BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Conceptualising Identity

Clare Sullivan
LLM (Adelaide), MBA (Adelaide)
Adjunct Lecturer, International Graduate School of Business, University of South Australia. PhD Candidate, Law School, University of Adelaide, South Australia
Email: clare.sullivan@adelaide.edu.au

This paper examines the legal nature of identity and identification in the context of transactions, considering recent developments in the United Kingdom and Australia. Identity and identification have not previously been analysed in this context, from a legal perspective.

The composition and legal function of identity are considered, having regard to legislative changes in both countries. In particular, the concept of identity under the United Kingdom Identity Cards Act 2005 c 15 (UK) is compared to the concept of identity developing under Australian legislation.

The distinction between that concept of identity and identification of an individual is considered and the legal nature and role of identity for transactional purposes is analysed. The legal meaning, legal function and practical implications of authentication of identity and verification of identity under the Identity Cards Act are compared to the requirements under Australian legislation. The distinctions between 'identifying information', 'personal information' and 'personal identification information' under United Kingdom and Australian legislation are also discussed.

Overall, the paper challenges the assumption that the United Kingdom and Australian legislation are merely establishing an evidentiary standard for identification of individuals for transactional purposes, and asserts that identity is emerging as distinct, new legal concept. A framework is presented for conceptualising identity in this context from a legal perspective, and the major ramifications of the new concept are outlined.

I. INTRODUCTION

Traditionally, parties to commercial transactions are generally assumed to be indifferent to identity. In the absence of transactions clearly founded on trust or imbued with confidential or personal obligations, the law focuses on arm's length dealings, often leaving the precise nature and role of identity in the shadows.[1] Focus on other elements of the transaction has resulted in identity being a rather nebulous concept.

Now identity is emerging from the shadows. Although arguably a concept of identity has been present in embryonic form in commercial practice for some years,[2] a legal concept of identity for

[1] As one commentator observes, 'much legal doctrine obscures the salience of identity qua identity, though when confronted directly with the issue, the law does give substance to the importance of identity.' See Richard R.W. Brookes 'Incorporating Race' (2006) 106 *Columbia Law Review*, 2023, 2097.
[2] A bundle of information which usually comprises name, account or card number with an expiry date and a handwritten signature has been used for credit and debit card transactions, and for electronic banking for many years.

transactions,[3] is now clearly emerging as a result of recent legislation introduced in the United Kingdom and in Australia.

The Identity Cards Act 2006 c 15 (UK) ('the Identity Cards Act,' 'the Act') and the Human Services Bill 2007 (Cth) ('Access Card legislation'/ 'the Bill') [4] establish national schemes of identity registration. Although the Act and the Bill appear to merely set criteria for identification of an individual for the purposes of the scheme, this legislation is potentially much more significant in the change it makes to the law and in its ramifications for commercial transactions involving individuals. Despite being designed for different specific purposes, analysis of the legislation and each registration scheme, reveal the emergence of the same new legal concept of identity.

My thesis is that this concept consists of two components, which I call 'database identity' and 'token identity,' respectively. Database identity is all the data and information recorded about an individual in the database/s accessible under a particular scheme. Token identity is a subset of the information which constitutes database identity. Token identity is a defined and limited set of information which determines an individual's identity for transactional purposes.

This paper examines the nature and role of token identity and database identity firstly in the United Kingdom, and then as emerging in Australia. The broader implications of the new concept of identity are discussed and considered.

II. IDENTITY IN THE UNITED KINGDOM

A. *Token Identity*

Section 1 of the Identity Cards Act covers the establishment and maintenance of the National Identity Register ('the NIR')[5] which is the basis of the National Identity Scheme ('NIS').[6] Section 1 (7) states that:

---

[3] In this paper 'transaction' and 'dealing' is used in their widest sense, to describe any dealing, whether in person (i.e. face to face) or using remote communication (such as a telephone, the internet or a computer network), for which an individual is required to identify himself/ herself. A transaction or dealing may be between an individual and a government department or agency or with a private sector entity, and can range from an enquiry to a contract. In this paper a transaction/dealing does not include transactions and dealings of a non- business nature such as domestic and social interaction.

[4] Although not framed in terms of identity, the Human Services (Enhanced Service Delivery) Bill (Cth) 2007 contains provisions which are very similar to those in the United Kingdom Identity Cards Act. The customer identification procedures under the new Federal Anti-Money Laundering/ Counter-Terrorism Financing Act 2006 (Cth) ('AML/CTF Act') enacted on 12 December 2006, also contain similar concepts of identity to those in the Identity Cards Act.

[5] Although a new single database was originally planned, the government has since announced that existing databases will be used for the NIS. Reportedly, the data and information will be held on three existing separate databases. See British Broadcasting Corporation 'Q &A: Identity Card Plans', *British Broadcasting News*, 19 December 2006<http://newsvote.bbc.co.uk/mpapps/ pagetools/print/news.bbc.co.uk/1/hi/uk_politics/31276. Reportedly, 'the Department of Work and Pensions database will contain biographical information', the Home Office database will contain biometric data, and 'the remaining information' will be stored on the Identity and Passport Service database. See Lucy Sherriff, 'UK Ditches Single ID Database' *The Register,* (London), 19 December 2006 <http//:/:www.theregister.co.uk/ 2006/ 12/19/bigbro_cubed/print/html> 29 March 2007.Recently, however, the Prime Minister has again raised the possibility of a single database and plans to make it easier to share information across government departments. See Nigel Morris, 'Big Brother: What it Really Means in Britain Today,' *The Independent* (London), 15 January 2007 <http//:/:www.news:theindependent.co.uk/uk/politics/article2154844.ece> 29 March 2007. For ease of reference, in this paper NIR is used to refer to all the databases comprising the NIS.

[6] The NIR is the basis of the Scheme, not the ID card as the title of the Act suggests. Note that the Act is enabling legislation which sets up the framework for the scheme. Much of the detail will be specified in regulations which are yet to be drafted. However, intended operation of the Scheme can be discerned from publications of the Identity and Passport Service.

In this section *references* to an individual's identity are references to-

(a) his full name;
(b) other names by which he is or has previously been known;
(c) his gender;
(d) his date and place of birth and, if he has died, the date of his death; *and*
(e) external characteristics of his that are capable of being used for identifying him.

(Emphasis added)

This provision really does much more than just set out the information[7] which constitutes 'references' to an individual's identity for the purposes of section 1. It defines the information which collectively establishes and verifies an individual's identity for the purposes of the scheme. Considering that the NIS is a national identity scheme, in effect the information recorded in the NIR establishes an individual's identity.[8]

Under section 1(7), an individual's identity is an indivisible set of information[9] comprising name/s, address, gender, date and place of birth and death, and external identifying characteristics[10]consisting of a handwritten signature[11] and 13 biometrics (a photographic face scan, two iris prints[12], and ten fingerprints).[13]

---

[7] 'Data' is often defined in legislation as including 'information' as in section 1 of the United Kingdom Data Protection Act 1988 c 29 (UK) ('Data Protection Act'), for example. However, the Identity Cards Act uses both terms. 'Information' is defined to include 'documents and records.' 'Document' is defined to include 'a stamp or label' [7] but 'record' is not defined and neither is 'data.' Although, 'information' is used in relation to the NIR, 'data' is used in referring to biometrics and the chip on the ID card. For example, 'biometric information' is defined to mean 'data about an individual's physical characteristics.' See section 42. For that reason I also make the general and scientific distinction between 'data' and 'information' i.e. that data is the raw material, from which information is derived. I use 'data' to cover both singular and plural. However, because the distinction is not always crucial, for ease of reference I use 'information' as including 'data,' unless otherwise indicated.

[8] As set out in section 1 (3), the purpose of the NIR is to set up a 'secure and reliable record of registrable facts about individuals in the United Kingdom.' The information in the NIR is to be used for a wide range of purposes including provision of public services, crime prevention and detection and national security. See section 1(4). The government wants to make the NIS the 'gold standard of identity verification'. See report by the United Kingdom Information Commissioner, *The Identity Cards Bill – The Information Commissioner's Concerns* (June 2005), 1 <http://www.ico.gov.uk/eventual.html> 10 May 2006.

[9] Practical considerations support this interpretation. Use of one, two or even several of these components would not usually identify an individual with sufficient precision and would at best, make the section ineffective, and at worst, a nonsense. For example, there are undoubtedly a large number of individuals named or known as Lee Smith in the United Kingdom. More than one may have the same birth date. Lee is not a gender specific name, so adding gender narrows the field, as does birth place. Of course, the addition of biometrics and a handwritten signature not only further narrows the field, they provide a link to the physical embodiment of the individual, assuming of course, that the biometrics and signature are authentic and are correctly matched to the individual. It is not until all this information is considered as a whole, that it can be said to identify an individual with any acceptable degree of precision.

[10] The 'external identifying characteristics' referred to in this section are specified in Schedule 1 which sets out the categories of data and information that may be included in the NIR under section 3.

[11] Signature' is not defined but it is apparently intended that a handwritten signature be used. An individual's signature is included in the list of 'identifying information' implying that a handwritten signature is considered a distinguishing physical feature, though it is not mentioned at all in the definition of 'registrable facts,' nor in relation to 'identity' in s 1. See also Tom Geoghegan, 'I've got a Biometric ID Card', *British Broadcasting News*, 12 August 2004<http://news.bbc.co.uk/go/pr/fr/1/hi/uk/3556720.stm>29 March 2007. Georghean reports that when he obtained his ID card as part of the pilot scheme being conducted by the IPS, he 'had to give a copy of my signature which they store electronically.'

[12] It now appears that only fingerprints and a face scan will be used initially, though iris scanning may be used in the future. Iris scans will not be used initially, reportedly because of the high costs of the process and because most countries use fingerprints and face scans. Philip Johnstone, 'Iris Scans Dropped from ID Card Plans', *Telegraph*, 12 January 2007 <http://telegraph.co.uk/ core/Content /displayPrintable.jhtml;jsessionid=DWNA31GV>29 March 2007.

The Act clearly distinguishes this information from the other information in the NIR. This approach prompts the question as to why identity as defined in section 1 (7), is so distinguished especially when the other information in the NIR, which includes residential address, residential status and identification numbers,[14] could be used to identify an individual. The answer lies in the way an individual is identified under the NIS and the role the section 1 (7) information plays in not only identifying an individual but in authorizing the system to interact and transact with that identity.

When the legislation is considered with government documentation about the NIS, [15] it is clear that identification under the scheme consists of two stages. The first stage is the initial authentication of identity as part of registration. The second stage is verification of identity which occurs at the time of a transaction.[16] The integrity of the NIS and its ability to correctly identify an individual depend on the integrity and rigor of these two processes.

Identity is authenticated under the scheme, when an individual is registered under the NIS. An individual will usually be required to attend in person,[17] to be interviewed to obtain 'biographical' information, a signature and the biometrics.[18] On its website the Identity and Passport Service ('IPS') explains the registration process:

> When you apply for an ID card, we will check your 'biographical footprint'[19] against information held in other databases such as National Insurance or driving license records. We will not rely entirely on written documents for this information (as they could be forged).You will be asked to visit one of our local or mobile centres in person wherever possible. This will make it harder for someone to pretend to be another person when applying for an ID card. That information is subsequently used to verify an individual's identity at the time of a transaction.

---

[13] Identity and Passport Service, *Corporate and Business Plans 2006-2016,* 42 <http//:www.identitycards .gov.uk/scheme.html> 10 May 2006.

[14] Section 1 (5) states that ' [I]n this Act "registrable fact," in relation to an individual means:

(a) *his identity*;
(b) the address of his principal place of residence in the United Kingdom;
(c) the address of every other place in the United Kingdom or elsewhere where he has a place of residence;
(d) where in the United Kingdom and elsewhere he has previously been resident;
(e) the times at which he was resident at different places in the United Kingdom or elsewhere;
(f) his current residential status;[14]
(g) residential statuses previously held by him;
(h) information about numbers allocated to him for identification purposes and about the documents to which they relate;
(i) information about occasions on which information recorded about him in the Register has been provided to any person;
(j) information recorded in the Register at his request.' (emphasis added)

[15] The precise nature of the identification process is not clear from the Act because the Act establishes the framework for the NIS. Much of the detail regarding the operation of the NIS will be in subsequent legislation.

[16] 'Authentication of identity ' and 'verification of identity ' are used interchangeably (and therefore incorrectly) by many commentators. Under the NIS they are separate and distinct processes.

[17] Exceptions are clearly comtemplated in the case of incapacity and infirmity. See Home Office, *Regulatory Impact Assessment, Identity Cards Bill Introduced to House of Commons on 25 May 2005* (UK) <http//:www.homeoffice.gsi.gov.uk.html.> 16 May 2006. This regulatory assessment is an updated version of the one published alongside the Bill which was introduced into the House of Commons on 29 November 2004.

[18]Identity and Passport Service, *What is the National Identity Scheme?* <http//:www. identitycards.gov.uk/scheme.html> 10 May 2006.

[19] 'Your biographical footprint is simply the basic facts about your life, for example: name, date of birth and address.' Identity and Passport Service, *What is the National Identity Scheme?* <http//:www. identitycards.gov.uk/scheme.html> 10 May 2006.

> [O]nce we have checked your identity, we will record your biometric data. Recording facial and iris biometrics is just like having a high quality digital photo taken. Recording fingerprints is very simple too and no ink is involved. You just press your fingers against a reader.

The IPS then states that '[T]hese biometrics will be sealed to or permanently paired with your biographical information to create completely unique and secure identity data.'[20]

The foundation of the accuracy and reliability of NIS in authenticating identity and subsequently in verifying identity, is the use of 'identifying information,' i.e. external identifying characteristics, [21] particularly biometrics. The IPS states that:

> Because your biometrics are unique to you, they are the strongest way to 'seal' your identity details as held in the National Identity Register (NIR) to you. The most secure identity check would involve confirming, not just that you have a valid identity card , but that the card and the record that match it belong to you. This is a far more secure way of identifying yourself than using a personal identification number PIN or password which could be stolen or copied.
>
> The use of biometric data offers you the greatest protection from identity fraud. A criminal may steal your card, but your unique biometric data cannot be taken from you.[22]

After an individual is registered under the NIS, his/her identity is verified by matching information provided at the time of the transaction, with information recorded in the chip on the ID card[23] and in the NIR.[24] Identity is verified if the required information as presented, matches that information as recorded in the chip or NIR.

Verification of identity involves two steps. First, the section 1 (7) information is presented to establish identity. [25] This process can be thought of as a key being used to open a door. [26]The section 1 (7) information is the key. When this information is presented, it is like inserting the key into a lock. In the second step, the presented information is compared with that on record, in the chip on the ID card and/or in the NIR, to see if it matches. To use the key analogy, if the indentions on the key line align with the indentations in the lock, the key can open the door.

---

[20] Identity and Passport Service, *What is the National Identity Scheme?* <http//:www. identitycards. gov.uk/scheme.html> 10 May 2006.

[21] Identifying information' is confined to an individual's external characteristics that under section 1 (7) 'are capable of identifying him' and is therefore narrower than token identity. In Schedule 'identifying information includes a photograph of head and shoulders, fingerprints and 'other biometric information' as well as the individual's signature. 'Identifying information' is more limited than 'identity' under s 1(7).

[22] Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/scheme.html> 10 May 2006.

[23] Usually used for off-line verification. The ID card will be a smart card which is 'essentially a stand alone computer,' which can operate independently of the on-line system. See John Wadham, Coailfhionn Gallagher and Nicole Chrolavicious, *The Identity Cards Act 2006* (2006), 5. Subsections (1) and (2) of section 6 explain that the ID card will contain two sets of information: registrable facts as recorded on the NIR and data enabling the card to access the individual's record on the NIR. As an example of the latter, the Explanatory Notes specifically mention a personal identification number ('PIN').

[24] Including updating, to reflect any subsequent changes and to correct any errors. The information recorded in the chip is also recorded in the NIR.

[25] Presentation may be by personal attendance at which time the information is provided by a person and/or the ID card is presented or the required information may be provided by telephone or using the internet. Under s 6(3) the ID card 'must record only the prescribed information' and 'must record prescribed parts of it in an encrypted form'.

[26] My analogy.

Not all the section 1 (7) information is necessarily used to verify identity, for all transactions.[27] To use the key analogy, for some transactions it is not necessary to ensure that all the indentations align, as long as the required number match. Depending on the nature of the transaction, section 1(7) information may be also supplemented by additional information such as a Personal Identification Number ('PIN') or answers to designated questions about other information recorded in the chip and/or in the NIR.[28] This additional information can be thought of as establishing who is holding the key to the door, to ensure that it is in the correct hands. These aspects of course, do not alter the basic function of the section 1 (7) information, which is to establish and verify identity for transactional purposes.

The section 1 (7) information is fundamentally different from the other information recorded on the chip or in the NIR. The information defined as 'identity', is information about the essence an individual, as a human being. It is established at birth and usually remains unchanged until death.[29] Although subsequent change is possible and was acknowledged in Parliamentary debate,[30]name, gender, date and place of birth are considered factual in that they are established when entered in the Register of Births, Deaths and Marriages. Similarly, date of death is fixed. Even if an entry is incorrect, it becomes fact once it is recorded in that Register.[31]This factual information is linked to the physical embodiment of the individual by biometrics and a handwritten signature. When the biometrics and signature are combined with name, gender, date and place of birth and death, collectively this information is considered so unique, as to positively identify one individual out of a large population.

Section 1(7) information is core identity information which stands in place of the physical person. That set of information represents an individual.[32] It collectively constitutes an individual's identity credentials – his/her token identity.

Token identity does more than just identify. It is the key that opens the lock, so the system can interact and transact with the individual presenting that token identity. Token identity is used to single out an individual from the rest of the population and to *authorise* the system to deal with that identity. [33]

B. *Database identity*

Section 1 (7) information can be thought of as 'first screen' information. It is the first set of information which appears when the NIS identifies an individual, though of course, much more

[27] Public and private sector organisations accredited to use the NIS will be able to choose the verification method considered most suitable for the transaction. There are basically three levels of verification contemplated by the NIS. The lowest level will be a check using the photo on the ID card. The next level will involve the use of a PIN and/or answers to designated questions. The highest level check will include biometrics. See Identity and Passport Service, *What Kind of Organizations will use the Scheme?* <http://www.identity cards.gov.uk/scheme.html> 10 May 2006.

[28] Including, for example, a question about residential address. Residential address is not part of the section 1 (7) information.

[29] Name is the most likely piece of information to change but parts (a) and (b) of section 1 (7) link the name given to a baby to other names, whether as a result of a name change by marriage, deed poll, or through usage.

[30] Particularly in relation to gender. See United Kingdom, *Parliamentary Debates*, House of Lords, 30 January 2006, col 79 (Baroness Scotland of Asthal).

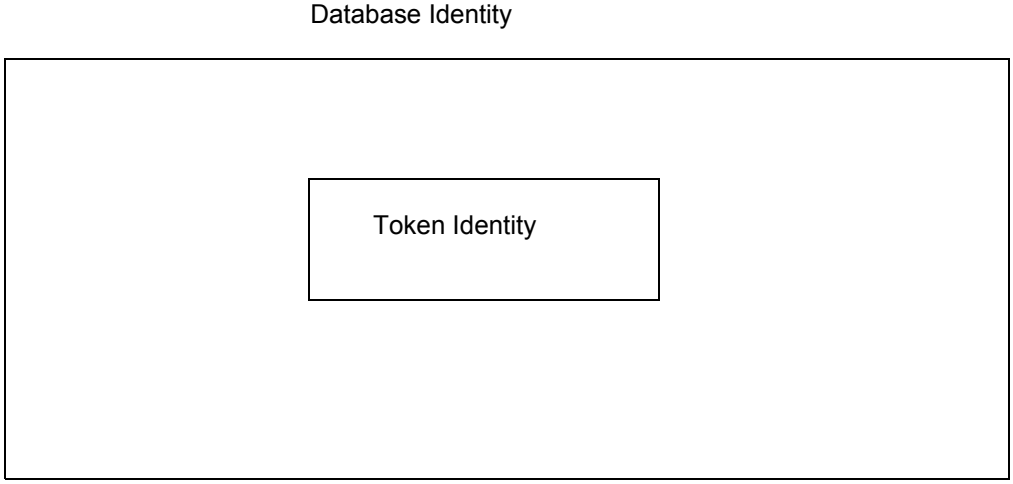
[31] Perhaps the most famous example is the celebrity Oprah Winfrey who was actually named Opah. Opah was incorrectly stated on the birth certificate as 'Oprah'. The birth certificate is a primary identity document in most common law countries and it is the most enduring identity document.

[32] Much like a token represents money.

[33] It enables the automated system and the human operators using that system, to transact with the individual who presents that token identity.

information about the individual is recorded in the NIR. Section 1 (7) information is just a token of all the information on record in the NIR[34] and in other databases accessible under the NIS.

The full set of information recorded in one or more databases[35] accessible under the NIS can be conceptualized as the individual's 'database identity.' Token identity is a subset of the full range of information recorded about an individual in the NIR and in other databases forming the NIS. The relationship between token identity and database identity can be depicted diagrammatically:



Whereas the function of token identity is to establish and verify identity for transactional purposes, database identity has a broader role. As mentioned above, parts of the information which constitutes database identity (and not token identity) such as a PIN or residential address, may be used to verify an individual's identity at the time of a transaction. Collectively, the recorded information can also be used to distinguish an individual from others. In that sense, all the information recorded about an individual in the NIR and in accessible databases, can be described as identifying an individual.
Whilst the conventional approach is to consider this information as 'personal data'[36] which is subject to the Data Protection Act 1988 c 29 (UK) ('the Data Protection Act'), conceptualizing it in terms of identity more accurately describes its actual role and effect for transactional purposes for

[34] With the possible exception of 'Records of Provision of Information', the other information in the NIR, even information like a PIN number and password, can be broadly described is biographic in that it is information about the individual.
[35] Although a new single database was originally planned, the government has now announced that existing databases will be used for the NIS, though the data and information they currently contain will be augmented.
[36] 'Data' is defined to include 'information' under section 1 (1) of the Data Protection Act. 'Personal data' is defined in section 1(1) to mean 'data which relate to a living individual who can be identified-

(a) from those data,or
(b) from those data and other information which is in the possession of , or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'. Under section 1(1)'data controller means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Some of the personal information may also be 'sensitive personal data' which is subject to special protection under the Data Protection Act. 'Sensitive personal data' is defined in the Act as information relating to racial or ethic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offence by the individual and/or proceedings for an offence committed or alleged to have been committed by the individual. See section 1(1).

both living and deceased individuals.[37] Identity is also a more enduring concept in that it clearly extends to deceased individuals, whereas the Data Protection Act only regulates the collection, storage and use of data and information relating to a person who is alive.[38]

However, like token identity, database identity does more than just identify, it tells a story. It is, in essence, a narrative about that identity. Whereas token identity singles out an individual so as to authorize dealings with that identity, database identity chronicles activities relating to that identity. In so doing, database identity tells a story about the individual linked to that identity.[39] Even information which at first sight seems largely administrative in nature,[40] such as Security Information and Records of Provision of Information, adds to the profile and the impression it conveys about the individual.[41] It is tempting to think of this information as influencing an individual's reputation and in a way it does, but it is not reputation in the traditional sense. The information on record can affect the way in which an individual is regarded by other people but even more significantly, it can affect how an individual is regarded by the automated system.
Database identity is necessarily a much broader concept than token identity but it is limited by the purposes and the architecture of the particular scheme. In this respect database identity is fundamentally different to Solove's concepts of 'digital dossiers' and hence, the 'digital person'[42] who Solove says is 'composed in the collective computer networks of the world.'[43]Solove's views are based on privacy, not on a legal concept of identity and he uses 'digital dossiers' to cover all digital data and information relating to an individual, wherever it is recorded.

In contrast, database identity comprises data and information accessible under a particular system or scheme. In the United Kingdom, an individual's database identity comprises all the data and information recorded about that individual in the NIR and in extant databases accessible under the Identity Cards Act and related legislation.[44] More importantly, however, database identity does not 'compose' an individual in the sense used by Solove. Database identity certainly profiles an individual but it is *connected* to an individual by his/her token identity and that connection can remain even after death. This is a crucial distinction and an important point to which we will return, as we examine developments in Australia and finally the ramifications of the new concept.

III. IDENTITY IN AUSTRALIA

[37] Date of death is included in the information in section 1 (7) of the Identity Cards Act.
[38] See the definition of 'personal data' in section 1(1) of the Data Protection Act.
[39] This other information includes historical information but database identity is also dynamic and will change as the NIR and other accessible databases are updated to reflect changes, transactions and access information.
[40] See Schedule 1. With the possible exception of 'Records of Provision of Information' in Schedule 1, the other information in the NIR, even information like a PIN number and password, can be broadly described is biographical in that it is information about the individual.
[41] Data and information entered in the NIR may not be adequately tested for authenticity, nor will it necessarily be completely up to date and accurate. The Act provides that once entered in the NIR, information 'may continue to be recorded in the Register 'only if and for so long as it is consistent with the statutory purposes for it to be so recorded'.[41] However, any errors and inaccuracies, including those resulting from 'gaps' in the personal information recorded and abbreviated data entries, can become 'facts.'
[42] Daniel Solove, *The Digital Person* (2004), 1.
[43] Daniel Solove, *The Digital Person* (2004), 1. Solove refers to an 'electronic collage that covers much of a person's life- a life captured in records, a digital person composed in the collective computer networks of the world.'
[44] The Act is enabling legislation. Enactment of further legislation is necessary to fully implement the scheme.

Token identity[45] has been evident in State legislation for some years[46] but recently the concepts of token identity and database identity have clearly emerged and crystalised in Federal legislation.[47] They first appeared in the Anti-Money Laundering/ Counter-Terrorism Financing Act 2006 (Cth) (the AML/CTF Act') enacted in December 2006 and the Draft Rules which are currently part of the public consultation process (collectively, 'the AML/CTF legislation'). The AML/.CTF legislation requires financial institutions and other prescribed businesses[48] to identify new and existing customers.[49]

---

[45] In Australia, 'identity' is mentioned in a wide range of Federal and State legislation. However, identity is rarely defined. When identity is defined, the definition is usually coloured by the nature of the legislation For example , see for example, section 4 of the Equal Opportunity Act 1995 (Vic) which defines 'gender identity.'

[46] See the Enforcement and National Security (Assumed Identities) Act 1998 (NSW) ('the NSW Assumed Identities Act').The Act provides 'for the acquisition and use of assumed identities by officers of certain law enforcement and national security agencies for the purposes of their official duties,' as stated in the long title of the Act. Identity may be assumed temporarily or permanently. Identity is defined to mean 'name, address or date of birth, or such other aspects of a person's identity as may be prescribed by the regulations for the purposes of this definition. See section 3. The regulations have not prescribed other aspects. At first sight this combination of information may seem unremarkable Name and address may be dismissed is an expected, frequently used combination. However, date of birth is not commonly used, other than in establishing identity. Other State legislation also defines identity as name, address and date of birth. See for example section 7.1.2 of the Gambling Regulation Act 2003 (Vic) which defines 'identity' in relation to a person to mean 'name, address, date of birth or a prescribed aspect of the person's identity.'

[47] Token identity was initially evident to an extent in Federal legislation, in the Migration Act 1958 (Cth). The Act does not define 'Identity', 'authenticate', 'identify' and 'identification' but 'identification test' means 'a test carried out in order to obtain a personal identifier'. A person who is suspected of being a 'non- citizen' may be required to provide a 'personal identifier'. Section 5 defines 'non-citizen' to mean ' a person who is not an Australian citizen.' Under section s188 (4A) '[A]n officer must not require, for the purposes of subsection (4), a person to provide a personal identifier other than any of the following (including any of the following in digital form):

(a) a photograph or other image of the person's face and shoulders;
(b) the person's signature;
(c) any other personal identifier contained in the person's passport or other travel document;
(d) any other personal identifier of a type prescribed for the purposes of this paragraph.Check

Note: Division 13AB sets out further restrictions on the personal identifiers that minors and incapable persons can be required to provide.

(5) Subsection (4) does not limit the officer's power under subsection (1) to require the person to show the officer evidence (other than a personal identifier) of the person's identity or evidence of the person being a lawful non-citizen.'

Section 5A defines 'personal identifier' to mean 'any of the following (including any of the following in digital form):

(a) fingerprints or handprints of a person (including those taken using paper and ink or digital live scanning technologies);
(b) a measurement of a person's height and weight;
(c) a photograph or other image of a person's face and shoulders;
(d) an audio or a video recording of a person (other than a video recording under section 261AJ);
(e) an iris scan
(f) a person's signature;
any other identifier prescribed the regulations, other than an identifier the obtaining of which would involve the carrying out of an intimate forensic procedure within the meaning of section 23WA of the Crimes Act 1914.'

However token identity as a subset of database identity, first became evident in the AML/CTF legislation. The AML/CTF legislation is part of an international initiative. Similar AML/CTF legislation was introduced into the United Kingdom prior to Australia so it can be argued that the approach and the emerging concept of identity have been imported into Australia United Kingdom. However, the origin of the concept does not in any way limit its significance.

[48] Section 5 defines 'reporting entity' as 'a person who provides a designated service'. 'Designated service is as set out in section 6. Section 6 sets out 70 different banking and finance services, bullion dealings and gambling services which are defined as 'designated services' under the AML/CTF Act.

[49] The approach adopted by the AML/CTF legislation in identifying customers is similar to the approach of the Identity Cards Act. Despite being designed for different specific purposes, the AML/CTF legislation, like

Now, however, token identity and database identity are even more clearly revealed in the Access Card legislation recently introduced into Federal Parliament.[50] The legislation establishes the framework for the new Health and Social Services Access Card, [51] (the Access Card'), a smart card[52] which will replace a range of cards currently used for government services and benefits. The stated purpose of the new registration scheme[53] and the card is to 'streamline and modernize Australia's delivery of health and social service benefits.'[54]

The Bill establishes a national system of identity registration and proof of identity in Australia, in that the access card will become the primary means of identifying Australian citizens and residents for health and social security purposes.[55] Considering that the new access card will replace the current Medicare card[56] held by most Australian residents, the reach of the new scheme is considerable. Like the United Kingdom identity card, the Access Card may be used by an individual at his/her discretion, to prove his/her identity.[57]

A. *Token Identity*

---

the Identity Cards Act, establishes two tiers of identity. The first tier is the 'minimum Know Your Customer information' ('KYC information'). At the time of writing only Draft AML/CTF Rules have been released for public consultation, but draft rule 2.2.2 states that '[A]s part of its customer identification program, a reporting entity must collect, at a minimum, the following KYC information from a customer at the relevant time

(a) the customer's full name;
(b) the customer's date of birth; and
(c) the customer's residential address.'

Although the minimum KYC information is more limited than the set of information which constitutes token identity under the NIS, the basic concept of token identity is evident, and it is based on the individual's name/s and date of birth. The concept of database identity is also evident in the 'further KYC information.' Further KYC information includes citizenship and residency information as well as financial details which must be collected if the money laundering or terrorism financing risk is assessed as high. See Draft rule 1.3.1.

[50] On 15 March 2007 the Bill was delayed following a Senate Inquiry. Like the Identity Cards Act in the United Kingdom, the Bill establishes the framework for the new scheme. Operational details including security and privacy aspects were to be covered in subsequent legislation. The Senate Inquiry recommended that the entire legislative package be presented in one Bill. The government has agreed and the new Bill is expected to be introduced into Parliament in June 2007. The government has announced that it still wants to begin the scheme in April 2008, as originally planned. Although the clauses in current Bill will be augmented, it is unlikely that the clauses presently in the Bill will be substantially changed.. See Australian Broadcasting Corporation, '*Govt Stands by Smart Card Despite Senate Concerns*' <http//:www. abc.net.au/newsitems/200703s1873093.html> 16 March 2007.

[51] Commonly referred to in Australia as 'the smart card'.

[52] The card contains a chip which is a microprocessor capable of storing information and performing intelligent functions off- line.

[53] Like the NIS, the basis of the new scheme is the Register, not the card.

[54] *Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum*, 2. A new chip and Personal Identification Number ('PIN') card will replace the existing Medicare Card which does not have a PIN or an embedded chip, and which specifies only the individual's name, Medicare number and card expiry date. The new card will replace 'up to 17 existing Australian Government benefits cards and vouchers.' See Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 1.

[55] The government has stated that '[I]t is the intent of the Australian Government that access card registrations meet the Gold Standard Enrolment Framework of the National Identity Strategy to the greatest possible extent. This will ensure that the risks of identity fraud are managed and appropriate protections to Australian Government outlays are provided.' See Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 24.

[56] And a key proof of identity document.

[57] As is the case under the Identity Cards Act, the Bill only prohibits a person from *requiring* production of the card. See clauses 45 and 46 of the Bill and section 16 of the Identity Cards Act.

Although the government maintains that the Access Card is not an identity card, the Bill is clearly identity legislation.[58] It is clear from the context of the Bill and the Explanatory Memorandum that one of the (unstated) purposes of the legislation is to identify individuals claiming Federal benefits. Although the stated purposes are to 'reduce fraud'[59] and improve efficiency in delivery of health and social services benefits,[60] 'strengthened proof of identity will be a fundamental element in the registration process for an access card.'[61]

The Bill is remarkably similar to the United Kingdom Identity Cards Act though the former is not generally couched in terms of 'identity'[62] and 'identification,' [63] and of course, 'identity' is not defined. Although the Bill closely follows the approach of the Identity Cards Act, in comparison the Bill is clearer and contains more detail about the information recorded in the Register and on the access card and how the scheme will work. As a result, not only is the new concept of identity clearly evident, the nature and functions of token identity and database identity can be more easily discerned.

The information required to identify an individual will usually be provided by presenting the Access Card. [64] Information will be stated on the card surface and stored in a chip on the card.[65] The information which must be included on the card surface can be divided into two categories: personal identity information, and information of an administrative nature. The administrative information comprises card number, expiry date and on the individual's request, specified pension information.[66] The personal identity data and information is the individual's name, date of birth[67], photograph and a digitized copy of the individual's handwritten signature.[68]

In operation, the Australian scheme is remarkably similar to the NIS. At the time of a transaction the individual must establish his/her identity by providing a set of information which comprises name and date of birth, photograph and handwritten signature. This set of information is an individual's token identity under the Australian scheme and it is obtained from the individual in a registration process which is almost identical to that required for the NIS.[69]

---

[58] Attempts to present it otherwise can be explained by political expediency. A national identity card is still a political hot potato in Australia. The Federal government is obviously trying to avoid controversy and the debate that has followed each attempt to introduce a national identity card in Australia. The Australia Card legislation introduced into Federal Parliament in the 1980s proved to extremely controversial and did not proceed in face of the public outcry. In 2006 the Prime Minister floated the idea of a national identity card, again sparking public debate which subsided when it became apparent that the legislation was not imminent. Indeed, the introduction of the Human Services Bill has been a surprise to many observers who assumed that the Access Card legislation would not be introduced into Parliament until after the next Federal election in 2007.

[59] 'Fraud' not 'identity fraud' is used. See clause 6.

[60] *Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum,* 2.

[61] *Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum*, 3.

[62] See however, clause 17 which refers to 'a password for authenticating identity'.

[63] See however, clause 17 and clause 34. Clause 17 also refers to 'documents used to prove identity.'

[64] Like the United Kingdom scheme, the basis of the Australian scheme is registration , not the Access Card. Strictly speaking, the Access Card is not compulsory.

[65] 'Chip' means 'a microchip or any other device that stores or processes information.' See clause 29 and clause 5.

[66] The individual must request this information be stated on the surface of the card. The categories of disability and entitlements are specified in clause 30.

[67] According to the Explanatory Memorandum stating date of birth on the surface of the card will be at the individual's discretion. See *Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum,* 34 and clause 30.

[68] *Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum*, 34.

[69] The major differences are that a facial scan is the only biometric and in addition to proving identity using documents like a passport, driver's license and Medicare card; there is mention that 'evidence of use of the identity in the community' will need to be shown. How this will shown (and checked) is unclear but on present indications, it is unlikely to be a major hurdle. See Australian Government '*Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007',* 61.

The information which constitutes token identity for the Australian scheme differs from token identity under the NIS in that it does not include gender, place of birth, date of death and the other biometrics.[70] However, although less detailed than the information which is defined as 'identity' under the Identity Cards Act, it consists of the same core identity information i.e. name and date of birth,[71] which are linked to the physical embodiment of the individual, by a handwritten signature and a photograph.[72]

More importantly, this set of information has the same function as 'identity' as defined in section 1 (7) of the Identity Cards Act. Collectively, it is initially presented to establish an identity and then verifies that identity, thereby authorizing the system to transact with that identity.[73] As in the NIS, identity is verified when the information constituting token identity, as presented,[74] matches the information recorded in the chip[75] and/or in the Register. [76] The information in the chip is used to verify identity off- line.[77]Information in the Register is used to verify identity for on-line transactions. Like the concept of token identity under the Identity Cards Act, some or all of the information recorded on the chip may be used to verify identity.[78] Also as in the NIS, a PIN or additional information such as answers to designated questions,[79] may be required as an

[70] Iris scans and fingerprints are included in the NIS. Under the Australian scheme, sex is recorded in the chip and in the Register and date of death is recorded in the Register

[71] Under the Access Card legislation date of birth is included on the surface of the card and in the chip on the card, if requested by the individual. However, it must be included in the Register, unless it is excluded under clause 18. Clause 18 empowers the Secretary of the Department to exclude particular information when a individual is under the National Witness Protection Program or if including it would be inconsistent with Commonwealth law. Under section 1 (7) of the Identity Cards Act, the other personal information included in 'identity' is place of birth and gender as well as date of death.

[72] Although a face scan will be done at the time of registration, unlike the NIS, the photo on the surface of the Access Card will not contain biometrics. Biometrics will only be recorded in the Register. The photo appearing on the card and ' a numerical template of [the individual] derived from that photograph' will be recorded in the Register. See clause 17. The reason given for this approach is a pragmatic one. The card readers presently used by service providers (particularly medical, dental and other health services practitioners and pharmacists) for point of sale for credit and debit card transactions, will be used for the Access Card. Use of biometrics for routine identity verification for transactional purposes will require upgrading of the card readers presently used, which would add to the costs of establishing and operating the scheme. See Australian Government ,*Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007,* 33 and 36.

[73] Recall that under the Identity Cards Act, a face scan and signature of an individual are 'external characteristics of his that are capable of being used for identifying him'. See section 1 (7). The NIS also includes other biometrics - fingerprints and iris prints.

[74] The information can be provided by presenting the Access Card or by providing the required information in person , by telephone , by internet or by providing a paper document.

[75] The chip has two areas, the Commonwealth area and the Individual's area. The latter can contain next of kin details, organ donor status and medical alerts. The Commonwealth's area contains all the information specified on the surface of the card which includes the information that constitutes token identity, as well as additional information including address, sex, PIN or password, information about benefit cards, Medicare number, whether proof of identity is 'full' or 'interim' and an emergency payment number. See clause 34.

[76] The Register contains all the information on the surface of and in the chip on the Access Card as well as additional information. See clause 17.Like the Identity Cards Act, the basis of the Australian scheme is registration,, not the Access Card. The Bill does not require an individual to apply for an Access Card after registration and there is no requirement to carry the card once it is issued. See Division 2 and clause 42 of the Bill. Card not present verification is clearly contemplated. See also *Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum,* 26 and 42

[77] The card contains a microprocessor and memory so information can be stored and processed using only the card, independently of an on- line system. The chip is like a mini computer minus keyboard and screen. The card is placed in a card reader like those in use at point of sale for credit and debit card transactions in many retail stores and businesses.

[78] The chip has two areas- a government area and an area in which an individual can include information such as next of kin details, organ donor status and medical alerts. Information in the government area of the chip is used to verify identity.

[79] A question may be asked about other information such as the individual's address, for example.

additional step for some transactions. Under both the Australian and the United Kingdom schemes that additional information is used to determine that token identity is in the right hands.

The Australian scheme highlights a further refinement to the concept of token identity which is also a feature of the NIS - the use of the card number as an identifier. The Access Card number will be used in telephone and internet dealings to enable an individual to quickly establish his/her identity.[80] Using a number increases efficiency by reducing the time that is spent on a transaction.[81] When the number is entered, it brings up the information which collectively constitutes the individual's token identity. The individual is typically required to verify that identity by stating his/her name and date of birth. The card number represents the information which collectively comprises token identity. The number, not the card , is used to establish identity.

The concept of token identity and the use of a number to represent the information which collectively comprises that concept, are evident in the South Australian identity theft provisions in Part 5A of the Criminal Law Consolidation Act 1935 (SA),[82] ('the SA provisions'). This is the only legislation in Australia specifically designed to address identity crime.[83] The focus of the SA provisions is on the use of an assumed identity, as a precursor to the commission of an offence. Consequently, intent to commit 'a serious criminal offence'[84] or use 'prohibited material'[85] for a criminal purpose is required. However, the significance of this legislation lies not in the offences it creates, but in the definitions it uses.

The information which typically constitutes token identity is included in the definition of 'personal identification information.' Even more significantly, the definition includes identification numbers which are used by State and Federal government departments and agencies and by commercial entities, to represent token identity. 'Personal identification information' is 'information used to identify the person including:

(i) information about the person such as his or her name, address, date or place of birth, marital status, relatives and so on;
(ii) the person's drivers license or driver's license number;
(iii) the person's passport or passport number;
(iv) biometric data relating to that person;
(v) the person's voice print;[86]
(vi) the person's credit or debit card, its number, and data stored or encrypted on it;
(vii) any means commonly used by the person to identify himself or herself, (including a digital signature);[87]

---

[80] See Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 25

[81] Australian Government , *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 32.

[82] Part 5A of the Criminal Law Consolidation Act 1935 (SA).

[83] The other States and the Federal government consider that 'identity theft' and 'identity fraud are adequately covered by existing law. Nevertheless amendments have been made to cover specific activities. See for example, Part 10.8 'Financial Information Offences' of the Criminal Code Act (Cth) 1995. Although that legislation is not generally of particular relevance to this discussion, the definition of 'personal financial information is interesting. It is defined in section 480.1 (1) to mean 'information relating to a person that may be used (whether alone or in conjunction with other information) to access funds, credit or other financial benefits.' Part 10.8 also extend to personal information of both living and deceased persons. See section 480.1 (3).

[84] 'Serious criminal offence' is defined in section 144 A as an indictable offence or 'an offence prescribed by regulation for the purposes of this definition.'

[85] 'Prohibited material' is defined in section 144 A as 'anything (including personal identification information) that enables a person to assume a false identity or to exercise a right of ownership that belongs to someone else to funds, credit, information or any other financial or non-financial benefit.'

[86] Voice print is defined in section 144 A to mean 'any computer data recording the unique characteristics of a person's voice.'

(viii) a series of numbers or letters (or a combination of both)intended for use as a means of personal identification.'[88]

Moreover, the SA provisions extend to personal identification information of deceased individuals. It is an offence to use that information with intent to commit or facilitate the commission of a serious criminal offence irrespective of whether the person whose information is used consents, or whether he/she is living or dead. Similarly, 'false identity' is defined as 'a person assumes a false identity if the person pretends to be or passes himself or herself off as, some other person.'[89] That other person may be living or dead, real or fictional, natural or even corporate.[90] In these respects, the legislation is ground breaking.

B. *Database Identity*

Like the NIS, all the information recorded on the surface of the access card and in the chip on the card is also recorded in the Register. Also like the NIR, the Register contains additional information.

Although date of death and sex are not part of the information which (ostensibly[91]) constitutes token identity, they are recorded in the Register[92] and are therefore part of the individual's database identity under the Australian scheme. Like the additional information recorded in the NIR, the Register also includes citizenship, [93] residency, information about other cards,[94] information about registration including whether proof of identity is 'full' or 'interim' and a copy of and information about 'a document you produced in relation to proving your identity' as well as technical and administrative information.[95] This information identifies and it tells a story about the individual. Like the information in the NIR, it can influence how an individual is perceived by both other people and the automated system.

With the possible exception of the technical and administrative information, the information which constitutes database identity is 'personal information' within the meaning of the Privacy Act 1988 (Cth) so that the information privacy protections established under that Act apply to its collection, use and storage. [96] Some of the information may be 'sensitive personal information'[97] a subset of 'personal information' which is afforded a higher level of protection under the Privacy Act.

---

[87] Digital signature is defined in section 144A to mean 'encrypted electronic or computer data intended for the exclusive use of a particular person as a means of identifying himself or herself as the sender of the electronic communication.' 'Electronic communication' means 'a communication transmitted in the form of electronic or computer data.' See section 144A.

[88] See section 144 A. Under section 144 C it is an offence to use another person's personal identification information intending, by doing so, to commit or facilitate the commission of , a serious criminal offence...'

[89] Section 144 A. 'Identity' is not defined. Under section 144B it is an offence to assume a false identity 'intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence.'

[90] Section 144 A.

[91] When the individual is present, these aspects are usually obvious.

[92] Unlike the NIS, date of death and sex are not part of the core identity information. See section 1(7) of the Identity Cards Act.

[93] And indigenous status in the case of Aborigines. See clause 17.

[94] Benefit cards and Medicare number. See clause 17.

[95] Presumably this information will also include access information.

[96] The Privacy Act is modeled on the United Kingdom Data Protection Act. 'Personal information' is defined under s 5 as ' *[I]nformation* or an *opinion* (including information or an opinion forming part of a data base) *whether true or not*, and whether recorded in material form or not, about an individual *whose identity is apparent*, *or can reasonably be ascertained from the information or opinion.*[96] (emphasis added) This definition clearly contemplates that identity can be ascertained from information or opinion. The Act does not apply to personal information collected, used or disclosed for personal, family or household purposes. See section 7B(1) and section 16E.

[97] 'Sensitive information' is health information about an individual as defined in section 6, or personal information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade

However, the Privacy Act is limited in its operation in that it does not apply to all private sector organizations[98] or State contractors,[99] which may be users of the scheme. The Privacy Act is also not considered to apply to personal information of deceased individuals.[100] These weaknesses in the current privacy regime highlight the need to provide adequate and appropriate protection not just for information from which an individual is *identifiable*, but for information that constitutes *identity*.

IV. RAMIFICATIONS

There are many ramifications of the new concept of identity, but the most significant consequences relate to establishing and verifying token identity. Recall that token identity is used to single out an individual from the rest of the population and to authorise the system to transact with that identity.

The key purposes of the United Kingdom and Australian schemes is to 'strengthen proof of identity in the registration process' and to 'reduce fraud'[101] but how effective are the schemes in achieving these objectives?

A. Who's Who?

In the movie 'The Net' the character Angela Bennett played by the actress Sandra Bullock is arrested as Ruth Marx. She tries to explain to her sceptical court- appointed lawyer that she is not Ruth Marx and that she is the victim of identity theft, following an incident in which her purse containing her passport and credit cards were stolen while she was on vacation in Mexico:

> Just think about it. Our whole world is just sitting there on the computer. It's in the computer. Everything. Your DMV records, your Social Security, your credit cards, medical files. All right there. A little electronic shadow on each and every one of us, just begging for someone to screw with it. And you know what, they did it to me. You know what; they

---

association, membership of a trade union , sexual preferences or practices and criminal record. See section 6 (1).

[98] The Privacy Act does not apply to private sector businesses with an annual turnover of $A 3 million or less, though those that hold health information, provide health services or trade in personal information are covered by the Act. See section 6D(4).

[99] State contractors are exempt under section 7B (5). State and Territory public sector bodies are also not within the definition of 'agency' and are specifically excluded from the definition of 'organisation' in the Privacy Act , though by request of the State or Territory, they may be brought into the regime by regulation.

[100] This point has been highlighted by the Australian Privacy Commissioner. See Office of Australian Privacy Commissioner, *Getting in on the Act. The Review of Private Sector Provisions of the Privacy Act 1988*, March 2005, 21. Section 6 (1) of the Privacy Act defines 'individual' as 'a natural person.' The meaning of 'natural person' is not defined in the Privacy Act or in the Acts Interpretation Act 1901 (Cth), nor has it been the subject of judicial consideration. However, 'natural person' is generally considered to be a living person. See Office of Australian Privacy Commissioner, *Getting in on the Act. The Review of Private Sector Provisions of the Privacy Act 1988*', March 2005, 281. Roth also points out that '[I]t is normally accepted that in law, deceased persons have no privacy interests. This is presumably on the basis of the reason d'etre for privacy protection no longer exists, since dead people can feel no shame or humiliation. The underlying common law principle here is much the same as in the law of defamation, which in most jurisdictions does not countenance civil actions that seek to vindicate the reputation of the dead.' See Paul Roth, ' Privacy Proceedings and the Dead' (2004) 11 *Privacy Law and Policy Reporter* 50.

[101] Human Services (Enhanced Service Delivery) Bill 2007, Explanatory Memorandum, 3. The objectives of the NIS are to reduce illegal immigration and illegal working, enhance the United Kingdoms' ability to counter terrorism and serious and organized crime and reduce identity theft. See Home Office, *Regulatory Impact Assessment, Identity Cards Bill Introduced to House of Commons on 25 May 2005*, 1 <http//:www.homeoffice.gsi.gov.uk.html.> 16 May 2006.

> are going to do it to you. I am not Ruth Marx. They invented her and put her on the computer with my thumbprint.[102]

Is this just the stuff of fiction or could this scenario really happen under the NIS or the Australian Access Card scheme ('the ACS')?

Certainly the 'displacement crime' mentioned by McCullagh 'with criminals compelling users to undergo biometric scanning',[103] is not far fetched. McCullagh points out that 'a person's hand or retina prints could be surgically removed – with or without the person's consent'.[104] Seem farfetched? Well, these procedures are possible. Indeed, until recently face transplants such as those depicted in the movie 'Face Off' in which the central characters played by John Travolta and Nicholas Cage surgically swapped faces, were considered science fiction.[105] However, in 2005 the world's first face transplant was successfully performed on a woman in France.

Biometrics can also be obtained from a database or during transmission. The imaging technology which can be used to send and record the biometric data in a database can be used to reproduce accurately the contours of a fingerprint and an iris and facial scan. If a fingerprint, iris or facial scan is obtained, it can be replicated.[106]It may then be attached to information recorded in a database.

Considering the millions of registrations that will be required under both the NIS and AACS[107]and the extent of the information recorded and updated it is at least possible, and probably likely, that not all the data and information entered in the Registers will be accurate and completely up to date. Mistakes, system errors and data manipulation are possible. Even if checks, cross checks and system integrity are particularly robust, no system is infallible. The Registers and the chips on the cards may contain inaccurate information. Furthermore, once data and information are in the chips and Registers they are accorded a level of authenticity which can be enduring - and misleading. As a consequence, the NIS and the ACS may provide ideal conditions in which to construct a false identity.

Consider, for example, a person who constructs a false identity using fabricated information; or who uses an identity of a deceased person not recorded on the Register, rather than assuming

---

[102] '*The Net'*, 1995 Columbia Pictures Industries Inc. Dialogue of the character Angela Bennett played by the actress Sandra Bullock.

[103] Karen McCullagh, 'Identity Information: The Tension between Privacy and the Societal Benefits associated with Biometric Database surveillance' (paper presented at the 20th British and Irish Law, Education and Technology Association Conference, Queens University, Belfast, April 2005) 4 <http//:www.biletapapers/brombyness.html > 27 April 2006.

[104] Karen McCullagh, 'Identity Information: The Tension between Privacy and the Societal Benefits associated with Biometric Database surveillance' (Paper presented at the 20th British and Irish Law, Education and Technology Association Conference, Queens University, Belfast, April 2005) 4 <http//:www.biletapapers/brombyness.html > 27 April 2006. Note, however, that the NIS will use iris scans, not retina scans. Garfinkel also maintains that the danger of mutilation will increase as society increases its reliance on biometrics. Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (2000) 66. The latest biometric readers also detect blood flow as a measure to counteract the use of biometrics from dead bodies and severed body parts.

[105] Paramount Pictures (1997). An undercover agent assumes the physical appearance of a major criminal in order to infiltrate a crime organization. The catch phrase for the movie is '[I]n order to catch him, he must become him'.

[106] Fingerprints and facial features can be reproduced using latex, silicon and other like materials used for theatrical makeup and prostheses. Iris prints can be reproduced using contact lenses or even grafts. A replica can be attached almost invisibly so as to verify identity when using a biometric reader. If the biometric is verified remotely using the Internet, deception can be even easier

[107] 50 million is the estimated number of individuals who will eventually be registered under the NIS. See Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/scheme.html> 10 May 2006. 16.7 million are expected to be registered under the Australian scheme. Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, x.

an identity of a living individual. A 'biographical footprint' can readily be constructed by the perpetrator so that each official document and/or record depends on the one before it, to form a pyramid of falsified identity. On registration the perpetrator will provide authentic biometric data. In the Register that data will be 'sealed to or permanently paired'[108] with registrable facts which are in reality, false. Subsequently, if there is reason to doubt the authenticity of the information and its correlation with the individual, biometric data may be sought.

In this situation, the system will work exactly as designed. Biometric data will be sought from the individual who originally supplied it. It will match and apparently verify the authenticity of the identity. One would expect the authorities to counter that this person would not be registered under the scheme in the first place. However, the possibility of a false identity being created and used in the United Kingdom in this way is acknowledged by the Home Secretary.[109]

Whilst the Home Secretary concedes that a person who operates using false personal and or identifying information may be registered in the NIR using a false identity, he maintains that it would be impossible for such a person to register more than one identity. '[T]here can't be 2 people with the same biometric on the same database claiming to be the same person.'[110] The IPS on its website elaborates on this point: '[B]iometrics are … the best way to prevent criminals from registering for more than one identity card – they could supply a false name and forged documents but their biometrics would be picked up.'[111] Indeed, the Home Office Minister was recently reported to state that '[b]y linking unique biometric information to a secure database with strict rules outlining its use, the scheme will give us all a means of confirming identity.[112] Is this correct? Will fingerprint, iris and facial scans really provide authentic identification?[113]

The first point to be made in response to this question is that all biometrics have error rates. None of the biometrics proposed for the NIS and the ACS currently provide foolproof identification. Mistakes and errors can occur as a result of the conditions under which the biometric is obtained, stored and transmitted. Errors also occur in interpretation of a match. The accepted error rate for automated facial scanning is 10%[114] although an error rate of 2% has been reported in Australia under controlled conditions.[115]

---

[108] Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/scheme.html> 10 May 2006.
[109] Home Secretary, '*IPPR Speech'* 18 November 2004 <http//:www.identitycards.gov.uk**.** html> 16 May 2006.
[110] Home Secretary, '*IPPR Speech'* 18 November 2004 <http//:www.identitycards.gov.uk**.** html> 16 May 2006.
[111] Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/scheme.html> 10 May 2006.
[112] See Mark Ballard, 'UK Govt says Broken Passport System Justifies ID Cards' *The Register,* (London), 20 March 2007<http//:/:www.theregister. co.uk/ 2007 03/20/passport_fraud/print.html> 29March 2007.
[113] Note that the term 'reliable' has deliberately not been used in framing this question. A result may be reliable in the scientific sense so that when the measurement procedure is repeated, the same result is consistently produced. Reliability in this sense is applicable to verification of identity using the NIR but not to authentication of identity. The fact that a result is reliable does not necessarily mean it is valid. See Sandy Zabell, 'Fingerprint Evidence' (2005) 13 *Journal of Law and Policy* 143 for an excellent discussion of recent issues regarding fingerprint evidence from a scientific and mathematical perspective.
[114] One report states the error rate at 31 percent for 'photographs', though the conditions under which this rate was obtained are not specified. See Philip Johnstone, 'Iris Scans Dropped from ID Card Plans', *Telegraph*, 12 January 2007 <http://telegraph.co.uk/ core/Content /displayPrintable.jhtml;jsessionid =DWNA31GV>29 March 2007.
[115] Karen McCullagh, 'Identity Information: The Tension between Privacy and the Societal Benefits associated with Biometric Database surveillance' 3 (Paper presented at the 20th British and Irish Law, Education and Technology Association Conference, Queens University, Belfast, April 2005) 4 <http//:www.biletapapers/brombyness.html > 27 April 2006. Reportedly, an error rate of 2% was achieved in trialing Smartgate at Sydney airport using Qantas crew. However, lighting conditions in the building were modified to improve facial recognition, users were given special training , the system was used daily to scan a relatively small group of (recurring) faces ,and templates stored by the system and used for comparison, were updated daily. London School of Economics and Political Science and the Enterprise Privacy Group,

The likelihood of error may seem low, but even a low error rate can produce a significant number of mistakes in a large population To put this in perspective, consider a hypothetical error rate of say 2% for a population of 50 million people**,** which is the estimated number of individuals who will eventually be registered under the NIS[116] and in a population of approx 17 million who will be registered under the ACS[117]. In Australia, a 2% error rate potentially amounts to 340,000 incidents of incorrect identification in that population. In the United Kingdom that error rate could result in 1,000,000 people be affected. Of course any error rate is unacceptable if an individual is a victim of identity fraud and /or an individual finds that the system does not accept his/her legitimate identity.[118]

Verification of identity is of particular concern under the Australian scheme. While the NIS will use biometrics for some transactions,[119] and indeed several different biometrics, the ACS will not use any biometrics to verify identity.[120] The ACS uses only one biometric, a face scan, which is obtained at the time of registration and is stored in the Register. That scan is used to *authenticate* identity but not to routinely verify it for transactional purposes. Verification is by matching the token identity information on record with that presented at the time of a transaction. What this means in practice is that in addition to matching the other token identity information, a human being compares the physical appearance of the individual presenting the card with the photograph on the surface of the card.[121]

Verification by visual comparison is particularly prone to error unless the individual is known to the person making the comparison. As Bromby and Ness state:

> R]ecognising familiar faces is a fairly robust process. We can easily recognize people that we know in different contexts and view. However, for previously unfamiliar faces, recognition can easily be disrupted by changes in viewpoint, lighting and image quality. If the individual is not known to the person checking the ID card, matching the presenter with the photo even in optimal conditions, is likely to be inaccurate.[122]

In a study in which supermarket cashiers compared real people not known to them to photographs on credit cards they presented, only fifty percent accurately accepted or rejected the cards. When the card contained a photo resembling the person presenting it, only thirty six

---

'*The Identity Project. An Assessment of the UK Identity Cards Bill and its Implications'* Interim Report, March 2005, 49.

[116] Tony Mansfield and Marek Rejman-Green, '*Feasibility Study on the Use of Biometrics in an Entitlement Scheme'* (2003), 6.

[117] 16.7 million adults will be registered over two years. See Australian Government,*Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, x.*

[118] As may occur if some of his/her token identity information has been used to construct a false identity or, if an individual is wrongly accused of assuming a false identity because the token identity presented does not match the information on record in the chip or Register.

[119] As the Identity and Passport Service states '[A]nyone trying to make a major financial transaction, for example, would have their biometrics data checked against those held in the NIR. If they were not the registered cardholder this check would fail.' See Identity and Passport Service, *Using the Scheme in Daily Life, Transferring Money,* <http//:/www. identity cards.gov.uk/scheme.html> 10 May 2006.

[120] Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 33 and 36.

[121] This approach is also used to compare a signature. A signature is on the surface of the Access Card. The photo and signature are the only links with the physical person.

[122] Interestingly, colour photography (video footage in the study) of itself does not improve identification. When the target was unknown to the identifier, colour increased the number of false alarms in the identification task. Michael Bromby and Haley Ness, 'Over-observed? What is the Quality of this New Digital World?' (Paper presented at 20th Annual Conference of British and Irish Law, Education and Technology Association, Queens University, Belfast, April 2005) 7 http//:www.biletapapers /brombyness.html > 27 April 2006. See also Graham Davies and Sonya Thasen, 'Closed Circuit Television: How Effective an Identification Aid?' (2000) 91(3) *British Journal Of Psychology* 411.

percent of the cashiers correctly rejected the card.[123] The higher the quality and clarity of the photo, the more accurate the identification process, providing the individual is known to the identifier.[124]

In other words, identification is by picture recognition rather than actual identification of the individual's face. 'A face must be learnt in order to be recognised- exposure to different angles, expressions and situations'.[125] Training and experience in identification does not increase the accuracy of identification.[126] Moreover, even obvious discrepancies are often explained or justified, without further investigation:

> You're trying to match a woman's face to a picture … [b]ut you see that the woman has a mole, and the face in the picture doesn't. Well maybe its covered up with make up, you say. OK, but the woman has straight hair and its curly in the picture. Maybe the woman in the picture had a permanent?[127]

Matching does not establish the validity of the data and information, merely that it cross checks. That it matches, appears to match, or is assumed to match, does not mean that it is accurate and authentic, yet correlation is considered to be verification under both the United Kingdom and Australian schemes. In fact, of course, the validity of the information which comprises token identity and database identity depends on the integrity of the processes used to collect, update, store and use that data and information.

V. CONCLUSION

The Identity Cards Act and the Australian Access Card legislation are founded on 'one person: one identity,' which has been hailed as a significant change to the common law.[128] Of even more significance, however, is the nature of the concept of identity now evident in both the United Kingdom and Australia and its ramifications.

---

[123] Richard Kemp, Nicola Towell and Graham Pike, 'When Seeing Should Not Be Believing: Photographs, Credit Cards and Fraud' (1997) 11(3) *Applied Cognitive Psychology* 211.

[124] An error rate of 30 percent was found when participants were asked to match for view and expression an unknown target with an array of video stills. A difference in viewing angle of the video still and target further decreased the accuracy of identification. Research also shows that the face is the most significant feature for recognition if the individual is known to the identifier. Although gait, body shape and clothes play a role, facial information is primarily used to make the identification. Vicki Bruce *et al*, 'Verification of Face Identities from Images Captured On Video' (1999) 5(4) *Journal of Experimental Psychology: Applied* 339. Even when only two images were presented, accurate identification of the target from an array of video stills was still low if the target was unknown to the identifier. Vicki Bruce and Andy Young, 'Understanding Face Recognition' (1986) 77(3) *British Journal of Psychology* 305. See also Vicki Bruce *et al*, 'Matching Identities of Familiar and Unfamiliar Faces caught on CCTV Images' (2001) 7(3) *Journal of Experimental Psychology: Applied* 207.

[125] Michael Bromby and Haley Ness, 'Over-observed? What is the Quality of this New Digital World?' (Paper presented at 20th Annual Conference of British and Irish Law, Education and Technology Association, Queens University, Belfast, April 2005) 7 <http//:www.biletapapers/brombyness.html > 27 April 2006.

[126] A Mike Burton *et al*, 'Face Recognition in Poor Quality Video: Evidence from Security Surveillance' (1999) 10(3) *Psychological Science* 243.

[127] Sarah Kershaw, 'Spain and US at Odds on Mistaken Terror Arrest', *New York Times* (New York), 5 June 2004, A1. Perception and 'seeing' what one expects or hopes to see can also lead to distortion of reality. See also Sandy Zabell, 'Fingerprint Evidence' (2005) 13 *Journal of Law and Policy* 143, 155 where the implications of justifications and explanations in relation to fingerprint evidence are discussed.

[128] See John Wadham, Coailfhionn Gallagher, Nicole Chrolavicius, *The Identity Cards Act 2006* (2006), 127. Identity should not be confused with the ID card. In some circumstances two ID cards may be issued to the same individual. The examples discussed in Parliamentary debate included transsexuals and Irish nationals. Transsexuals may be issued with two ID cards to reflect each gender and Irish nationals may be issued with two ID cards, one of which will only specify his/her UK citizenship. See United Kingdom, *Parliamentary Debates*, House of Lords, 30 January 2006, col 79 (Baroness Scotland of Asthal).

Identity is now more than an evidentiary standard. Identity has evolved into a legal concept in which an individual's identity consists of a defined collection of recorded data and information. Indeed, token identity can consist of just name, date of birth and address;[129] and may even be represented by a number. This information is linked to a physical person but that link can be tenuous even if it includes biometrics. The information is linked to a person *because that is how it is recorded* in chip and/or on the Register.

This new concept has immediate implications for residents of the United Kingdom and Australia as a consequence of the national identity registration schemes planned in those countries. Although at present those schemes are for defined purposes, ostensibly to gain access to government services,[130] they will require most adults to register and the system will be used by both public and private sector organizations. Both schemes also permit the identity card to be used at the discretion of the individual, to generally prove identity.[131] It does not take much imagination to envisage a future where an individual's identity for most, indeed probably all, transactions will have to be established and verified using token identity, as recorded in a national register.

The irony is that now that identity in this context is no longer just an evidentiary standard, the standards and procedures for establishing and verifying identity are in many respects less rigorous than traditionally required. The basis for establishing and verifying identity is by matching data and information with that data/ information on record,[132] even though matching does not necessarily mean that the data and information is accurate. Yet it is clear from the legislation that there is a presumption of accuracy[133] and that the burden of establishing that an identity (as recorded), is inaccurate, is borne by the individual. The presumed accuracy of this concept of identity, its potentially enduring nature and the level of authenticity accorded to it, can have wide ranging consequences, especially considering the nature and volume of data and information which potentially can be accessed - as both the fledgling United Kingdom and Australian schemes already vividly illustrate.

---

[129] See for example, the 'minimum KYC information' under the AML/CTF legislation. See draft rule 2.2.2.

[130] The data and information in the Register can be used for broader purposes. The Identity Cards Act includes national security and policing powers. See for example, section 18. Private sector organizations will be able to access at least some information on the NIR. For a recent report on plans to charge private sector organizations including banks and financial institutions for this information see James Slack and Sue Reid, 'Your ID Card Details will be Sold to Banks,' *Daily Mail*, 11 March 2007 <http://dailymail.co.uk/pages/text/print.html?/in_article_id=441586&in_page_id=1770>29 March 2007.Although nothing in the Access Card legislation authorises access by the law enforcement or security agencies, disclosure can be authorized by the Privacy Act and by warrant. The Australian government has stated that 'it is the policy intent that the Australian Federal Police (AFP) should have the ability to obtain and use information from the Register and the chip of the card under the Privacy Act to respond to threat-to –life or threat-of –injury situations, disaster victim identification and emergency responses and investigation of missing persons.' See Australian Government Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, 59.

[131] See section 16 of the Identity Cards Act and clause 40 of the Bill. See also Australian Government Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, 44.

[132] This is true for registration too because the individual will still establish his/her identity for registration purposed by producing documents such as birth certificate, driver's license, credit cards and other government issued cards. The information in these document is cross checked to see if it matches and where possible, it will also be checked against the database of the relevant department/agency.

[133] This more obvious in the Identity Cards Act. See for example, section 1 (3). The presumption is implicit in the Access Card legislation.