informatization and the Public Sector

Davies S. (1992) 'Big Brother: Australia's Growing Web of Surveillance' Simon and Shuster, Sydney, 1992

Davies S. (1994) 'Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine' Information Technology & People 7,4 (December 1994)

Eaton J.W. (1986) 'Card-Carrying Americans: Privacy, Security and the National ID Card Debate' Rowman & Littlefield, Totowa NJ, 1986

Ehrlich T. (1966) 'Passports' 19 Stanford L. Rev. 129-149 (1966-67)

FACFI (1976) 'The Criminal Use of False Identification: the Report of the Federal Advisory Committee on False Identification', U.S. Dept of Justice, 1976

Fox-Davies A.C. & Carlyon-Britton P.W.P. (1906) 'A Treatise on the Law Concerning Names and Changes of Name' Elliot Stock, London, 1906

Gibson W. (1984) 'Neuromancer' Grafton/Collins, London, 1984

Gramlich E.M. (1981) 'Benefit-Cost Analysis of Government Programs' Prentice-Hall 1981

Halsbury (1981) 'Halsbury's Laws of England' Butterworths, London, 4th Edition, Vol. 35, 1981, pp. 651-656

HEW (1973) 'Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems' (U.S. Dept. of Health, Education and Welfare) M.I.T. Press 1973

Hibbert C. (1992) 'What To Do When They Ask for Your Social Security Number' Comp. Professionals for Social Responsibility, version of June 1992, ftp from pit-manager.mit.edu in the file /pub/usenet/news.answers/ssn-privacy

HIC (1985a) 'An Outline Plan Prepared for the Inter-Departmental Committee on National Identification', Health Insurance Commission, May 1985

HIC (1985b) 'Establishment and Administration of a National Identification System: The Australia Card Program: Interim Planning Report', Health Insurance Commission, August 1985

IBM (1969) 'Identification Techniques' I.B.M. 1969 (GC20-1707-0)

IDC (1985) 'The National Identity System: Report of the Inter-Departmental Committee established to develop legislative requirements and other aspects necessary to complete the detailed implementation of the National Identity System (NIS)', Dept. of Health, August 1985 (published December 1985)

Josling J.F. (1980) 'Change of Name' Oyez Publishing, London, 1st Edition, 1946, 12th Edition, 1980

Moenssens A.A. (1969) 'Fingerprints and The Law' Chilton, Philadelphia, 1969

NZCS (1972) 'Investigation of a Unique Identification System' N.Z. Comp. Soc. May, 1972

OTA (1981) 'Computer-Based National Information Systems: Technology and Public Policy Issues' Office of Technology Assessment, Congress of the United States, Washington DC (September 1981)

OTA (1990) 'Genetic Witness: Forensic Uses of DNA Tests' Office of Technology Assessment, Congress of the United States, OTA-BA-438, Washington DC (July 1990)

Robinson M. (1986) 'The Registration and Certification of Births and Deaths in New South Wales' Discussion Paper for the N.S.W. Law Reform Commission (March 1986)

Rotenberg M. (1991) 'The Use of the Social Security Number as a National Identifier' Comp. & Society 21, 2-4 (October 1991) 13-19

Rule J.B. (1973) 'Private Lives and Public Surveillance' Allen Lane 1973

Rule J.B., McAdam D., Stearns L., Uglow D. (1980) 'The Politics of Privacy' Elsevier, New York, 1980

Rule J.B., McAdam D., Stearns L., Uglow D. (1983) 'Documentary Identification and Mass Surveillance in the U.S.' Social Problems 31:222-234 December, 1983

Sterling B. (Ed.) (1986) 'Mirrorshades: The Cyberpunk Anthology' Arbor House, New York, 1986

Stewart (1982) 'Royal Commission of Inquiry into Drug Trafficking, Interim Report No.2: Passports', Aust Govt Publ Serv, 1982

Sugden R. & Williams A. (1985) 'The Principles of Practical Cost-Benefit Analysis' Oxford U.P., 1985

Thompson M. (1980) 'Benefit-Cost Analysis for Program Evaluation' Sage, 1980

Thornberry C. (1974) 'Going Abroad: A Report on Passports' British Section of the International Commission of Jurists, Barry Rose Publishers, Chichester and London, 1974

Turack D.C. (1972) 'The Passport in International Law' D.C. Heath & Co., Lexington MA, 1972

Vic CCPPI (1987) 'Identification Tests and Procedures - Fingerprinting' Consultative Committee on Police Powers of Investigation, Melbourne, Australia (October 1987)

Walker G. de Q. (1986) 'Information as Power: Constitutional Implications of the Identity Numbering and ID Card Proposal', CIS Policy Report, 2,1, Centre for Independent Studies, St Leonards NSW, February 1986

Wambaugh J. (1989) 'The Blooding' William Morrow, New York NY, 1989

Westin A.F. and Baker M.A. (1972) 'Databanks in a Free Society' Quadrangle/N.Y. Times Book Co. 1972

Wigan M.R. (1994) 'The Influence of Public Acceptance on What Intelligent Vehicle Highway Systems Can Achieve' Information Technology & People 7,4 (December 1994)

Wilton G.W. (1938) 'Fingerprints: History, Law and Romance' William Hodge & Co., London, 1938

Navigation

Go to Roger's Home Page.

Go to the contents-page for this segment

Send an email to Roger

Created: 13 October 1995

Last Amended: 16 August 1997

These community service pages are a joint offering of the Australian National University (which provides the infrastructure), and Roger Clarke (who provides the content).

The Australian National University
Visiting Fellow, Faculty of
Engineering and Information Technology,
Information Sciences Building Room 211

Xamax Consultancy Pty Ltd ACN: 002 360 456
78 Sidaway St
Chapman ACT 2611 AUSTRALIA
Tel: +61 2 6288 1472, 6288 6916