Thesis for Degree of Doctor of Philosophy

Digital Identity: An Emergent Legal Concept

An analysis of the role and legal nature of digital identity in a transactional context

Clare Sullivan LLM, MBA

Law School, University of Adelaide

July 2009

Table of Contents

Abstract iv

Declaration vi

Publications and Presentations vii

Acknowledgment and Dedication viii

Abbreviations/Terms and Definitions ix

Prologue 1

1. Digital Identity – Introduction 3

1.1. Genesis of this Thesis 3

1.2. Importance 7

1.3. Approach of this Thesis 10

1.4. Structure of this Thesis 13

2. Digital Identity – A New Legal Concept 20

2.1. Introduction 20

2.2. Central Thesis 21

2.3. Registered Digital Identity in the United Kingdom 22

2.4. The Relationship between Token Identity and Database Identity in the United Kingdom 29

2.5. Distinguishing Solove's 'Digital Person' 32

2.6. Digital Identity in Australia 36

2.7. Conclusion 43

3. Digital Identity – The Nature of the Concept 46

3.1. Introduction 46

3.2. Registered Digital Identity 47

3.3. The Role and Nature of Token Identity 48

3.4. Is Token Identity the Legal Person? 55

3.5. Token Identity is the Legal Person 59

3.6. Conclusion 64

4. Digital Identity – Inherent Vulnerabilities 67

4.1. Introduction 67

4.2. The Fallibilities of the Identifying Information 69

4.3. Conclusion 79

5. Digital Identity – Consequential Individual Rights 81

5.1. Introduction 81

5.2. Identity Distinguished From Privacy 86

5.3. The Right to Identity under the Scheme 89

5.4. An Express Right to Identity 91

5.5. Right to Identity under European Human Rights Law 93

5.6. The Protection Provided By the Right to Privacy 102

5.7. Conclusion 123

6. Digital Identity – Protection 126

6.1. Introduction 126

6.2. The Wrong and the Harm Caused by Misuse of Token Identity 130

6.3. Identity Theft Distinguished from Identity Fraud 135

6.4. Is Identity Theft Really Theft? 138

6.5. Identity Theft is Theft 143

6.6. Criminal Damage 157

6.7. Conclusion 161

7. Digital Identity – Conclusion 165

7.1. Introduction 165

7.2. Insight Provided by this Thesis 166

7.3. 'Tomorrow is nearer than you think' 172

8. Bibliography 174

8.1. Articles/Books/Reports 174

8.2. Case Law 180

8.3. Legislation 183

8.4. Treaties 185

8.5. Other Sources 185

Abstract

This thesis examines the emergent legal concept of digital identity under the United Kingdom National Identity Scheme ('NIS') and its Australian counterpart, the Access Card Scheme('ACS') proposed in 2007. The *Identity Cards Act 2006* UK c 15 ('*Identity Cards Act'*) and the Human Services (Enhanced Service Delivery) Bill (Cth) 2007 ('Access Card Bill') reveal a remarkably similar concept of identity in terms of its constitution and especially its functions.

The United Kingdom scheme is currently being established, whereas the proposed Australian Scheme has been shelved following a change of government late in 2007. The NIS is therefore used as the model for this study but the analysis applies to any such scheme based on digital technology, including the ACS, should it be resurrected.

The emergent concept of digital identity which is the subject of this thesis arises from legislation. It is a legal construct which consists of a collection of information that is stored and transmitted in digital form, and which has specific functions under the identity scheme.

In this study, the information recorded about an individual for an identity scheme is referred to as an individual's 'database identity.' Database identity consists of information prescribed by legislation. Collectively, that information comprises an individual's registered identity. Under the United Kingdom scheme, it includes an individual's name/s, gender, date and place of birth and date of death, photograph, signature and biometrics, and other information such as citizenship and residential status including residential address/es, nationality, identity card number, passport number, work permit number, driver's licence number, and administrative information such as security and verification details.

Within database identity is a small subset of information which is an individual's transactional identity, that is, an individual's identity for transactional purposes. In this study, that subset of database identity is called an individual's 'token identity'. Under the NIS, token identity consists of name, gender, date and place of birth, date of death and biometrics. Token identity is the gateway to the other information which makes up database identity and token identity has specific functions at the time of a transaction which give it legal character. In effect, it operates as the individual's transactional 'key.' Presentation of the required token identity at the time of the transaction enables the system to recognise, and to deal with, the registered identity.

This thesis is therefore not about identity in the deep philosophical sense of 'who am I?' or 'what makes me, me?' It is about a legal concept of individual identity for specific purposes under a national identity scheme. In many ways, though, the concept of digital identity which is the subject of this thesis is just as important in a modern legal context. Under a national identity scheme, the response to the question 'who am I? ' is 'you are who the scheme (and in particular, the National Identity Register ('NIR')) says you are.'

As the first conceptual legal analysis of identity in a transactional context, this thesis examines the functions and legal nature of database identity, and particularly token identity. Token identity has specific functions at the time of a transaction which are analysed from a legal perspective to determine whether token identity is a form of legal personality.

This thesis also contends that individual personal and proprietary rights necessarily apply as a result of the functions and legal nature of this emergent concept of identity. In addition to the

well- recognised right to privacy, this thesis argues that the concept gives rise to the right to identity which has been overlooked in this context.

For the first time, identity as a legal concept is distinguished from privacy which is the focus of legal scholarship and jurisprudence in this area. The right to identity is contrasted with the right to privacy and the protection afforded by the right to identity in this context by those human rights in the United Kingdom is considered. The protection afforded to an individual in the United Kingdom is contrasted with the situation in Australia which does not currently have a comprehensive national human rights charter.

In view of the limited protection which is currently provided to token identity by the civil law, the protection provided by the criminal law in both the United Kingdom and Australia becomes particularly significant in considering the obligations and rights which arise under the scheme. The adequacy of the criminal law in addressing the nature and consequences of the dishonest use by a person of another person's identity information is therefore also examined.

Identity theft is defined and distinguished from identity fraud, having regard to the emergent concept of digital identity and the wrong and the harm caused by its misuse. In particular, the nature of token identity is examined and the consequences of its misuse by another person are considered in determining whether token identity is property which is capable of being the subject of theft and criminal damage.

The thesis concludes by summarising the major insights provided by chapters 1-6 with a view to the future when national identity schemes like that of the United Kingdom, and indeed international schemes, will be commonplace and token identity routinely required for most commercial transactions. In that environment, being asked to provide one's token identity is likely to be as common and as routine as being asked one's name.

Declaration

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution to Clare Linda Sullivan and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of my thesis when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968. The author acknowledges that copyright of published works contained within this thesis, as listed in the Bibliography, resides with the copyright holder(s) of those works.

Clare Sullivan
July 2009

Publications and Presentations

Parts of this thesis have been published in the following peer reviewed articles and presentations

Clare Sullivan, 'Digital Identity – The 'Legal Person'?' (2009) 25(2) *Computer Law and Security Law Review* page number yet to be assigned.

Clare Sullivan, 'Digital Identity – The 'Legal Person'?' paper accepted for presentation at the International Workshop in E – Forensics law at the International Conference on Forensics Applications and Techniques in Telecommunications, Information and Multimedia, Adelaide, Australia 19-21 January 2009.

Clare Sullivan, 'Is Identity Theft Really Theft?' (2009) 23(1-2) *International Review of Law, Computers and Technology* 85.

Clare Sullivan, 'Is Identity Theft Really Theft?' paper accepted for presentation at the 2007 British and Irish Law Education and Technology Association conference in the United Kingdom in April 2007.

Clare Sullivan, 'Identity or Privacy?' submitted on request for Special Issue: Identity, Privacy and New Technologies in (2008) 2(3) *International Journal of Intellectual Property Management* 289.

Clare Sullivan, 'Who's Who – Conceptualising Identity' (2007) 21(3) *International Review of Law, Computers and Technology* 327.

Clare Sullivan, 'Conceptualising Identity' paper accepted for presentation at the 2007 British and Irish Law Education and Technology Association conference in the United Kingdom in April 2007 and for publication as a *BILETA paper* on-line at bileta2007.co.uk/papers.

Clare Sullivan, 'The United Kingdom Identity Cards Act – Civil or Criminal?'(2007) July *International Journal of Law and Information Technology* 1.

Clare Sullivan, 'The United Kingdom Identity Cards Act 2006 – Proving Identity?' (2006) 3 *Macquarie Journal of Business Law* 259.

Acknowledgment and Dedication

I thank my supervisors Mr Ian Leader-Elliott Reader in Law and Professor Ngaire Naffine of the Law School, University of Adelaide for their guidance and support.

I acknowledge, with gratitude, the financial support provided by the Faculty of the Professions, University of Adelaide in awarding me the Divisional Scholarship which has supported me throughout my candidature. I thank the Law School for supporting the award of the Divisional scholarship and in enabling me to attend the BILETA conferences in the United Kingdom in 2007 and 2008 to present my thesis. My thanks go to the academic staff for their guidance and support, and to the professional staff of the Law School, University of Adelaide, and of the International Graduate School of Business, University of South Australia for their help and kindness.

I thank my family and friends for their unwavering support, patience and understanding. I dedicate this thesis to my mother, who gave me the gift of life, and whose death gave me an even greater gift, in showing me how to live that life.

I thank God for giving me the opportunity to do this thesis and I thank God that it is finished!

Clare Sullivan
July 2009

Abbreviations/Terms and Definitions

Abbreviation/Term	Definition for this Thesis
ACR	Access Card Register i.e. the database/s to be used for the proposed Access Card Scheme
ACS	The Australian Access Card Scheme proposed under the Human Services (Enhanced Service Delivery) Bill 2007 (Cth)
Access Card	The 'smart' identity card to be used in the ACS
Access Card Bill	The Human Services (Enhanced Service Delivery) Bill 2007 (Cth)
BBC	British Broadcasting Corporation
biometrics	The fingerprints, face scan and iris scans proposed for the NIS and the face scan proposed for the ACS
Charter of Fundamental Rights of the European Union	Charter of Fundamental Rights of the European Union (Official Journal of the European Communities 2000/C 364/01) 18 December 2000
Computer Misuse Act	*Computer Misuse Act 1990* (UK) c 18
Convention on the Rights of the Child	The United Nations *Convention on the Rights of the Child*, opened for signature 20 November 1989 1558 UNTS 530 (entered in to force in the United Kingdom 15 January 1992) (entered into force in Australia 16 January 1991)
Criminal Law Consolidation Act	*Criminal Law Consolidation Act 1935* (SA)
Criminal Code Act	Criminal Code Act *1995* (Cth)
Criminal Code	The *Criminal Code* forming the Schedule to the *Criminal Code Act 1995* (Cth)
Criminal Damage Act	*Criminal Damage Act 1971*(UK) c 48
database identity	The prescribed information which constitutes an individual's identity under an identity scheme. Database identity includes token identity which is an individual's transactional identity under an identity scheme
database identity information	The individual components of the prescribed information which constitutes database identity, that is, the separate components, not the set which collectively constitutes database identity
Data Protection Act	*Data Protection Act 1998* (UK) c 29

Abbreviation/Term	Definition for this Thesis
Data Protection Directive	*Data Protection Directive 95/46 EU* of the European Parliament and of the European Council of 24 October 1995
DNA	Deoxyribonucleic acid
identity	An individual's identity composed of information which is stored and transmitted in digital form, with a particular focus on the NIS and ACS
ECHR	*European Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950) 213 UNTS 221, (entered into force 3 June 1952)
European Court	European Court of Human Rights
FBI	United States Federal Bureau of Investigation
Fraud Act	*Fraud Act 2006* (UK) c 35
Human Rights Act	*Human Rights Act 1999* (UK) c 42
identifying information	The identifying information as set out in Schedule 1 of the *Identity Cards Act*, that is, the individual's handwritten signature, head and shoulders photograph and biometrics which under the NIS are fingerprints, a face scan and iris prints
ID card	The identity card issued under the NIS
Identity Cards Act	*Identity Cards Act 2006* (UK) c 15
Identity Cards Bill	Identity Cards Bill 2004(UK)
identity crime	Identity crime includes identity theft and identity fraud as defined in this thesis
identity fraud	Dishonest, false representation as to any registered database identity information including token identity information
identity register	Database or databases which constitute the identity register for the identity scheme and which contain the information which collectively comprises database identity including token identity
identity scheme	A scheme which requires an individual to establish his/her identity at the time of a transaction by providing information which matches the information digitally recorded in the identity register

Abbreviation/Term	Definition for this Thesis
identity theft	Dishonest misuse by a person of another person's registered token identity for a transaction
individual	A natural person. In this thesis individual includes both living and deceased natural persons
information	Information in this thesis includes 'data,' unless otherwise indicated
IAFIS	Integrated Automated Fingerprint Identification System
IPS	United Kingdom Identity and Passport Service
ITAIS	Integrated Automated Fingerprint Identification System
legal person	The being, entity or unit which bears legal rights and duties and so possesses what is called a legal personality
MCCOC	Model Criminal Code Officers' Committee of the Standing Committee of Attorneys- General
MCLOC	Model Criminal Law Officers' Committee of the Standing Committee of Attorneys- General
NIS	National Identity Scheme in the United Kingdom established under the *Identity Cards Act*
NIR	United Kingdom National Identity Register, that is, the databases which collectively comprise the identity register for the NIS
PIN	Personal Identification Number
privacy	Unless otherwise indicated, 'privacy' in this thesis includes data protection rights and duties arising under legislation such as the *Data Protection Act* and the *Data Protection Directive* and its equivalent in Australia, the *Privacy Act*; as well as the rights and duties now recognised in the United Kingdom under recent developments in the law of confidence and which are developing in Australia under the tort of privacy
Privacy Act	*Privacy Act 1988* (Cth)
registered identity	The identity as registered under the identity scheme. Registered identity is the individual's database identity including token identity as registered, that is, recorded, under the identity scheme

Abbreviation/Term	Definition for this Thesis
State government	Governments of the States and Territories of Australia, either collectively or individually as indicated by the context
the system	Operations for the identity scheme
Theft Act	*Theft Act 1968* (UK) c 60
TIA	'Total Information Awareness' the fictional identity database featured in the BBC series *The Last Enemy*
token identity	The set of identity information which constitutes an individual's transactional identity under an identity scheme. Token identity is a subset of the information which comprises an individual's database identity under an identity scheme
token identity information	The individual components of the information which constitutes token identity, that is, the separate components, not the set which collectively constitutes token identity
token identity transaction	A transaction for which an individual is required to establish his or her identity by using his or her token identity
transaction	A dealing whether in-person (that is face to face) or using remote communication (such as a telephone, the internet or a computer network), for which an individual is required to establish his or her identity. A transaction 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 but does not include transactions and dealings of a non- business nature such as domestic and social interaction. When discussed in the context of legal relations such as in relation to the legal person, 'transaction' is a legal transaction such as a contract, for example
transactional identity	The identity which is verified under an identity scheme for a transaction. An individual's transactional identity is his or her token identity as recorded in the identity register
United Kingdom	United Kingdom of Great Britain and Northern Ireland
United States	United States of America

Prologue

From the outset, the United Kingdom Identity Cards Bill was controversial. The Bill was rejected on five occasions by the House of Lords before a compromise was reached which enabled the Bill to be passed two years after its introduction. The Conservatives and Liberal Democrats still oppose the legislation and the NIS it establishes, and the Conservatives announced that they will repeal the legislation if they win the next election. That, however, is a most unlikely prospect because as the then Home Secretary, Charles Clarke commented, the scheme will be unstoppable by that time.[1]

The NIS has since been subject to change in relation to logistical details and the implementation schedule; and there is still uncertainty as to some aspects of its operation. Much of the detail will be specified in regulations which are yet to be drafted. However, the basic features of the Scheme and its intended operation are clear from the *Identity Cards Act* and from publications produced by the Home Office and the Identity and Passport Service ('IPS') which is responsible for its operation.

The NIS is currently being trialled and is scheduled to be phased in from late 2008. The aim is that registration will eventually be 'universal' and the intention expressed at the time the *Identity Cards Act* was enacted was that the NIS will eventually be compulsory for all United Kingdom residents over 16 years of age. According to Shadow Home Secretary David Davis the government is 'trying to introduce this very slowly so that by the time they come to make it compulsory they will have more than half the population already on and the politics will have gone out of it.'[2]

In March 2008, the government announced that the scheme will initially be compulsory for some non-European Economic Area foreign nationals living in Britain from late 2008 and for United Kingdom citizens, and European Economic Area nationals who work in 'sensitive' airside airport jobs, from 2009. From 2011, registration on the NIR will be compulsory for all British citizens applying for a passport, with a view to registration becoming generally compulsory in 2017.

Identity cards are not new for British citizens. An identity card was used during World War II as part of national security, primarily to deter, and detect, enemy spies. The card was discontinued in 1952 because it was considered unnecessary in peace time. Reportedly, the card also hindered police investigations because many citizens resented being asked to produce a card to establish their identity. This background has coloured the debate in the United Kingdom and on 18 November 2004 in his speech about the new identity card, Charles Clarke alluded to 'the clumsy way in which they were handled in the post war era.'[3]

The new scheme has broad similarities with the earlier scheme, in that it was also established for national security purposes and has been introduced against a background of heightened security concerns, but the *Identity Cards Act* applies to residents in the United Kingdom, not just British citizens. The new scheme also has broader purposes, including control of

---

[1] British Broadcasting Commission News, *Q&A Identity card plans* <http:// www. newsvote. bbc.co.uk.html> at 3 April 2006.
[2] British Broadcasting Commission, '*Rethink on Identity Cards* <http://www.bbc.co.uk/mpapps/page tools/print/ news.bbc.co.uk/2/hi/uk_new/politics> at 7 March 2008.
[3] Home Secretary, *IPPR Speech* (2004) <http://www.identitycards. gov.uk./publications.html> at 16 May 2006.

immigration and employment and delivery of public services. It is clear that the government intends that the scheme will be used generally to establish identity and that it will be used by both the public and private sectors. Significantly, the foundation of the identity scheme established by the 2006 legislation is the information recorded in the NIR, not the national identity card. The card is optional and if an ID card is issued, there is no compulsion to carry it.

In 2007, a Bill similar to the *Identity Cards Act* was introduced by the federal government in Australia. The Access Card Bill closely followed the United Kingdom legislation, though its purposes were expressed less broadly, that is, to 'reduce fraud,' and improve efficiency in delivery of health and social services benefits.

The Access Card Bill clearly established a system of national identity registration and attempts by the government to present it otherwise can be explained on the basis of political expediency, considering the debate caused by the Australia Card decades earlier. A national identity card has long been a controversial issue in Australia. The proposed Australia Card legislation introduced into Federal Parliament in the 1980s proved to be extremely controversial and did not proceed in face of public outcry. Similarly, when the Prime Minister again floated the idea of a national identity card in 2006, it sparked public debate which subsided when it became apparent that legislation was not imminent.

Indeed, the introduction of the Access Card Bill in 2007 surprised many observers who assumed that it would not be introduced into Parliament until after the federal election in 2007. The Bill was introduced with comparatively little publicity, and after a very short period of public consultation. Its passage was not smooth and on 15 March 2007, it was delayed following a Senate Inquiry.

Like the United Kingdom, the Access Card Bill established the framework for the new ACS and operational details including security and privacy aspects were to be covered in subsequent legislation. However, the Senate Inquiry recommended that the full legislative package be presented in one Bill, so that the entire scheme and all its consequences could be assessed. The government agreed, and the new Bill was to be introduced into Parliament in 2007, with a view to beginning the scheme in April 2008. However, the Federal election late in 2007 and the subsequent change of government led to the Access Card Bill being shelved, as the new government pursued different policy and funding objectives.

Although there are no immediate plans to resurrect the proposed scheme, it is inevitable that a national identity scheme will be established in coming years in Australia and indeed in most other countries. As automated transactions become the norm, transactional identity must be established using a referent standard and that referent standard must necessarily be a database, preferably a national identity database. In Australia, an identity scheme can be established by linking government databases and through sharing of information between federal and State governments, and that is now well underway. Eventually, however, there will be a need to rationalise that information and to authenticate it; and that can only be done though a scheme of national identity registration. That may be done by introducing a scheme like that in the United Kingdom, or it may be done with less fanfare, on a gradual, incremental basis. However, irrespective of how it is packaged, systematic identity registration must be done on a national basis. The information which is recorded as a result of that process will then be regarded as an individual's identity. It is that consequence, and its inevitability, which prompted this thesis.

1. Digital Identity – Introduction

'The document trail started with a tour of cemeteries to collect names and dates of births and deaths of children from their tombstones. The next step was to apply for death certificates through the mail and, using the information on them, to apply again through the mail for birth certificates. The birth certificates were then used to accumulate collections of other documents in the various names, including Medicare cards, voting registration and memberships from clubs and libraries.

Next the proof of identity documents were presented at branches of the four major banks to open accounts in the various names. By then the bank accounts and array of documentation from government agencies and other organisations were so comprehensive that the false identities were, to all intents and purposes, real people. By using personal information to obtain documents which could be used to prove identity, the perpetrator was able to construct 26 identities before being detected.' [4]

1.1. Genesis of this Thesis

Identity is a feature of modern commerce. It is now routinely required for transactions and 'identity theft,' unheard of until comparatively recently, is regularly the subject of news, industry and government reports. These developments prompted me to ask what is one's identity, in a transactional context. In particular, what constitutes it? What exactly, is its function and what is its legal nature? When I set about answering these questions, I found a lot more than I expected.

First, I discovered that although 'identity' is commonly used, it is rarely defined, and its functions and legal role have not previously been analysed in a transactional context. Identity has traditionally been a nebulous notion and in referring to 'identity' without defining it, much of the legal literature in this area lacks precision. It gives the impression that 'identity is identity' whereas the constitution, function and nature of identity depends on context, and as

[4] Gary Hughes, '*Passport to Fraud*', *The Age* (Melbourne), 6 July 2003 <http://www.theage.com.au/articles /2003/07/06 /105 7179212905.html> at 30 October 2008.

Welsey Hohfeld observed, it is important to differentiate the 'purely legal relations' from other non-legal conceptions.[5]

Secondly, I found that, while it is certainly an unintended consequence, the *Identity Cards Act* and the Access Card Bill reveal the emergence of a distinct legal concept of individual identity which includes a new concept of transactional identity. The timing of its emergence in legislation is significant because a concept of transactional identity, consisting of a defined set of information, has been used in commercial practice for years. Its presence in legislation which establishes a national identity scheme and which will be used for a range of transactions with public and private sector entities, confirms its emergence as a distinct legal concept.

That concept is the subject of this thesis. It is constituted by a set of designated information which is given legal force and effect by the enabling legislation and by the operation of the national identity scheme. This collection of prescribed information is what I term an individual's 'database identity.' Under the United Kingdom scheme, database identity consists of the information prescribed by Schedule 1 of the *Identity Cards Act*. The Schedule 1 information consists of an individual's name/s, gender, date and place of birth, date of death, photograph, signature and biometrics, citizenship and residential status including residential address/es, nationality, identity card number, passport number, work permit number, driver's licence number, and administrative information such as security and verification details.

[5] Wesley Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) 23 *Yale Law Journal* 16, 20.

Within database identity is a subset of information which I refer to as an individual's 'token identity.' Under the United Kingdom scheme, an individual's token identity consists of name, gender, date and place of birth, date of death, signature, photograph and biometrics consisting of a face scan, iris scans and fingerprints, as registered under the scheme. Token identity is an individual's identity for transactional purposes. Token identity has specific functions under the scheme which extend beyond just identification of the individual. These functions, especially those which occur at that time of a transaction, give token identity a distinctive legal character.

The discovery of this concept of identity prompted further questions as to its ramifications, especially considering that the identity recorded under the national identity scheme becomes the individual's officially recognised identity. In particular, what are the consequences for an individual whose identity information is used by another individual? These concerns led to specific questions: Do individual rights arise as a consequence of this emergent concept? Specifically, is there a right to identity and, if so, what does it entail in the context of a national identity scheme?

To date, privacy has been the primary focus of legal scholars and the courts in addressing the impact of technology on individuals and there is an extensive body of international legal scholarship on protection of personal information. Because of this focus on privacy, the fundamental human right to identity and its significance in this context has been overlooked. There are several neglected questions. How does identity differ from privacy? Does privacy protect identity? In particular, how do the right to privacy and the right to identity relate to the concept of identity which is the subject of this thesis?

Although they are closely related and often overlap, identity and privacy are separate and distinct concepts. The right to identity and the right to privacy are both fundamental human rights but they protect different interests in different ways. Privacy and identity relate to individual autonomy, but privacy protects an individual's informational autonomy and, specifically, an individual's right to be informed of, and in some respects to control the collection and use of his or her personal information. The right to identity also relates to autonomy, but it is autonomy in a very different sense. The right to identity is the right of a person to be recognised as a unique individual. In the context of a national identity scheme, the right to identity is essentially the right to be recognised and to transact as a unique individual.

Protection of the right to identity prompted an examination in this study of the wrong and the harm caused by the misuse of an individual's identity by another person and raised the questions whether the criminal law protects the use of identity information and, if so, under what circumstances. The criminal law in the United Kingdom and Australia protects against data manipulation, and the *Identity Cards Act* contains new offences aimed at fraud at the time of registration, but there is a question whether existing offences apply to the type of criminal activity that can be expected with the establishment of a national identity scheme. In particular, does the criminal law provide appropriate protection against 'identity theft' as defined in this thesis, that is, the misuse by a person of another individual's token identity?

This thesis considers these questions as they apply to digital identity in the context of a national identity scheme. This journey has been one of discovery. It has taken many unexpected turns, and has resulted in some surprising findings. Most surprising of all is the emergence of a unique, new legal concept of digital identity which fundamentally changes the

way in which an individual is recognised and how transactions are conducted, and the legal implications.

1.2. Importance

This thesis is the first conceptual analysis of digital identity in a transactional context. In analysing the functions and legal nature of an individual's digital identity, in the context of a national scheme of identity registration, and the consequences for an individual, identity is given 'a definite or stable connotation.'[6] In doing so, this thesis adds an important new dimension to current international legal scholarship.

In view of the growing requirement to establish identity for transactions, this research is pivotal in understanding the nature and role of this concept of identity and its implications, especially for individuals but also for government, and for public and private sector bodies using the scheme. The study is conducted against a background of identity crime, specifically where a person misuses the token identity information of another person. Despite government reassurances as to the accuracy of the scheme, it is certainly possible for an identity to be registered using identity information that relates to another person and for another person's registered token identity to be used for a transaction. Both situations have implications for the entities which rely on the accuracy of the identity as registered and presented, and for the government as scheme administrator, and in its security and law enforcement capacities. However, the most significant impact is on the individual whose identity is misused.

[6] Ibid.

In establishing the existence of a legal concept of identity for transactions, and the emergence of a new consequential individual right, that is, the right to token identity, this thesis significantly advances existing legal knowledge. Although this thesis is not about identity in the deep sense of 'who am I?' or 'what makes me, me?,' the enquiry is fundamental and important, because a person's identity as recorded in the national identity register will determine his or her ability to be recognised and to transact as a unique individual under the scheme. Where an individual's token identity information is misused by another person, the individual's ability to be recognised and to transact is fundamentally affected, and the individual will face considerable challenges in establishing not only that 'I am who I say I am' but in establishing 'I am not who the identity register says I am.'

As dealings previously conducted in-person are replaced by dealings conducted without any history of personal acquaintance, and frequently without personal interaction, it is inevitable that identity will assume a crucial role in most, if not all, transactions. The Belgian eID scheme illustrates the pervasive development that can be expected. Belgium was the first European country to issue 'smart' identity cards. The eID scheme rolled out in 2003 and individuals in Belgium now use their identity card to transact with government entities for transactions ranging from filing taxes and applying for official documents such as a marriage certificate, to accessing public libraries and sporting facilities. Even more significantly, the private sector uses the eID card infrastructure for commercial transactions.[7]

Under an identity scheme, identity must be established by providing information which is then verified by comparing it to a referent standard. In modern commerce that referent standard is necessarily a database, whether it is a centralised database, a network of databases, or the data

in the chip on a 'smart' card like the identity card used in the United Kingdom scheme ('ID card') and proposed for the Australian scheme.[8] Transacting entities and government, especially in its security and law enforcement capacity, must be concerned to establish an individual's identity by reference to an authenticated source, that is, an official database.

The NIS which is now being established in the United Kingdom, is the most recent example of a national digital scheme in a major jurisdiction with a common law heritage and which currently also has an established national human rights regime. However, this study and particularly the role of token identity as an individual's transactional identity, the consequential emergence of the right to token identity in the context of the NIS and the implications for protection of identity especially from identity crime, extend to other identity schemes which are founded on a defined set of information. The analysis can be extrapolated to any such scheme which uses a concept of transactional identity that consists of a defined set of information that is stored and transmitted in digital format. Just as registration under the United Kingdom scheme transforms the information which constitutes identity from just information, into a set which has specific legal functions and legal character, and which gives rise to individual rights, so too does registration under other identity schemes. The consequences differ depending on the nature of the scheme, with the most far reaching consequences arising in relation to a national identity scheme.

In comparing the United Kingdom with Australia, this thesis particularly advances legal scholarship in those two jurisdictions. Issues which have been considered primarily on the

---

[7] *Belgium Starts First Phase of Smart Card Rollout*, Card Tech Today, May 2003, 3. See also eIDServices.,*eID* <http//:eid.belgium.be/en/navigation/12000/ index.html> at 19 May 2007.

[8] The chip is a micro processor which is capable of storing information and performing intelligent functions off-line. 'Smart' card technology is used in the United Kingdom scheme and was proposed for the Australian ACS.

basis of privacy are now considered from a new perspective–identity. In exploring the relationship between identity and privacy, and in clearly distinguishing the two concepts, this study contributes to international legal scholarship in relation to identity and privacy, and the attendant international human rights.

For the first time, identity theft and identity fraud are defined and distinguished on the basis of identity as a distinct new legal concept. The adequacy of the criminal law in the United Kingdom and Australia in addressing the type of identity crime that can be expected on the establishment of a national identity scheme is assessed having regard to that concept.

1.3. Approach of this Thesis

This study deals with an emergent concept under a national identity scheme which is not fully established in the United Kingdom and a proposed scheme in Australia which has since been shelved. Nevertheless, implementation of the NIS is well underway, with the first phase beginning in late 2008 and the tenor of this thesis is that the establishment of a similar scheme in Australia is inevitable as automated transactions become standard and identity assumes a significant role. This study therefore assumes that the United Kingdom scheme is in operation and generally adopts the present tense when discussing both the NIS and the ACS. However, operational aspects which are not yet clear are considered in a predictive tense and at times the discussion of the specifics of the proposed Australian scheme must necessarily be in the past tense.

The possibility of a person misusing the token identity information of another person to register under the scheme and subsequently using that identity forms a backdrop to the discussion. Real and hypothetical scenarios are used to illustrate how an individual's token identity information can be misused by another person to register and how an individual's token identity can be used by another person after registration for a transaction. This possibility is introduced in chapter 3, practical aspects are examined in chapter 4 and the impact, especially on the individual, is considered in detail in chapter 5, in relation to individual rights, and in chapter 6, in relation to the protection provided by the criminal law.

The United Kingdom scheme is the most recent operational model of a national scheme of identity registration in a major common law jurisdiction and its features are typical of a modern scheme, so it is used as a Weberian 'ideal type,' that is, as the conceptual model on which to base the analysis.[9] In line with this approach, the United Kingdom legislation is used for the analysis in chapters 4, 5 and 6 but the same issues arise in relation to an Australian scheme.

There are obvious similarities between the United Kingdom's NIS which is used as the basis for the analysis and the proposed ACS, and there are many areas of commonality between the law of United Kingdom and Australia which are explored in this thesis. The composition, functions and legal nature of the emergent concept of digital identity, the consequential individual rights which arise, and the protection afforded by the law in the United Kingdom and in Australia, are all examined in this study.

[9] Max Weber, '"Objectivity" in Social Science' in E. Shils and H. Finch (eds) *The Methodology of the Social Sciences* (1949) 90–1. Weber explains that the 'ideal-type'… 'is not a description of reality' but is used to

In particular, there are also strong similarities between the United Kingdom and Australia in relation to human rights, especially in relation to privacy and identity. In relation to privacy, the Australian *Privacy Act 1988* (Cth) ('*Privacy Act*') is in very similar terms to the United Kingdom *Data Protection Act 1998* (UK) c 29 ('*Data Protection Act*') which is based on the *Data Protection Directive 95/46 EU* of the European Parliament and of the European Council of 24 October 1995 ('*Data Protection Directive*'). The *Convention on the Rights of the Child* opened for signature 20 November 1989 1558 UNTS 530[10] ('*Convention on the Rights of the Child'*) which is considered in relation to the right to identity is also part of the international law of the United Kingdom and Australia. Although Australia does not have a national identity regime like the United Kingdom, the European *Convention for the Protection of Human Rights and Fundamental Freedoms* opened for signature 4 November 1950) 213 UNTS 221,[11] ('*ECHR*') and the rights-based jurisprudence of the United Kingdom is influential in Australia. Victoria and the Australian Capital Territory have recently enacted human rights legislation which is modelled on the *Human Rights Act* 1999 (UK) c 42 ('*Human Rights Act'*) and the *Bill of Rights Act 1990* (NZ) and to an extent, on the bills of rights in the Canadian and South African Constitutions. Other Australian States and the federal government may enact similar legislation over the coming years. The issues examined in this thesis illustrate the importance of establishing a national identity scheme within a national human rights regime.

---

arrange 'certain traits, actually found in an unclear, confused state... into a consistent ideal-construct by an accentuation of their essential tendencies.'

[10] Entered in to force in the United Kingdom 15 January 1992 and entered into force in Australia 16 January 1991.

[11] Entered into force 3 June 1952.

There are also similarities between the criminal law of the two countries. The Australian offences of dishonesty, theft and criminal damage in the federal *Criminal Code*[12] are based on the English offences. However, the South Australian *Criminal Law Consolidation Act 1935* (SA) (‘*Criminal Law Consolidation Act’*) contains modifications which are particularly relevant to identity crime so it is used for comparison and in some respects, as a legislative model.

1.4. Structure of this Thesis

The legislative analysis in chapter 2 reveals the emergence of a remarkably similar legal concept of identity in both the United Kingdom and Australia. Although a similar concept of identity is also evident in anti–money laundering legislation in both countries, the *Identity Cards Act* and the Access Card Bill and the respective schemes, illustrate the operation of the emergent concept particularly clearly.

An individual’s identity under both the NIS and the under the ACS consists of a collection of prescribed information. While the information recorded under both schemes is very similar, its function under the scheme is the important consideration. Within the larger body of recorded information which makes up ‘database identity,’ the small subset of information, ‘token identity’ is presented at the time of a transaction to establish identity. That token identity, as presented, is an individual’s transactional identity. Identity is verified if the information, as presented, matches the information as recorded in the identity register. Verification is a two-step process. Token identity first singles out a registered identity from

[12] The Code forms the Schedule to the *Criminal Code Act 1995* (Cth).

the population as recorded in the register and then enables the system to transact with that identity.

Chapter 3 considers the transactional functions and legal character of token identity. The analysis reveals that token identity is the legal person in a transaction, not the individual who presents it, or who is presumed to present it. If this argument is accepted by the courts, it is a significant change to the common law which has implications for void and voidable contracts. The formation of a contract between token identity and the transacting entity also has wide implications when an individual's registered token identity is misused by another person.[13] These implications extend beyond the individual who is connected to that token identity as recorded in the national identity register, to the transacting entity, the general public and to the government, as scheme administrator and in its law enforcement role.

Chapter 4 examines the inherent vulnerabilities of a national identity scheme like the NIS, particularly in relation to the identifying information. None of the identifying information, including use of biometrics, is infallible and the examination in chapter 4 adds perspective to the preceding analysis in chapter 3 by highlighting the main practical implications, especially for the individual, of verifying identity by matching information. It also sets the scene for the discussion of consequential individual rights in chapter 5.

As discussed in chapters 3 and 4, the scheme relies on comparison of information to establish identity. Identity is verified for a transaction if the required token identity information presented for a transaction matches that on record in the identity register. The required information is mostly biographical but usually some identifying information will be required.

[13] There are also implications for agency relationships, which are beyond the scope of this thesis.

The 'identifying information' under the NIS as set out in Schedule 1 of the *Identity Cards Act* is a signature, a head-and-shoulders photograph and biometrics. Biometrics, in particular, are promoted under the scheme as reliable identifiers but as the discussion in chapter 4 shows, none of the identifying information is foolproof. The consequences for an individual are potentially serious and highlight the need for a national identity scheme to be established within a regime which recognises and protects human rights.

Chapter 5 examines the individual rights which arise as a consequence of the emergent concept of identity. The *Identity Cards Act* is largely silent as to rights of the individual but considering the nature of the emergent concept of identity, the consequences especially for individuals and the vulnerabilities inherent in the NIS, this thesis argues that individual rights arise as a consequence of the scheme. The argument presented in chapter 5 is that the right to identity arises in specific form under the NIS as the right to token identity.

To date, the nature and importance of the right to identity has been obscured by the focus on privacy, so in chapter 5 the fundamental differences between privacy and identity are examined. The analysis contrasts the right to privacy with the right to identity. The nature and origins of the right to identity are considered. The most explicit statement of the right to identity is found in the *Convention on the Rights of the Child* and the reasons for its specific inclusion in the *Convention on the Rights of the Child* resonate with concerns about the use of the NIS to conceal identity and create a false identity. Of course, the right to identity under the *Convention on the Rights of the Child* only applies to children. Although the NIS applies to United Kingdom residents from the age of 16 years and token identity is largely composed of information established at birth, the right to identity under this treaty has limited application.

The European Court of Human Rights ('European Court), however, has stated that a right to identity which applies to adults and children is protected under Article 8 of the *ECHR* which is incorporated into the domestic law of the United Kingdom by the *Human Rights Act*. Chapter 5 examines the right to identity under Article 8. Considering that token identity is an individual's transactional identity, this thesis argues that the right to identity in the context of the NIS, is the right of an individual to an accurate, functional, unique identity and to its exclusive use. It is further argued that abrogation of this right can only be justified on public interest grounds under Article 8(2), in extraordinary circumstances. The unilateral removal or alteration of an individual's token identity in effect disenfranchises the individual and renders him or her non-existent for the purposes of the scheme. Consequently, in an environment where token identity is required for most transactions, the infringement of an individual's right to identity raises significant issues of proportionality, even having regard to the national security and crime detection and prevention purposes of the scheme.

The argument developed in chapter 5 is that in the context of the NIS, the right to identity provides greater protection to an individual's transactional identity than the right to privacy which is more likely to be subordinated to the public interest. Article 8 of the *ECHR* is usually invoked in relation to the right to privacy, so decisions of the European Court on Article 8 are used to examine the interaction between privacy and the emergent concept of digital identity. The analysis shows that the right to privacy does not clearly protect token identity. Although the other Schedule 1 information which comprises database identity is covered by the *Data Protection Act* (and its Australian equivalent, the *Privacy Act*), the privacy interests of the individual are subject to broader societal interests under Article 8(2) of the *ECHR*. At a time of heightened security concerns, public interest considerations may well outweigh individual

interests. The analysis also reveals that in the event of an individual's biographical information being used by another person to register an identity under the NIS, the *Data Protection Act* and the *Data Protection Directive* can operate to protect the privacy of the fraudster and shield the fraud from scrutiny.

Chapter 5 asserts that observance of minimum human rights standards is the most important consideration for a scheme like the NIS. This is especially so, considering the functions and legal character of token identity at the time of a transaction, the inherent fallibilities discussed in chapter 4 including the consequences for the individual, and because the protection and redress currently available under the common law is limited. The discussion highlights the potential impact of the scheme on human rights and the need to recognise and protect those rights. This point is particularly significant for Australia because it does not have a national human rights Act like that of the United Kingdom. This thesis postulates that the United Kingdom approach to the recognition and protection of human rights provides a national model for Australia.

Chapter 6 considers criminal sanctions because they are an integral part of the protection afforded to human rights. Although in time it is likely that the common law will recognise the transactional role of token identity and will develop to protect it, the protection currently available is very limited, even considering the recent extension of the law of confidence in the United Kingdom and to an extent also in Australia. The protection provided by the criminal law is therefore especially significant. The offences of theft and criminal damage can readily apply to the misuse of token identity and, under the European regime, criminal sanctions are a major consideration in determining whether a human right is recognised and adequately protected.

Chapter 6 defines identity theft and distinguishes identity theft from identity fraud, using the emergent concept of digital identity. The nature of the wrong and the harm caused by identity theft are also distinguished from identity fraud in the context of the type of misuse of identity information which is likely to arise under a national identity scheme. The offences enacted in the Identity Cards Act address fraud at the time of registration. However, use by another person of an individual's token identity after registration is not included in the suite of new offences. Dishonest use of an individual's token identity by another person is not an offence under the *Fraud Act 2006* (UK) c 35 ('*Fraud Act'*) because it does not necessarily involve a financial gain or loss.[14] The misuse also does not necessarily involve data manipulation so as to come within the specific computer crime offences in the United Kingdom and Australia.

Because of its nature and consequences, this thesis contends that misuse of an individual's token identity by another person should be an offence. The offence is essentially one of misappropriation, not fraud, and the consequential damage can be criminal. This thesis therefore argues that the appropriate offences are theft and criminal damage. Central to this argument is the contention that token identity is intangible property which can be the subject of these offences.

In the absence of specific identity theft legislation which makes dishonest misuse of token identity an offence in its own right, this thesis asserts that the basic theft offence applies. The analysis in chapter 6 focuses on the individual as owner of the registered token identity and reveals that that the theft offence can, and should, apply to dishonest use of an individual's token identity by another person. The analysis is based on the elements of the offence which

[14] See, ss 2 and 5 *Fraud Act*.

are common to both the United Kingdom and Australia. There are close similarities between the criminal law of the United Kingdom and Australia at both Federal and State level. While the federal *Criminal Code* is the equivalent national legislation in Australia, in some important respects the law in South Australia is more developed and is better able to deal with the unique features of identity crime, so the discussion draws on the South Australian modifications in relation to theft and particularly criminal damage. While the offences of criminal damage in the United Kingdom and under the Australian Federal criminal law are restricted to in their application to tangible property, the South Australian offence extends to intangible property so it can apply to misuse of an individual's token identity under a national identity scheme. This thesis presents the South Australian offence as a model for a criminal damage offence which is capable of applying to misuse of token identity.

Chapter 6 also considers the importance of the accurate labelling of offences and argues that dishonest use of an individual's registered token identity by another person for a transaction should be regarded as identity theft and labelled accordingly. Similarly, intentional or reckless use which damages an individual's registered identity should be considered criminal damage.

Chapter 7 summarises the insights provided by this thesis in a broader context in which schemes like the NIS and the ACS are common not just on a national level but internationally, and where the requirement to establish digital identity for transactions will be as routine as an individual being asked for his or her name. To some, that situation may seem futuristic but my response is that the future is nearer than you think.

The law in this thesis is as of 2008.

2. Digital Identity – A New Legal Concept

In the movie 'Sleepless in Seattle' 8 year old Jonah Baldwin wants to travel from Seattle to New York to meet Annie, the woman he thinks should be his new stepmother. Jonah's 8 year old friend, Jessica books him a seat on United Airlines flight 597 using her mother's computer. Jessica's parents are travel agents. As Jessica makes the booking, she and Jonah have the following conversation:

Jessica: (keying in the details for Jonah's booking) 'I am telling them that you are 12 so the stewardess won't carry you around and stuff like that.'
Jonah: 'Are you crazy! Who would believe that I'm 12?'
Jessica: 'If it is in the computer, they will believe anything.'
Jonah: 'Are you sure?'
Jessica: 'Do you want me to say that you are really, really small for your age and they shouldn't say anything because it will hurt your feelings?'
Jonah: 'Yeh, that's a great idea!'

Needless to say, Jonah travels unaccompanied on the plane to New York without any question being raised about his age.[15]

2.1. Introduction

This chapter examines the composition and legal function of the emergent concept of digital identity in the United Kingdom and Australia. The concept of identity under the *Identity Cards Act* is compared to the concept of identity in Australia, which is most clearly evident in the Access Card Bill introduced into federal Parliament in 2007. While the Act and the Bill appear to set criteria for identification of an individual for the purposes of the scheme, on examination they are much more significant in their potential ramifications for individuals, government and the broader community.

The central thesis is that analysis of the *Identity Cards Act* and the Access Card Bill, and the respective schemes, reveal the emergence of a new legal concept of identity. This chapter examines the composition, function and practical implications of authentication of identity

[15] '*Sleepless in Seattle'* Tristar Pictures Inc (1993).

and verification of identity under the *Identity Cards Act* in comparison to the requirements under the Access Card Bill. Though designed for different specific purposes, analysis of the Act, Bill and their respective schemes, reveals the emergence of essentially the same new legal concept of identity.

In this chapter, identification is distinguished from identity as an emergent legal concept, and the implicit assumption that the *Identity Cards Act* and the Access Card Bill merely establish an evidentiary standard for identification of individuals, is challenged. The chapter presents the central thesis that digital identity is emergent as a distinct, new legal concept.

2.2. Central Thesis

The *Identity Cards Act* and the Access Cards Bill confirm the emergence of a new legal concept of identity which consists of database identity and the subset of information which is token identity.[16] Database identity is all the data and information recorded about an individual in the database/s accessible under the scheme. Those databases include the NIR and other government databases and in some circumstances, private sector databases.[17] Token identity is a defined and limited set of information which determines an individual's identity for transactional purposes.

[16] Although, 'information' is used in the *Identity Cards Act* in relation to the NIR, 'data' is used in referring to biometrics and the chip on the ID card. S 42, for example, defines 'biometric information' as 'data about an individual's physical characteristics.' In this thesis 'information' includes data unless otherwise indicated.

[17] Access to proprietary databases may require a court order, although the power to require information for validating the NIR conferred by the *Identity Cards Act* is wide. See s 9 and particularly subs (5)(e). See also ss 7 -21which give extensive power to the Secretary of State to disclose information in the NIR and to obtain information without the individual's consent, usually on public interest grounds although the authority under s 19 does not expressly require that disclosure be in the public interest.

In this chapter the nature and role of token identity and database identity are examined firstly in the United Kingdom, and then in Australia. The implications of the new concept of identity are then examined in detail in the following chapters.

2.3. Registered Digital Identity in the United Kingdom

Section 1 of the *Identity Cards Act* covers the establishment and maintenance of the NIR[18] which is the basis of the NIS. Section 1(7) states that:

> 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)

While section 1(7) appears to be relatively insignificant, it does much more than just set out the information which constitutes 'references' to an individual's identity for the purposes of section 1. The full import of the section becomes evident when the overall scheme of the Act is considered.

[18] The NIR will probably comprise several databases but the British Government has changed its position on this point several times. While a new single database was originally planned, the government has since announced that existing databases will be used for the NIS. Reportedly, the information will be held on three existing separate databases: '[T]he 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 IPS database. See, British Broadcasting Corporation, above n 1.See also, Lucy Sherriff, 'UK Ditches Single ID Database' The Register, (London), at 19 December 2006 <http//:/:www.theregister.co.uk/ 2006/ 12/19/bigbro_cubed/ print/html> at 29 March 2007. In 2007, the Prime Minister 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.the independent.co.uk/uk/politics/article 2154844.ece> at 29 March 2007. However, in March 2008 the Home Secretary confirmed that the NIR will comprise separate databases and that for security reasons biographical information will not be stored in the same database as biometrics (which will initially be just fingerprints) and photographs. See, Home Secretary, 'The National Identity Scheme–Delivery Plan 2008' Speech by the Right Honourable Jacqui Smith, MP, 6 March 2008, 3.

Section 1(7) defines the information which collectively establishes and verifies an individual's identity for the purposes of the NIS. In effect the information recorded in the NIR establishes an individual's officially recognised digital identity.[19] Under section 1(7), an individual's identity is the set of information comprising name/s, gender, date and place of birth and date of death, and external identifying characteristics[20] which are a handwritten signature,[21] 13 biometrics (a face scan, two iris prints,[22]and 10 fingerprints) and a head-and-shoulders photograph. The Act clearly distinguishes this information from the other information recorded in the NIR under Schedule 1.[23] The relationship between the section 1(7) information and the other information recorded in the NIR, can be presented diagrammatically:

[19] As set out in s 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, s 1(4) *Identity Cards Act*.

[20] The 'external identifying characteristics' referred to in this section are specified in Schedule 1 which sets out the categories of information included in the NIR under s 3 *Identity Cards Act.*

[21] Signature' is not defined but it is apparently intended that a handwritten signature be used. See, Tom Geoghegan, 'I've got a Biometric ID Card', *British Broadcasting News* (London), 12 August <http://news. bbc.co.uk/go/pr/fr /1/hi/uk/ 3556720.stm> at 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.' An individual's signature is included in the list of 'identifying information' in sch 1, implying that a handwritten signature is considered a distinguishing physical feature, although it is not mentioned at all in the definition of 'registrable facts,' nor in relation to 'identity' in s 1 *Identity Cards Act.*

[22] It now appears that only fingerprints and a photograph will be used initially, though face and 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 but there are also questions about their reliability as identifiers. See, Philip Johnstone, 'Iris Scans Dropped from ID Card Plans', *Telegraph*, (London) 12 January 2007 <http://telegraph.co.uk/core/Content/displayPrintable.jhtml;jsessionid=DWN A31GV> at 29 March 2007. Recently, however, the Home Secretary referred to only fingerprints, giving the impression that a photograph rather than a face scan may now be used. See Home Secretary, *The National Identity Scheme–Delivery Plan 2008*' Speech by the Right Honourable Jacqui Smith, MP, 6 March 2008, 9.

National Identity Register

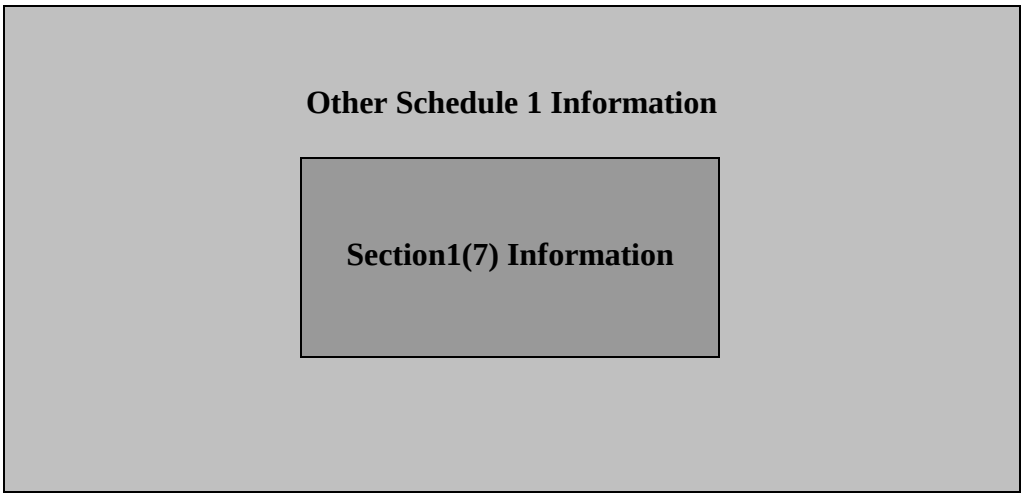

Fig.1.

This approach is intriguing because the other Schedule 1 information includes for example, address, residential and citizenship status as well as numbers such as driver's licence number and passport number, which could be used collectively, or the case of numerical identifiers, used individually, to identify an individual.[24] It prompts the question: why is the section 1(7) information distinguished in this way?

The answer lies in the role the section 1(7) information plays in first identifying an individual for transactional purposes, and then in authorising the system to interact and deal with that

---

[23] Identity and Passport Service, *Corporate and Business Plans 2006-2016,* 42 <http//:www.identitycards .gov.uk /scheme.html> at 10 May 2006. For a recent statement see, Identity and Passport Service, '*Corporate and Business Plans 2006-2010'* <http//:www.ips.gov.uk/identity/publications-corporate.asp> at 1 September 2008.

[24] S 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;[24]
(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;

identity. When the legislation is considered with government documentation about the operation of the scheme, it is clear that the section 1(7) information does not just identify an individual. It enables the system to transact with the registered identity.

Under the NIS, authentication of identity and verification of identity are separate and distinct processes. Identity is initially authenticated at the time an individual is registered under the scheme. Identity is subsequently verified at the time of each transaction. The integrity of the NIS depends on the integrity and rigour of these two processes.

2.3.1. Identity Authentication in the United Kingdom

An individual will usually be required to register in person[25] in order to be interviewed to obtain 'biographical' information, to be photographed and to record the signature and the biometrics. On its website the IPS explains the registration process:

> When you apply for an ID card, we will check your 'biographical footprint' 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.
>
> [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'.[26]

(j) information recorded in the Register at his request.'(emphasis added)

[25] Exceptions are clearly contemplated 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.> at 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.

[26] Identity and Passport Service, '*What is the National Identity Scheme?*' <http//:www.identitycards.gov.uk/ scheme.html> at 10 May 2006. For a recent statement in similar terms see, Identity and Passport Service, *What is the National Identity Scheme?* <http//:www.ips.gov.uk/identity/scheme-what-produced.asp> at 1 September 2008.

As the IPS explains, '[y]our biographical footprint is simply the basic facts about your life, for example: name, date of birth and address.'[27]

The foundation of the accuracy and reliability of NIS in authenticating identity and in subsequently verifying identity is the use of 'identifying information.' Identifying information is a photograph of head and shoulders, fingerprints and 'other biometric information' as well as the individual's signature.[28] The IPS states that,

> [b]ecause 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.[29]

After an individual is registered under the NIS, identity is verified by matching information provided at the time of the transaction with the information recorded in the chip on the ID card if one is issued,[30] or as recorded in the NIR.[31] The information recorded in the chip is also recorded in the NIR.

---

[27] Ibid. See also, Identity and Passport Service, *Using the Scheme in Daily Life* <http://www.ips.gov.uk/identity/how-idcard-daily-providing. asp> at 1 September 2008.

[28] Sch 1 *Identity Cards Act*. 'Identifying information' is confined to an individual's 'external characteristics' that under s 1(7) 'are capable of identifying him' and is therefore narrower than token identity.

[29] Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/scheme.html> at 10 May 2006. For a more recent statement in the same terms see, Identity and Passport Service, *What is the Benefit of Using Biometrics* <http//:www.ips.gov.uk/identity/faqs-biometrics-benefits.asp www.identitycards.gov.uk/scheme.html > at 1 September 2009.

[30] The ID card is not compulsory and it is also not compulsory to carry or present it. The ID card will be a smart card–'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.

[31] Although on-line verification of identity is clearly contemplated, in March 2008 the Home Secretary stated that none of the databases that will comprise the NIR 'will be online, so it won't be possible to hack into them.' It is unclear what this means, however, especially since identity must be either be verified by comparing the token identity presented with the information stored in the chip on the ID card, with the NIR by using on-line verification. Considering that the ID card is not compulsory and that when a card is issued, it is also not compulsory to present it, on-line verification must be a feature of the scheme.

2.3.2. Identity Verification in the United Kingdom

The information required at the time of a transaction is the section 1(7) information which comprises name, gender, date and place of birth (and date of death), and usually at least one piece of the identifying information which is the photograph, signature and the biometrics. Verification of identity involves two steps. First, the required section 1(7) information is presented to establish identity. Presentation may be by personal attendance at which time the information is provided verbally by a person and/or by presenting the ID card.[32] Alternatively, the required information may be provided by telephone or using the internet. This process can be thought of as a key being used to open a door. The required section 1(7) information is the key. When this information is presented, it is like inserting a key into a lock. In the second step, the presented information is compared with that recorded in the chip on the ID card, or in the NIR, to see if it matches. To use the key analogy, if the indentations on the key align with the indentations in the lock, the key opens the door.

Not all the section 1(7) information is necessarily used to verify identity for all transactions. Public and private sector organisations using the NIS will be able to choose the verification method considered most suitable for the transaction. At present, there are basically three levels of verification contemplated by the NIS. The lowest level will be a check using the photo. The next level will involve answers to designated questions and/or a PIN.[33] The highest

---

[32] Under s 6(3) *Identity Cards Act*, the ID card 'must record only the prescribed information' and 'must record prescribed parts of it in an encrypted form.'

[33] There are conflicting statements on the IPS website as to the circumstances in which a PIN will be used. In one example, the IPS states that,'[b]y handing over the card and entering his PIN, Colin is in effect giving his permission for the company to check that the card is genuine and belongs to him.' See, Identity and Passport Service, *Using the Scheme in Daily Life* <http://www.ips.gov.uk/identity/how-idcard-daily-providing.asp> at 1 September 2008. This accords with the definition of 'Security information' in sch 1 *Identity Cards Act*. However, the IPS states elsewhere that,.'[y]ou won't need to carry the card with you at all times, and if you need to prove your identity without the card you will be able to do so by providing a few details about yourself along with a biometric, such as a fingerprint or PIN,' although this use of the PIN does not accord with the examples on the IPS website. See, Identity and Passport Service, *Benefits to the Individual* <http://www.ips.gov.uk/identity/ benefits -individual-british.asp> at 1 September 2008.

level check will include biometrics.[34] Consequently, to return to the lock analogy, it is unnecessary to ensure that all the indentations align, as long as the required number matches.

Depending on the nature of the transaction, the section 1(7) information may be supplemented by additional information such as a PIN or answers to designated questions about other information recorded in the chip and/or in the NIR.[35] Subsections (1) and (2) of section 6 of the Identity Cards Act state that the ID card will contain two sets of information: 'registrable facts'[36] as recorded in the NIR, and information enabling access to the individual's record on the NIR. As an example of the latter, the Explanatory Notes, Identity Cards Act 2006 (UK) ('Explanatory Notes') specifically mention a PIN.[37] This additional information can be thought of as the equivalent of establishing who is holding the key to the door, to ensure that it is in the correct hands. However, these aspects 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 Schedule 1 information, in that it is mostly established at birth and usually remains unchanged until death.[38] Although name and gender may subsequently be changed,[39] birth name, gender, date

---

[34] Identity and Passport Service, '*What Kind of Organizations will use the Scheme?* <http://www.identity cards. gov.uk/scheme.html> at 10 May 2006, and Identity and Passport Service, *Using the Scheme in Daily Life* <http:// /www.ips.gov.uk/identity/how-idcard-daily-providing.asp> at 1 September 2008.

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

[36] As defined in s 1(5) *Identity Cards Act*.

[37] Explanatory Notes, Identity Cards Act 2006 (UK) 9 <http//:www.opsi.gov.uk.html> at 19 May 2006. 'Security information' in sch 1 Identity Cards Act includes 'a personal identification number,' 'a password or other code' 'to be used for facilitating the making of applications for information to be recorded in his entry and for facilitating the provision of that information'. It also includes 'questions and answers to be used for identifying a person seeking to make such an application or to apply for or to make a modification of that entry.' See sch 1 pt 8 Identity Cards Act.

[38] Name is the most likely piece of information to change as a result of marriage, for example, but s 1(7) pts (a) and (b) Identity Cards Act link the name given to a baby to other names used as a result of marriage, a change by deed poll, or a change through usage.

[39] This point was acknowledged in Parliamentary debate on the Identity Cards Bill 2005, particularly in relation to gender. See, United Kingdom, Parliamentary Debates, House of Lords, 30 January 2006, col 79 (Baroness Scotland of Asthal).

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.[40] Under the NIS, an individual's biographical information- specifically name, gender, date and place of birth and date of death, is linked to a physical individual by the biometrics, photograph and handwritten signature as recorded in the NIR. When this identifying information is combined with the biographical information, collectively it is considered to be unique, so as to single out one identity from a large population.

However, the section 1(7) information does more than just identify. It also acts as the 'key' which opens the lock, so the system can transact with the registered identity. The section 1(7) information represents the registered identity which is connected to an individual by the identifying information, that is, the biometrics, signature and photograph as recorded in the NIR. In effect, that information is the individual's transactional identity under the scheme. The section 1(7) information represents the registered identity and hence the individual to whom it is connected. It is that individual's 'token identity,' that is, his or her transactional identity.

2.4. The Relationship between Token Identity and Database Identity in the United Kingdom

The section 1(7) information is just a token of all the information on record about that identity in the NIR and other databases accessible under the scheme. The full set of recorded

[40] Perhaps the most famous example is the celebrity Oprah Winfrey who was reportedly 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.

information can be conceptualised as the individual's database identity. Database identity includes the subset of information which is token identity.

Recall Fig.1 above which depicts the relationship between the section 1(7) identity information and the other information recorded about an individual in the Register. If this relationship is expressed in terms of identity, it becomes:

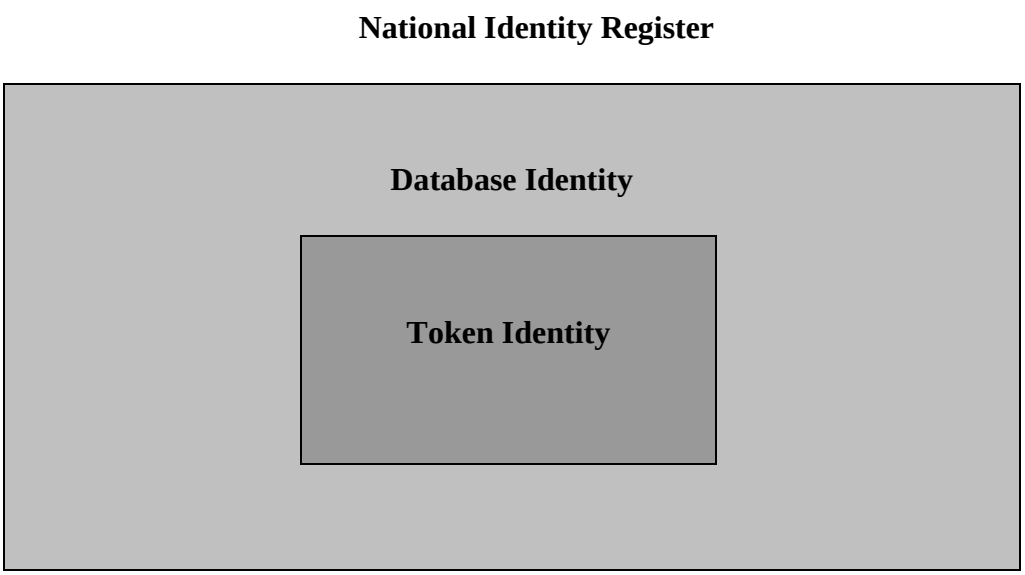

Fig.2.

Database identity has a broader role than the subset of information which constitutes token identity. Some of the information which constitutes database identity (and not token identity) such as a PIN and residential address, may also be used at the time of a transaction and collectively all the information recorded about an individual in the NIR identifies that individual. Like token identity, database identity does more than just identify but its function is different from that of token identity.

Whereas token identity verifies identity for transactional purposes, database identity is the narrative about the registered identity. While token identity singles out an individual so as to authorise dealings with that registered identity, database identity chronicles activities relating to that identity. Unlike token identity, which is relatively static, database identity is dynamic.

The information which is recorded under the scheme and which becomes an individual's database identity, is prescribed by the *Identity Cards Act* and section 3(1) 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.' However, information about an individual's dealings and access to his/her entry in the NIR by the individual and others including public and private sectors using the scheme to verify identity at the time of a transaction, is collected on an on-going basis.[41] This accumulation of information about an individual is an important feature of the scheme and its consequences are explored in the following chapters because as information is updated and new information is collected, it becomes part of database identity. Even information which at first sight seems largely administrative in nature,[42] such as 'Security information' and 'Records of provision of information,' adds to the profile and the impression database identity conveys about the individual linked to that identity.[43] In so doing, database identity tells a story about that individual.[44] It is tempting to think of this information as influencing an individual's reputation and it does, although it is not reputation in the traditional sense of reputation in common law

[41] This facility is typical of this type of system.
[42] See, sch 1. With the possible exception of 'Records of provision of information' in sch 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.
[43] Any errors and inaccuracies, including those resulting from gaps in the personal information recorded and abbreviated data entries, can become 'facts,' even though the information may not be adequately tested for authenticity, or may not be completely up to date and accurate.
[44] This other information includes historical information but database identity is also dynamic and changes as the NIR and other accessible databases are updated.

defamation.[45] The information in the NIR affects how a registered identity and the individual linked to that identity, are regarded by others who have access to the NIR and by the system, which in turn can impact on an individual's ability to transact under the NIS. For example, Schedule 1 provides that an individual's entry in the NIR must include notification under section 10 of the *Identity Cards Act* requiring the individual's attendance to provide information to ensure that the entry is up to date and accurate. Such a notice can trigger the system to prevent transactions until the individual has complied with the notice.[46]

Database identity is necessarily a much broader concept than token identity, although it is limited by the purposes and the architecture of the identity scheme. In the United Kingdom, an individual's database identity comprises all the information as prescribed by the *Identity Cards Act* under Schedule 1. That information is recorded in the NIR in accordance with the *Identity Cards Act* and related legislation[47] which limits the information recorded for the purposes of the scheme.

2.5. Distinguishing Solove's 'Digital Person'

Daniel Solove's 'digital person' is currently the conceptualisation which is closest to my thesis. But database identity is fundamentally different from Solove's 'digital dossiers' which Solove says cover *all* the digital data and information relating to an individual, wherever it is recorded. By contrast, information recorded in the NIR is prescribed by legislation.[48] Solove's

[45] That is, in the sense that if it is published, it brings a person into disrepute in the eyes of other people.
[46] See, s 10 and sch 1 pt 7 *Identity Cards Act*.
[47] The *Identity Cards Act* is enabling legislation. Enactment of further legislation is necessary to fully implement the scheme.
[48] Daniel Solove, *The Digital Person, Technology and Privacy in the Information Age* (2004). Daniel Solove is a Professor at the Law School, George Washington University. Professor Solove has written extensively on digital information and its impact on privacy, especially under US law and is widely regarded as a leading international expert in this field. His work is insightful and is highly influential. Professor Solove's publications which are most relevant to this thesis are: Daniel Solove, 'Identity Theft, Privacy and the Architecture of Vulnerability

views are also driven by his concern about privacy whereas this thesis is about the functions and legal nature of digital identity, and particularly, token identity as an individual's transactional identity. This thesis does not negate Solove's views. Rather, it provides a new perspective, and adds depth by analysing the functions and legal nature of an individual's digital identity, particularly in the context of a national identity scheme.

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.'[49] Bearing in mind that Solove's views are based on privacy under the law of the United States of America ('United States'), not on a legal concept of identity,[50] the relationship between an individual's database identity including token identity under the NIS and information recorded elsewhere about that individual can be depicted diagrammatically:

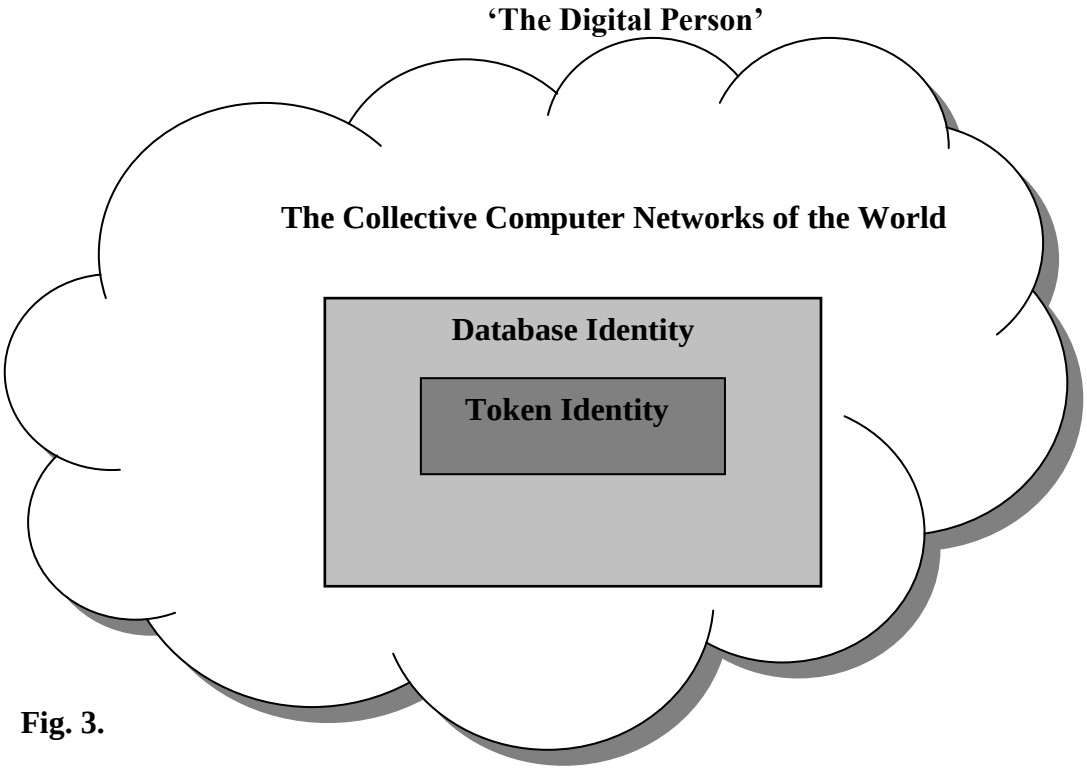

Fig. 3.

(Enforcing Privacy Rights Symposium)' (2003) 54 *Hastings Law Journal*, 1227; Daniel Solove, 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure' (2003) 53 *Duke Law Journal* 967; and Daniel Solove, 'Power and Privacy: Computer Data Bases and Metaphors for Information' (2001) 53 *Stanford Law Review* 1393.

[49] Ibid, 1.

Unlike Solove's 'digital person,' the information which comprises database identity is defined and is limited to the prescribed information which is recorded in the NIR and which is accessible in extant databases in accordance with legislation-principally the *Identity Cards Act* but also in accordance with other legislation such as the *Data Protection Act*. The information which is recorded in the NIR, especially the information which comprises token identity, is authenticated at the time an individual is registered under the NIS and is subject to further updating and checking after registration. It is intended to be accurate, whereas the information 'in the collective computer networks of the world' is recorded at different times and for different purposes, and is therefore likely to contain inaccuracies and inconsistencies which, of course, drives Solove's concerns.

Moreover, while the information stored in a range of disparate government and private sector databases can be thought of as composing Solove's 'digital person,' there are barriers between these databases which limit the extent to which all that information can constitute an individual's identity, especially for transactional purposes. Although the ability to search information from a range of sources is increasing, there are still legal and practical obstacles which prevent all the data and information relating to an individual being accessible and available, even to government. It is difficult to determine exactly what information is being collected, where it is being stored and who owns it, let alone gain access to it.

By contrast, the identity registered under the NIS is the identity which is authenticated and verified by the government of the United Kingdom. It is the identity which is officially registered and recognised in the United Kingdom. This point is significant because

---

[50] Ibid.

information is collected and recorded in the NIR on an on-going basis. Information collected at the time an individual conducts a transaction or when a notation is added to the record as a result of an investigation for example, becomes part of the individual's database identity. That information, as recorded and updated in the NIR, profiles the individual for the purposes of the scheme. When the NIS is fully operational, information from other sources, including those which comprise Solove's digital person, will become less authoritative and less relevant. If, as the government plans, the scheme becomes 'the gold standard,' the identity registered under the scheme will be, in effect, considered the individual's identity for transactional purposes.[51]

The structure of the concept of identity under the NIS is also fundamentally different from Solove's 'digital person.' Database identity under the NIS is *connected* to an individual by token identity, and primarily by the 'identifying information,' that is, the signature, photograph and the biometrics as recorded in the NIR. The other Schedule 1 information which comprises database identity under the NIS is also usually accessed via token identity as recorded in the NIR. The validity of the link between the individual and the other Schedule 1 information which comprises an individual's database identity under the scheme therefore depends on token identity and, in particular, on the rigour of the authentication process on registration, and of the verification process at the time of a transaction. This is an important point which will be considered further, after examining the development of this concept of identity in Australia.

[51] According to the United Kingdom Information Commissioner, the government wants to make the NIS the 'gold standard of identity verification.' See, United Kingdom Information Commissioner, *The Identity Cards Bill–The Information Commissioner's Concerns* (June 2005) <http://www.ico.gov.uk/eventual.html> at 10 May 2006.

2.6. Digital Identity in Australia

The elements of token identity[52] have been evident in State legislation in Australia for some years[53] and recently the elements of database identity have also emerged in federal legislation.[54] The customer identification procedures under the *Anti-Money Laundering/ Counter-Terrorism Financing Act 2006* (Cth) enacted by the federal Parliament in Australia on 12 December 2006, for example, adopt the same two-tier approach[55] although the role of the procedures is still essentially identification, rather than to establish identity in a transactional context.

---

[52] In Australia, 'identity' is mentioned in a wide range of federal and State legislation but is rarely defined and when it is defined, the definition is usually coloured by the nature of the legislation. See, for example, s 4 *Equal Opportunity Act 1995* (Vic) which defines 'gender identity.'

[53] See, the *Law Enforcement and National Security (Assumed Identities) Act 1998* (NSW). 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. S 3 defines 'identity' as '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. The regulations have not prescribed other aspects. At first sight this combination of information may seem unremarkable. Name and address may be dismissed as 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, s 7.1.2 *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.'

[54] Token identity was initially evident, to an extent, in federal legislation in the *Migration Act 1958* (Cth). That Act does not define 'identity,' 'authenticate', 'identify' or '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.' S 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 by 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.'

[55] The first tier, the 'minimum Know Your Customer information,' is the customer's full name, date of birth and residential address. The second tier, the '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. The *Anti-Money Laundering/ Counter-Terrorism Financing Act 2006* (Cth) is part of an international initiative and similar legislation has also been enacted in United Kingdom.

Database identity, including token identity for transactional purposes, first clearly emerged in the Access Card Bill, the proposed framework legislation for the ACS. Although it was shelved in December 2007, the Bill sought to establish a national system of identity registration and proof of identity for Australian citizens and residents, for health and social security transactions.[56] The Access Card, a 'smart' card,[57] was designed to replace a range of cards currently used for government services and benefits,[58] including the Medicare card[59] which is held by most Australian residents.

2.6.1. Identity Authentication and Verification in the Australian Access Card Bill

Although the then Australian Government maintained that the proposed Access Card was not an identity card, the proposal bears a striking resemblance to the controversial Australia Card which was defeated in the Senate in 1987.[60] Indeed, in 2006, the proposed ACS was

---

[56] The then government 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.

[57] The card was to contain a chip. The Bill defines 'chip' to mean 'a microchip or any other device that stores or processes information.' See, cl 29 and cl 5.

[58] The stated purpose of the new registration scheme and the card was to 'streamline and modernize Australia's delivery of health and social service benefits.' See, Explanatory Memorandum Human Services (Enhanced Service Delivery) Bill 2007, 2.

[59] The new chip and PIN card was to 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 would have replaced '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.

[60] Attempts to present it otherwise can be explained by political expediency. The Australia Card proposed in the 1980's was extremely controversial and a national identity card is still a political 'hot potato' in Australia. For a striking comparison of the features of the ACS with the earlier Australia Card scheme and their obvious similarities see, Graham Greenl[60] The stated purpose of the new registration scheme and the card was to 'streamline and modernize Australia's delivery of health and social service benefits.' See, Explanatory Memorandum Human Services (Enhanced Service Delivery) Bill 2007, 2.
eaf, 'Australia's proposed ID Card: Still Quacking like a Duck' (2007*) University of New South Wales Faculty of Law Research Serie*s 1.

acknowledged to be the 'first ever national photographic database of virtually the entire adult population.'[61]

It is clear from the context of the Bill and the Explanatory Memorandum that one of the purposes of the proposed scheme was to identify individuals claiming federal benefits. Although the stated purposes are to 'reduce fraud'[62] and improve efficiency in delivery of health and social services benefits,[63] 'strengthened proof of identity is a fundamental element in the registration process for an access card.'[64] Like the United Kingdom identity card, the proposed Access Card could generally be used by an individual at his or her discretion, to prove identity.[65]

The Access Card Bill is remarkably similar to the United Kingdom Identity Cards Act though the Bill is not generally couched in terms of 'identity'[66] and 'identification.'[67] Although the Bill closely follows the approach of the *Identity Cards Act*, the Bill is clearer and contains more detail about the information to be recorded in the ACR and on the Access Card and scheme operation. As a result, not only is the new concept of identity clearly evident in the Bill, the intended nature and functions of token identity and database identity can be more easily discerned.

---

[61] Minister for Human Services' Consumer and Privacy Taskforce, *Discussion Paper on the Registration Process*, Discussion Paper, 40> http:/www.accesscard.gov.auvarious/Registration%20Paper%FINAL%20 Released %2023%20 March> at 20 March 2006.
[62] 'Fraud' not 'identity fraud' is used. See cl 6 Human Services (Enhanced Service Delivery) Bill 2007.
[63] Explanatory Memorandum, Human Services (Enhanced Service Delivery) Bill 2007,2.
[64] Ibid, 3.
[65] As is the case under the *Identity Cards Act*, the Bill only prohibits a person from *requiring* production of the card. See, cl 45 and cl 46 and s16 *Identity Cards Act*.
[66] See, however, cl 17 Human Services (Enhanced Service Delivery) Bill 2007 which refers to 'a password for authenticating identity' and refers to 'documents used to prove identity.'
[67] However, see, cl l7 and cl 34 Human Services (Enhanced Service Delivery) Bill 2007.

Just as the section 1(7) information is clearly distinguished under the United Kingdom *Identity Cards Act*, the Access Card Bill clearly distinguishes its equivalent – the clause 17 information which comprises the individual's name, date of birth[68], photograph and a digitised copy of the individual's handwritten signature[69] – from the other information recorded in the Access Card Register ('ACR') under clause 30.[70] The relationship between the clause 17 information and the other information in the databases under the ACS can be depicted diagrammatically:

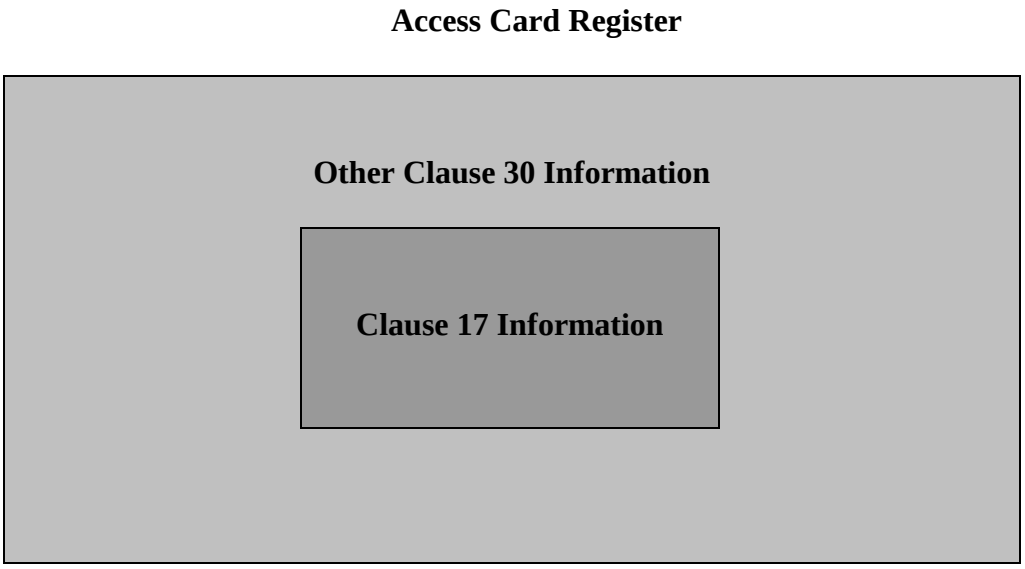

Fig.4.

The clause 17 information was to be obtained from the individual in a registration process which is almost identical with that required under the NIS[71] and it has the same function as the

[68] According to the Explanatory Memorandum, stating date of birth on the surface of the card would be at the individual's discretion. See, Explanatory Memorandum, Human Services (Enhanced Service Delivery) Bill 2007, 30.
[69] Explanatory Memorandum, Human Services (Enhanced Service Delivery) Bill 2007, 34.
[70] Cl 30 Human Services (Enhanced Service Delivery) Bill 2007is the equivalent of sch 1 *Identity Cards Act.*
[71] The major differences are that a facial scan was to be 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' would need to be shown. How this would be shown and checked is unclear, however.

section 1(7) information. Under the proposed scheme, at the time of a transaction, the individual must establish his/her identity by providing the clause 17 information[72] which comprises name and date of birth, photograph and handwritten signature. The information provided is compared to the information to be recorded in the ACR. If it matches, identity is verified. The clause 17 information is an individual's token identity under the Australian scheme. When this relationship between the clause 17 information and the other clause 30 information is conceptualised in terms of identity, a familiar diagram appears:

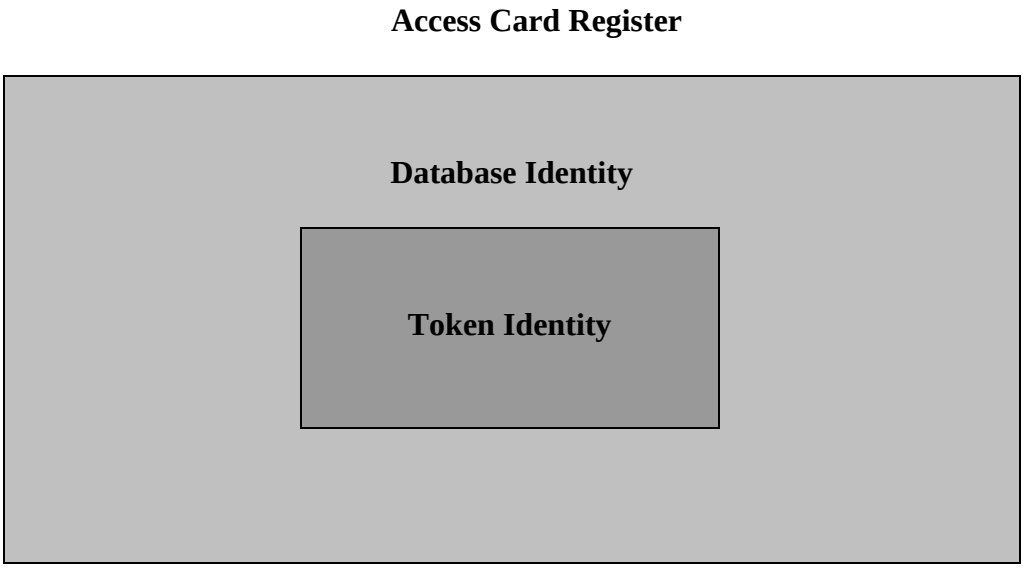

Fig.5.

The information which constitutes token identity for the Australian scheme differs from token identity under the NIS in that it does not include place of birth, gender and date of death[73] and the other biometrics, that is, the fingerprints and iris scans planned for the United Kingdom

---

See, Australian Government, Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, 61.

[72] Usually by presenting the Access Card but like the NIS, the basis of the ACS is registration of the required information, not the Access Card. Strictly speaking, the Access Card was not compulsory.

[73] Under the ACS, however, gender was to be recorded in the chip and in the ACR, while date of death would be recorded in the register.

scheme.[74] 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, that is, name, and date of birth, which are linked to the physical embodiment of the individual, by a handwritten signature and a photograph.[75] More importantly, this set of information has the same function as the section 1(7) information under the NIS in that it verifies identity and enables the system to transact with that identity. As in the NIS, identity is verified when the information constituting token identity, as presented,[76] matches the information recorded in the chip[77] on the Access Card or in the register. As in the United Kingdom, information constitutes identity under the scheme, not the Access Card.[78] The information in the chip on the card is used to verify identity off-line and the register is used to verify identity on-line. 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 for a transaction and a PIN or additional information such as answers to designated questions, may be required for some transactions.

---

[74] While the NIS uses biometrics to verify identity for some transactions, the Australian scheme did not use any biometrics to verify identity for a transaction. Only one biometric, a face scan, was proposed for the ACS. The face scan was to be obtained at the time of registration and stored in the ACR. That scan was to be used to authenticate identity to enable an individual to access his or her entry on the register. See, Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 33 and 36.

[75] Although a face scan was to be done at the time of registration, unlike the NIS, the photo on the surface of the Access Card did not contain biometrics. Biometrics were only to be recorded in the register. See, cl 17 Human Services (Enhanced Service Delivery) Bill 2007. The reason given for this approach is a pragmatic one. The card readers used by service providers (particularly medical, dental and other health services practitioners and pharmacists) for point of sale for credit and debit card transactions, were to be used for the ACS. Use of biometrics for routine identity verification for transactional purposes required upgrading of the card readers which would have added 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.

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

[77] The chip was to have two areas, the Commonwealth area and the Individual's area. Information in the Commonwealth area of the chip was to be used to verify identity. Originally, the latter was to contain next of kin details, organ donor status and medical alerts. The final proposal was that the Commonwealth's area contain 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, gender, PIN or password, information about benefit cards, Medicare number, whether proof of identity is 'full' or 'interim' and an emergency payment number. See, cl 34 Human Services (Enhanced Service Delivery) Bill 2007.

[78]The Access Card Bill did 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, div 2 and cl 42 Human Services (Enhanced Service Delivery) Bill 2007. Card-not-present verification was clearly contemplated. See, Explanatory Memorandum Human Services (Enhanced Service Delivery) Bill 2007, 26 and 42

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 proposed Australian scheme highlights a further refinement to the concept of token identity, that is, the use of the card number to represent token identity.[79] The Access Card number was to be used in telephone and internet dealings to quickly verify 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 for the transaction. The individual is then typically required to verify that information by confirming for example, his or her name and date of birth.

2.6.2. The Relationship between Database Identity and Token Identity in the Australian Access Card Bill

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 ACR. The ACR also contains additional information. Although gender, date of death and place of birth are not part of the information which ostensibly[82] constitutes token identity under the Australian scheme, that information is recorded in the ACR[83] and is therefore part of the individual's database identity under the scheme. Like the additional information recorded in the NIR, the ACR also includes citizenship and residency, as well as information about other cards,[84] information about registration including whether

[79]The number, not the card, was to be used to establish identity at the time of a transaction. A number was also planned for the NIS but this feature has since been downplayed.
[80]Australian Government, Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, 25
[81]Ibid, 32.
[82] When the transaction is in-person gender is usually obvious.
[83] Unlike the NIS, date of death, gender and place of birth were not part of the core identity information under the ACS.
[84] Benefit cards and Medicare number. See, cl 17 Human Services (Enhanced Service Delivery) Bill 2007.

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.[85]

This information identifies an individual and it tells a story about that individual. Like the information which comprises an individual's database identity in the United Kingdom, it is limited by the parameters of the scheme but it can influence how an individual is perceived by other people and by the system. Just as the identity registered under the NIS is the identity which is recorded and recognised by the United Kingdom government, the identity registered under the ACS would have been the identity officially recognised in Australia.

The composition of the concept of identity and its intended functions under the Australian scheme are the same as the concept now evident in the United Kingdom. Database identity is connected to an individual by his or her token identity, primarily by the signature and photograph as recorded on the card and in the ACR which performs the same function as the identifying information under the United Kingdom scheme. Similarly, the validity of the link between the individual and the other information recorded in the ACR which comprises the individual's database identity depends on token identity and particularly on the rigour of the registration process and the verification of identity at the time of a transaction.

2.7. Conclusion

Although arguably a concept of transactional identity has been developing in commercial practice for some years,[86] a legal concept of digital identity has now clearly emerged as a

[85] Presumably this information includes access information.

result of the *Identity Cards Act* in the United Kingdom. A very similar concept is also evident in the Access Card Bill which is likely to be the model for any future Australian national identity scheme.

An individual's digital identity consists of a set of information stored in digital form for the purposes of the particular scheme. This set of information, which is contained in the identity register and other databases accessible under the scheme, is an individual's database identity. Within the set of information which constitutes database identity is a small subset of information which is the individual's token identity. Token identity is the set of information which is presented at the time of a transaction. It is the individual's transactional identity. At the time of a transaction, token identity does not just identify an individual. Token identity singles out an identity from the rest of the population as recorded in the identity register and *then* authorises the system to deal with that registered identity. Token identity is the metaphorical key that opens the lock, so the system can transact with the registered identity.

Database identity is linked to an individual via token identity. In addition to enabling the system to deal with a particular registered identity for transactional purposes, token identity provides the gateway to, and acts as gatekeeper of, database identity. Like token identity, the information which constitutes an individual's database identity can be used to identify him/her but database identity chronicles activities which tell a story about the individual linked to the identity. That narrative can affect the way in which an individual is regarded by other people and by the system.

---

[86] A bundle of information which usually comprises name, account or card number with an expiry date and a handwritten signature, is used for credit and debit card transactions, and for electronic banking, for example.

The information which constitutes database identity and token identity is linked to an individual because that is how it is recorded in the chip on the identity card and/or in the identity register. The basis for establishing and verifying identity is by matching the information which constitutes token identity with that information on record[87] even though matching does not necessarily mean that the information is accurate. These features and their implications for individuals, for entities using the scheme, and for government, are considered in the following chapters.

An individual's identity under the *Identity Cards Act* is a collection of designated information which is given legal status and effect by the *Identity Cards Act* and the NIS. Token identity, in particular, plays a pivotal role especially at the time of a transaction. The legal nature of token identity in that context is examined in the next chapter.

[87] This is true for authentication on registration as well for verification at the time of a transaction because the individual establishes his or her identity by producing documents such as birth certificate, driver's license, credit cards and other government issued cards. The information in these documents is cross checked to see if it matches and where possible, it is checked against the database of the relevant department/agency.

3. Digital Identity – The Nature of the Concept

In the movie 'The Net' Angela Bennett, played by the actress Sandra Bullock, goes to the American Consulate to apply for a temporary visa in order to return to the United States, after her purse containing her passport is stolen while she is on vacation in Mexico. In the Consulate office she is approached by a consular officer holding an application form:

Officer: 'Ruth Marx? Ruth Marx? Excuse me, are you Ruth Marx?'
Angela: 'No.'
Officer: 'You are not the woman who was here about a temporary visa?'
Angela: 'No, I am here about a temporary visa but…'
Officer: 'Is your social security number 915301717?'
Angela: 'Yes.'
Officer: 'Do you live at 407 Finley Avenue, Venice, California?'
Angela: 'Yes.'
Officer: 'Well then. According to the California Department of Motor Vehicles you are Ruth Marx. [88]

3.1. Introduction

This chapter examines the legal function and nature of the new concept of identity in a transactional context. The analysis in chapter 2 reveals the pivotal role played by token identity. This chapter builds on that functional analysis and considers the legal role played by token identity and its legal nature in a transaction, as a prelude to examining the inherent vulnerabilities of the scheme in chapter 4, the individual rights arising as a consequence of the emergent concept of identity which are considered in chapter 5, and the misuse of an individual's token identity information by another person which is examined in chapter 6.

This chapter particularly focuses on the functions of token identity at the time of a transaction, and argues that token identity takes on legal personality at that time. The NIS is used as the basis for the examination. However, while the analysis is based on the *Identity Cards Act* and the United Kingdom scheme, the same issues arise in relation to the ACS because, as

[88] '*The Net'* Columbia Pictures Industries Inc (1995).

discussed in the previous chapter, the Access Card Bill contains the same concept of identity. Indeed, the issues discussed in this chapter apply to any such scheme which uses a concept of transactional identity that consists of a defined set of information which is stored and transmitted in digital format.

3.2. Registered Digital Identity

Considering the stated purposes of the NIS, the digital identity registered under the scheme becomes the identity of the individual to whom it is attributed in the NIR. This is especially so considering the long term objectives of the United Kingdom scheme[89] and that it is founded on the basis of one person: one identity. Token identity as recorded in the NIR determines an individual's ability to be recognised and to transact under the scheme.[90]

Registration brings into existence an officially recognised identity, which consists of token identity, and the other Schedule 1 information, which collectively comprise database identity. As discussed in Chapter 2, this concept of identity is a collection of digitally stored and transmitted information which is given legal effect by the *Identity Cards Act* and by the scheme.

---

[89] See, s 1(4) *Identity Cards Act.* Recall that the *Identity Cards Act* is enabling legislation. Consequently, the Act does not contain all the detail of the operation of the NIS. That detail is contained in the Business Plan and Framework Agreement. See, Identity and Passport Service, *Corporate and Business Plans 2006–2016* <http//:www.identitycards.gov.uk scheme.html> at 10 May 2005 and the Identity and Passport Service, *Framework Agreement*, 14 <http//:www.ips.gov.uk.html> at 10 May 2006. For more recently published information see Identity and Passport Service, *Corporate and Business Plans 2006–2016* <http//:www.ips.gov.uk/identity/publications-corporate.asp> at 1 September 2008; and Identity and Passport Service, *Framework Agreement*, 14 <http//:www.ips.gov./idenity/publications-general.asp.l> at 1 September 2008.

[90] With the individual's consent, the information in the NIR can be used to prove his/her identity as provided in s 1(3) *Identity Cards Act.* See also, s16 *Identity Cards Act* which provides that it is unlawful to make it 'a condition of doing anything in relation to an individual to require the individual' to provide information recorded in the NIR or to establish his/her identity by producing an ID card.

Token identity plays a significant role. Recall that it is the gateway to the information which comprises the remainder of database identity. Token identity also provides the link between an individual and the information which constitutes his or her database identity, through the 'identifying information,' that is, the registered handwritten signature, photograph and biometrics. Most importantly, token identity is the identity which is used for transactions.

3.3. The Role and Nature of Token Identity

The information which comprises token identity is limited. Under the NIS, it comprises name, date and place of birth and date of death, signature, photograph and the biometrics, although not all the token identity information is used for all transactions. What this means is that within that full set of information which constitutes registered token identity, the information used for a particular transaction depends on the nature of the transaction and the requirements of the transacting entity.

Under the NIS, the minimum set of information required for a transaction will invariably consist of name, gender, date and place of birth. In-person transactions will usually also include at least one piece of identifying information which for most routine transactions will be appearance, in comparison with the head and shoulders photograph. Handwritten signature may also be used,[91] with biometrics only being used for major financial transactions.

In comparison with the other information which comprises database identity, token identity is relatively stable. Other than in exceptional cases, such as gender re-assignment and changes required under the witness protection program, the only birth information which is more

commonly subject to change is name, mainly for women in the event of marriage, though also as a consequence of change of name by deed poll. By contrast, the information which makes up database identity is much more extensive, and it is augmented on an on-going basis. Transactions, access to an individual's entry in the NIR, and notification of changes become part of database identity.

Recall that under the scheme, there is a difference between identification and identity. Identification is just one part of the two processes used to establish identity which are firstly, the initial authentication of identity at the time of registration and, secondly, verification of identity which occurs at the time of a transaction. Information collected at the time of registration is used to authenticate identity in the sense that it is used to 'establish the truth of; establish the authorship of; make valid'[92] the identity. Of the information recorded at the time of registration, the signature, photograph[93] and biometrics provide the link to a physical individual.[94] The signature, photograph and biometrics identify an individual under the scheme in that they are regarded as being 'identical with, or as associated inseparably with,' the individual[95] to whom they are attributed in the NIR.

---

[91] Although usually when a signature is necessary on an application form, for example, rather than just as a means of identification for a simple enquiry.

[92] Definition of 'authenticate' in the *Concise Oxford Dictionary*. *The Macquarie Dictionary* similarly defines 'authenticate' as 'to establish as genuine.'

[93] Many transactions will only involve matching the appearance of the person present with the photo, rather than using the face scan which is part of the biometrics used in the scheme. Under the ACS, only a photograph was be used for transactional purposes.

[94] While the NIS will use biometrics to verify identity for some transactions, under the ACS, the biometric (a face scan) was not to be used to verify identity for transactional purposes. The photograph and a digitised copy of the individual's handwritten signature were to be used to verify identity for a transaction. See, Explanatory Memorandum, Human Services (Enhanced Service Delivery) Bill 2007, 34 and Australian Government, Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, 33 and 36.

[95] 'Identify' is defined in the *Concise Oxford Dictionary* as to '[T]reat (thing) as identical *with*; associate oneself inseparably *with* (party, policy, etc); establish identity of.' The *Macquarie Dictionary* defines 'identify' as 'to recognise or establish as being a particular person or thing; attest or prove to be as purported or as asserted.'

Token identity links database identity to an individual, through the 'identifying information,' that is, signature, photograph and biometrics, and is used to access the more extensive information which, with token identity, comprises database identity. The relationship between an individual and database identity, including token identity, can be depicted diagrammatically:

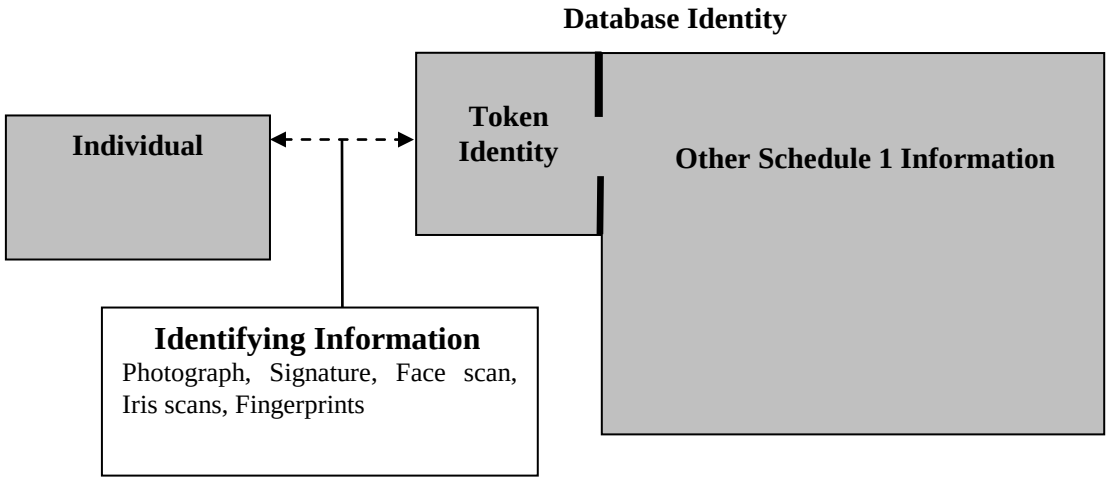

Fig. 6.

At the time of a transaction, identity is verified when all the required token identity information presented, matches the information on record in the NIR,[96] most, if not all, of which is recorded during registration.[97] If the token identity information as presented, match that on record in the NIR,[98] identity is verified under the scheme. Matching as a feature of identity is evident in its general definition. The *Concise Oxford Dictionary* defines 'identity'

---

[96] 'Verify' as used in the United Kingdom scheme and the ACS, accords with the definition in the *Concise Oxford Dictionary*: '[e]stablsh the truth or correctness of by examination or demonstration…'although under both schemes truth is really a *presumption* of truth. The *Macquarie Dictionary* defines verify as 'to prove something to be true, as by evidence or testimony, confirm or substantiate' and 'to ascertain the truth or correctness of espc. by examination or comparison.'

[97] Although all the token identity information is recorded at the time of registration, there may be subsequent changes as a result of a change of name following marriage, for example.

[98] And where applicable, on the identity card although it is the matching of the token identity information presented with that on record that is necessary.

as 'absolute sameness.'[99] Under the NIS, however, the matching is not with a human being. As discussed in Chapter 2, identity is verified by matching the information which is presented at the time of a transaction, with information recorded in the register. When presented at the time of a transaction, token identity is a token, that is a 'sign, symbol, evidence …serving as proof of authenticity'[100] of identity under the scheme.

Through this matching process, token identity performs a number of vital, sequential functions at the time of a transaction. First, token identity identifies, by singling out *one* identity from all the identities registered under the scheme. The photograph, signature and biometrics are used to identify the individual, though depending on the nature of the transaction and the requirements of the transacting entity, not all the identifying information need be used.[101] Secondly, token identity verifies identity by determining whether there is a match between all the token identity information presented, with that on record. These two steps enable the system to recognise and then transact with the registered identity.

The role and legal significance of token identity will inevitably exceed the original intentions and objectives of the government in establishing the scheme. The intention was that dealings be with the individual who is presumed to be correctly represented by the token identity information and who is presumed to present that token identity at the time of the transaction. On this view, the transaction is via the registered identity, but is with the individual:

---

[99] The definition also adds 'individuality, personality,' aspects which are also examined in a legal context later in this chapter. The *Macquarie Dictionary* defines identity as 'the state or fact of being the same one, as under varying aspects or conditions' and 'the condition of being oneself or itself and not another...'

[100] This is the definition of 'token' in the *Concise Oxford Dictionary*. The *Macquarie Dictionary* defines 'token' as 'something serving to represent or indicate some fact…something used to indicate authenticity, authority…'

[101] This is especially so for transactions conducted remotely using telephone or the internet. Bear in mind that not all transactions will use all the identifying information. Routine transactions only require that appearance match the photo or that the signature matches, for example.

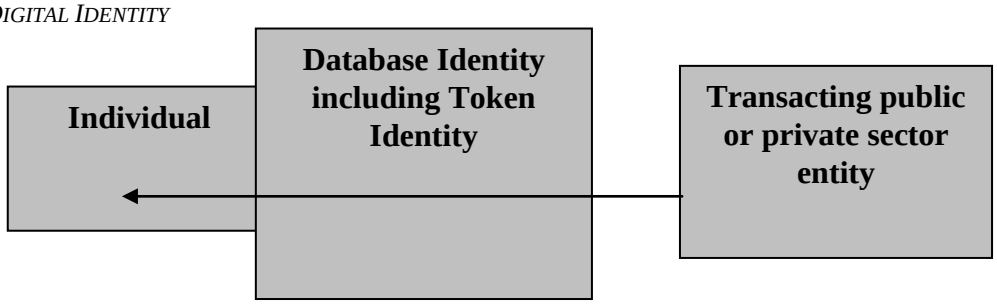

Fig.7.

Although it is not clear, the information which constitutes token identity was probably intended to be just a credential, to be presented by an individual as part of the identification process in much the same way as a passport is used, for example.[102] However, there are crucial differences between the function of a traditional identity document like a passport and token identity.

A passport, for example, has traditionally been, and still is, used to support claimed identity. Although the identification function of token identity may seek to replicate this function, there are two important distinctions. First, identity papers, like a passport for example, are presented in-person. A human being is not only present but central to the identification process. Secondly, although apparently valid identity papers are needed to support an officer's decision, that decision requires judgment, based on a number of factors including first-hand observation of the individual.[103] Any authorisation given by an officer is based on his or her judgment and, to an extent, his or her discretion.[104]

---

[102] See, Explanatory Notes, Identity Cards Act 2006 (UK), 9 <http//:www.opsi.gov.uk.html> at 19 May 2006.
[103] Including responses to additional questions, if necessary.
[104] There is also a further point of difference. Token identity is used for a wide range of transactions including commercial transactions. Identity papers were usually used for more limited purposes such as mobility for example, specifically to enable access to defined geographical areas and in the case of a passport, to afford safe passage. The safe passage request in the Australian passport, for example is to 'allow the bearer, an Australian Citizen, to pass freely without let or hindrance and to afford him or her every assistance and protection of which he or she may stand in need.'

Unlike an identity document like a passport, the information which comprises token identity plays the critical role in the transaction, not the individual who presents the token identity information, or who is presumed to present it, in the case of transactions which are not in-person.[105] The system looks for a match between the information presented and the information on record. Most significantly, token identity does not just identify an individual. It enables the system to transact – with the registered identity. Regardless of whether the token identity information is presented in-person or remotely, if all the token identity information presented at the time of the transaction matches the information recorded in the NIR, then the system automatically authorises dealings with that identity. Within these parameters the system can, to use David Derham's words, 'act and will for itself'[106] to recognise the defined set of information which comprises token identity and then to transact with the registered identity.

The individual who is assumed to be represented by that registered identity is connected to token identity by the signature, appearance (through the photograph) and biometrics as recorded in the NIR, but is not essential to the transaction. The individual's connection to the identifying information is contingent. Token identity can be separated from that individual and it is possible for token identity to function independently.[107] The system and the transacting entity deals with the registered identity via token identity, not with the individual represented by the token identity:

---

[105] The information may be presented remotely and even automatically using computer programming, without any active involvement by an individual *at the time of a transaction*, though of course some human involvement is required at some stage.

[106] David Derham, 'Theories of Legal Personality' in Leicester Webb (ed) *Legal Personality and Political Pluralism*, (1958) 1, 14.

[107] This is especially so if, for example, the transaction does not require biometrics. Of course, at some stage a person has to arrange for it to be presented for a transaction but that does not alter the fact that token identity can operate independently at the time of a transaction.

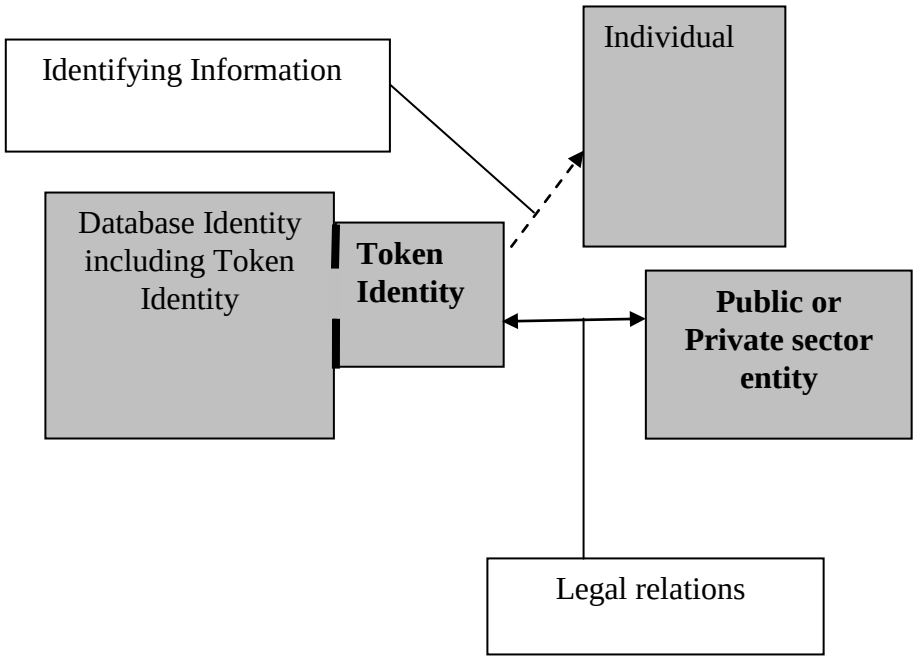

Fig. 8.

Although the intention may have been to 'reach behind' token identity to deal with the individual presenting it, the system does not actually operate in that way. If the token identity data/information presented at the time of a transaction matches the record in the NIR, the system will recognise the identity.[108] More significantly, the system will not recognise, nor deal with, the individual presenting that token identity,[109] even if the token identity is otherwise legitimate and authentic. No doubt procedures will be established for dealing with situations in which the system, through an apparent malfunction, does not recognise what seems to be a legitimate registered identity, and to deal with people who for a variety of

[108] There are other examples of this type of automation. Richard Fox has written about the impact of 'high technology' in relation to automated infringement notices for traffic offences. Although that technology is not as far reaching in its application as the technology which applies to transactions in the context of a national identity scheme, Fox's observations are apt and analogy can be drawn to the way token identity works at the time of a transaction. In discussing the automated infringement notice system which is linked to vehicle registration, Fox states that '[t]he pursuit of efficiency has resulted in greater reliance on concepts of vicarious and strict liability. This means that the person who receives the infringement or penalty notice might not be the actual offender (i.e. the owner rather than the driver of the car), or may not be particularly culpable.' See, Richard Fox, Infringement Notices: Time for Reform, *No 50 Trends and Issues in Crime and Criminal Justice* (1995), 2.

[109] The authenticity of a registered identity is clearly presumed, primarily on the basis that biometrics are reliable identifiers, and on the overall integrity of the scheme. There is obviously a presumption that the initial registration process is sufficiently robust to ensure authenticity and that subsequent use of the token identity is by the individual to whom it is attributed in the NIR.

reasons are not registered.[110] However, this does not change the transactional role of token identity. It demonstrates its significance. If an individual's token identity is not recognized by the system, any protocol designed to deal with that contingency must authorise dealings with the individual in-person, not with the token identity.

The automatic authorisation to transact which occurs when the presented token identity information matches that on record in the NIR raises questions about the legal nature of database identity, and particularly the legal nature of token identity. The central question is who, or what, is the legal person[111] in the transaction, that is, who or what enters into legal relations? Is it the individual who is connected to the identity in the NIR, primarily by the identifying information and particularly by his or her biometrics, or is it the individual who presents the token identity at the time of the transaction? Although it is intended that it be the same person, it may not be. There is also another intriguing option: that token identity itself is the legal person. While this view is controversial because it invests token identity with legal personality, it is a view which sits easily with the functional role of token identity under the scheme.

3.4. Is Token Identity the Legal Person?

Who, or what, is a person in law, is the subject of vigorous intellectual debate. Central to this debate is whether the legal person must 'approximate a metaphysical person,' to use Ngaire

[110] Especially considering that the scheme will be used for government social security benefits, these procedures will require a delicate balance between equity and security concerns, with the balance likely to tip in favour of security, particularly given heightened terrorism concerns.
[111] The 'legal person' is the entity which bears legal rights and duties and so possesses legal personality.

Naffine's words.[112] Naffine usefully summarises the three main understandings of legal persons which she calls P1, P2 and P3, respectively.[113]

As Naffine explains, P1 is the orthodox positivist view. Personality arises from rights and duties, rather than from intrinsic humanity.[114] In the words of Alexander Nekam, '[e]verything… can be the subject-a potential carrier–of rights.'[115] 'There is nothing in the notion of the subject of rights which in itself would necessarily connect it with human personality, or even with anything experimentally existing.'[116] Once a legal right is in evidence, so is a (legal) person.[117] According to Derham, 'it follows of course, that any 'thing' which is treated by the appropriate legal system as capable of entering legal relationships 'is' a legal person, whether it can act and will for itself or must be represented by some designated human being(s)'[118] In other words, a 'thing' can be transformed into a legal person through the

---

[112] Ngaire Naffine, 'Who are Law's Persons? From Cheshire Cats to Responsible Subjects' (2003) May *Modern Law Review*, 346.
[113] Ibid, 350.
[114] In Nekam's words, '[t]he rights themselves are given not for human personality or will but for the interests which the law-maker wants to protect. It is the socially protected interests which in legal abstraction we call rights. Since any conceivable interest attributed to any conceivable entity may be regarded as socially important by some community, anything may become a subject of rights–anything existing or anything to which the lawmaking community attaches any existence at all; and human personality or will is by no means a preliminary condition to its formation.' See, Alexander Nekam, *The Personality Conception of the Legal Entity* (1938), 27.
[115] Ibid, 26. See also, Derham, above n 106, 13-15.
[116] Ibid, 26 and 28. Nekam also asserts that the proposition that every individual is a natural subject of rights by virtue of his or her humanity is flawed. However, as Nekam asserts, a connection between a right and a human being is inevitable. Nekam distinguishes the subject of the right from its administrator. While it is inevitable that the administrator of the right be human, the subject of the right need not be human.
[117] Margaret Davies and Ngaire Naffine, '*Are Persons Property? Legal Debates Debates About Property and Personality*' (2001), 54.
[118] Derham, above n 106, 13-15. Derham asserts that 'the wrong questions have been asked in the process of resolving many problems concerning legal personality.' He suggests that the appropriate questions are:
'*Is there personateness*? (a)Do the rules of the legal system establish that this entity…is to be recognised as an entity for the purposes of legal reasoning (i.e. to have the capacity to enter into legal relations)?
What is the personality? (b) If so, do the rules of the legal system establish just what kinds of legal relations this entity may enter, or more commonly, do those rules establish whether or not this entity may enter the legal relation claimed or denied on its behalf?
Should there be personateness? (c) If the rules of law in (a) above are silent or ambiguous, should this entity be recognised as an entity for the purposes of legal reasoning?
What kind of personality should there be? (d) If either the rules of law in (a) or (b) above are silent or ambiguous and if (c), being relevant, is answered in the affirmative, then should the entity be recognized as having a personality which includes the capacity claimed or denied on its behalf to enter the legal relation concerned ?'

legal endowment of rights and duties. The legal recognition of rights and duties can also bring something into existence.[119]

By contrast, P2 theorists maintain that humanity is absolutely necessary for true legal personhood. The abstract, artificial nature of P1 troubles P2 legal theorists who regard the human being as 'the paradigmatic subject of rights'[120] which begin at birth and cease on death. The rationale for the P2 view is that 'a human does not have to be sentient to be a (legal) person; his moral and hence legal status comes from being human' (my addition).[121] This view of the legal person is the basis for fundamental human rights, including the right to privacy and the right to identity, and now the emergent right to token identity, which is discussed in chapter 5, but it does not fit as well as P1 with the transactional role of token identity under the scheme.

Token identity is even further removed from P3. P3 theorists insist that the legal person must be human and further assert that the human being must be legally competent.[122] P3 theorists 'maintain that those who lack the will personally to enforce their own rights cannot be truly said to possess those rights and so, it follows that they cannot properly be regarded as legal persons.'[123] Richard Mohr takes this argument one step further to include judgment and responsibility.[124] Mohr asserts that '[t]he legal subject must be capable of acting and of

---

[119] The corporation is an example.
[120] P.Ducor, 'The Legal Status of Human Materials' (1996) 44 *Drake Law Review* 195, 200 cited by Naffine, above n 112, 358.
[121] Naffine, above n 112.
[122] As Naffine points out, this concept of the legal person as a moral agent is particularly evident in criminal jurisprudence. Naffine, above n 112, 362.
[123] Naffine, above n 112, 363.
[124] Richard Mohr, 'Identity Crisis: Judgment and the Hollow legal Subject,' (2007) 11 *Passages – Law, Aesthetics, Politics*, 106.

judging actions, must be prudent for the future and responsible for the past. He or she must have experience and must learn from it.'[125]

Neither P2 nor P3 are necessary to the effective functioning of token identity. Token identity is indeed abstract and artificial, and is a nice illustration of Naffine's P1. While a human being is linked to the registered identity, and specifically to token identity, through signature, appearance (photograph) and biometrics, the transactional functions of token identity under the scheme are not necessarily dependent on humanity, nor on a legally competent, rational human actor. While many transactions will be in-person, and depending on the type of transaction, will include comparison of appearance with a photograph, a signature and/or matching a biometric, the scheme clearly envisages remote transactions where these links with a physical person are either not required or are provided on-line, not in-person. Rationality and legal competency are also not part of the information which collectively comprises token identity. Rationality and legal competency do not affect the functions of token identity under the scheme, except perhaps in the case of individuals who are minors (which is obvious from the date of birth) and those who are flagged by system as not being competent. As Naffine observes,

> P1 has neither biological nor psychological predicates; nor does it refer back to any social or moral idea of a person and it is to be completely distinguished from those philosophical conceptions of the person which emphasise the importance of reason.…The endowment of even one right or duty would entail recognition of their ability to enter into legal relations and so be a person, even though a human would necessarily be required to enforce any right.[126]

---

[125] Ibid, 118.

[126] Naffine, above n 112, 351. Nekam also maintains that 'everything… can be the subject-potential carrier-of rights.' 'There is nothing in the notion of the subject of rights which in itself, would necessarily, connect it with human personality, or even with anything experimentally existing.' In other words, legal personality arises from rights and duties, rather than from inherent humanity. Nekam, above n 116, 26.

On this P1 view, the legal person should not be confused with flesh and blood people**.** As F. H. Lawson explains, '[a]ll that is necessary for the existence of the person is that the lawmaker… should decide to treat it as the subject of rights or other legal relations.'[127]

Unlike other notions of the legal person, that is, P2 and P3, the potentially expansive and inclusive nature of P1 also accords with the enduring nature of identity. Identity, unlike privacy for example, does not necessarily cease on death[128] though of course death affects the way in which rights and duties are enforced.

3.5. Token Identity is the Legal Person

In many ways, P1 fits the concept of token identity now established under the legislation and the actual functions of token identity under the scheme. Indeed, token identity is a relatively pure example of P1. Although date and place of birth, date of death, gender, appearance, signature and biometrics are part of token identity information, token identity need not be coloured by what Naffine refers to as 'metaphysical notions of what it means to be a person.'[129] Although there is a notional connection with a human being, it is the information which plays the crucial role in the transaction, not the individual to whom it is presumed to relate.

Token identity 'exists only as an abstract capacity to function in law, a capacity which is endowed by law because it is convenient for law to have such a creation.'[130] Although the lawmaker may not have made a conscious decision to create token identity, let alone endow it

---

[127] F.H. Lawson, 'The Creative Use of Legal Concepts' (1957) 32 *New York University Law Review*, 909, 915.
[128] Under the NIS, token identity includes date of death as well as date of birth. See, s 1(7)(d) *Identity Cards Act.*
[129] Although Nafffine notes that 'P1 is not immune from metaphysical notions of what it is to be a person.' Naffine, above n 112, 356.

with legal personality, the legislation has crystallised the concept and through the operation of the scheme, it has been endowed with legal personality.[131]

Recall the 'key' analogy used in chapter 2 of this thesis and that verification of identity involves two steps. First, the token identity information is presented to establish identity,[132] like a key being used to open a lock. In the second step, the presented information is compared with that on record in the chip on the ID card and/or on-line in the NIR, to see if it matches. If the information matches, then the indentations on the 'key' align with the indentations in the 'lock' to open the 'door,' to enable the system to transact with that registered identity.

Richard Tur's description of personality as 'an empty slot'[133] that can be endowed with legal capacity resonates with this role of token identity under the NIS. When the required token identity is presented, it is inserted into the 'lock' – or slot, to use Tur's metaphor. The 'lock' remains empty and non functional until the matching 'key' is inserted. At the moment the presented token identity matches the token identity recorded in the NIR, the empty slot is filled and the token identity is endowed with legal capacity.

On this view, legal relations are between the registered identity through token identity, and the transacting public or private sector entity. Transactional rights and duties initially attach to token identity and then to the registered identity, not necessarily to the individual (who is

---

[130] Naffine, above n 112, 51.

[131] Such an endowment is not unusual. There is a strong similarity between token identity being endowed with legal personality and a corporation being regarded as a separate legal entity and having legal personality, for example.

[132] 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.

[133] Tur, Richard 'The 'Person' in Law' in Arthur Peacocke and Grant. Gillett (eds), (1987) *Persons and Personality: A Contemporary Inquiry* 116, 121. Tur maintains that 'the empty slot can be filled with anything that can have rights and duties.'

associated with that registered identity as recorded in the NIR), nor to the individual who presents the token identity:

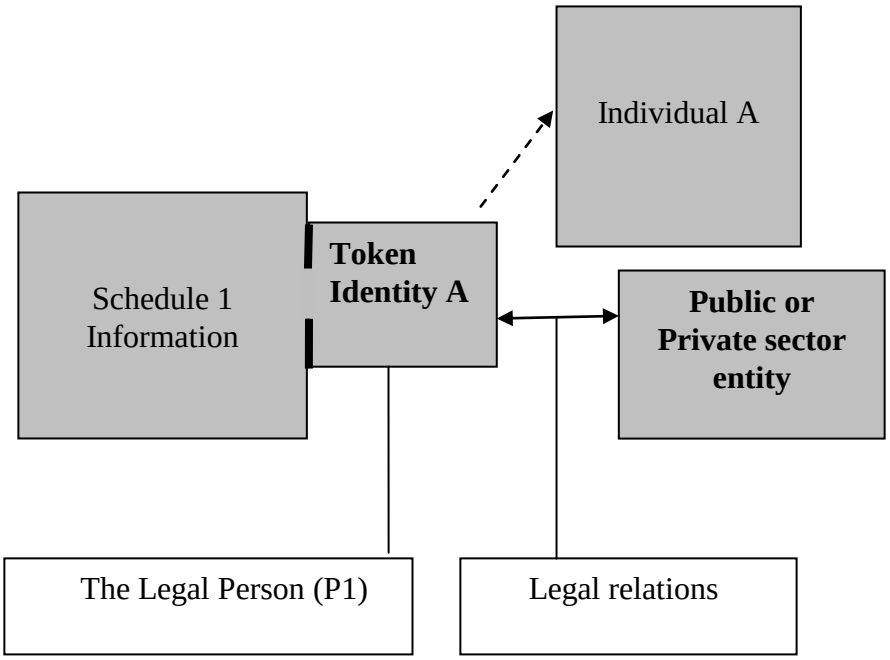

Fig.9.

In the context of the NIS, the most likely misuse scenario is that person B fraudulently uses individual A's token identity when dealing with a public or private entity. In this situation the contract is with registered identity A. If, there is subsequent default, the public or private sector transacting entity will, as a matter of practicality, first look to the registered identity:

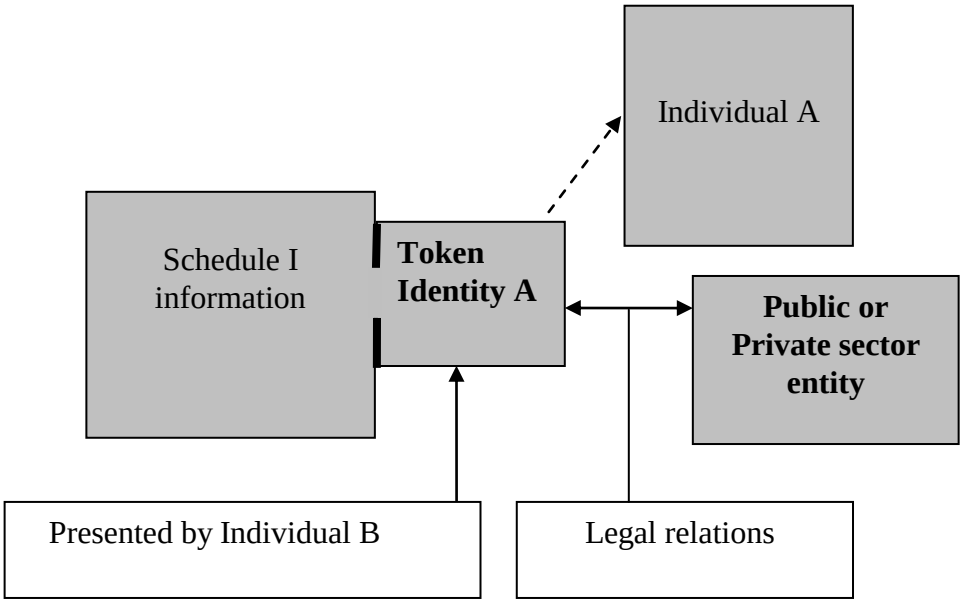

Fig.10.

This situation raises questions about the applicability of the line of English contract cases on mistaken identity when the transaction uses token identity. Those cases, which are still law in both the United Kingdom and Australia,[134] have been described as impossible to reconcile.[135] However, although reconciliation is difficult, it is not impossible. The cases turn on the intention of the contracting parties and the particular circumstances, including the nature and seriousness of the mistake, especially the consequences for a subsequent purchaser for value without notice of the fraud. While the consequences for an innocent purchaser is the general justification for the courts' approach in finding the contract voidable, there is a strong theme in the decisions that the law will presume that in face to face dealings each party intends to deal with the person who is physically present. That presumption can, however, be rebutted by clear, admissible evidence to the contrary.

---

[134] The leading cases on this point are *Ingram v Little* (1961) 1 QB 31, *Lewis v Avery* (1972) 1 QB 198 and *Cundy v Lindsay* (1878) 3 App Cas 459. See also *Phillips v Brooks Ltd* (1919) 2 KB 243 and *Shogun Finance Ltd v Hudson* (2004) 1 AC 919. In Australia, see also *Porter v Latec Finance (Qld) Pty Ltd* (1964) 111CLR 177 and *Papas v Bianca Investments Pty Ltd* (2002) 82 SASR 581.

[135] J W Carter, Elisabeth Peden, and G J Tolhurst, *Contract Law in Australia*, (5th ed, 2007), 459.

The NIS and token identity transform the way in which transactions are conducted, rendering that presumption obsolete. Unlike the parties in the line of mistaken identity cases, the public or private sector entity deals with token identity, not with an individual. This is so for all transactions which use token identity, but it is most clearly illustrated in remote transactions where the required token identity information is presented by telephone or using the internet. The token identity information is automatically compared to the information as recorded in the NIR. If it matches, the system deals with the registered identity. Information and advice is provided to that identity. Invitations to treat and contracts are made with that identity–an identity which is composed of digitally stored information, which is accorded authenticity and given legal personality by the scheme.

Of course, there are ramifications, especially for the individual whose token identity is misused. If A's token identity is dishonestly used by B, it may be difficult for A to establish that he or she did not present his or her token identity for the transaction. There is no indication that the identifying information actually presented at the time of a transaction will be recorded for future comparison. Consequently, an individual may only be able to prove that he or she did not present his or her token identity by establishing that it was impossible to have done so.[136] Specific rules may be needed to deal with this situation but the important point is that there is a contract with the registered identity, although it is voidable for fraud.

---

[136] As would be the case, for example, if it can be established that the token identity was presented in-person at location X when the individual was in location Y at the time and could not possibility have used the token identity for the transaction. However, if the transaction is conducted remotely the individual is likely to find it extremely difficult to establish that he or she did not use his or her token identity for that dealing.

3.6. Conclusion

It is a departure from the familiar to assert that there is an emergent legal concept of identity and hence of the person, which is comprised purely of a set of information (let alone to assert that it is endowed with legal personality). But to many, P1 is controversial because of it's abstract, artificial nature and its implicit denial that the human being forms the natural subject of rights.[137] Any assertion that token identity is invested with legal personality of this sort is therefore also likely to be controversial. However, when viewed from the perspective of other disciplines such as computer science, the notion that information has function as well as meaning is well established, as is machine intelligence whereby computers can make decisions and, indeed, act much like a human being.

No doubt a court will strive to find a human being behind the registered identity who can be considered the legal person in the transaction and in many ways it is appealing to follow the P2 theorists who look for a human subject. It is the approach adopted in the mistaken identity contract cases, for example, but much has changed about how transactions are conducted since those cases were decided. Computer technology, and in particular digital technology, is now an integral part of commerce and of transactions, particularly those of a routine nature. Most significantly, it is not the way the NIS actually works.

Under the NIS, the system recognises token identity and transacts with the registered identity, not with the individual who is associated with that identity or who presents it. Even when aspects of identity are discussed and clarified with a human being in-person, by telephone or using the internet, the details are entered in the system against the registered identity. Of course, there is nothing especially new in this method. It is widely used for consumer

transactions. What sets the scheme apart is that it is the official, national identity scheme of the United Kingdom. The scheme's size and particularly, its nature, means that to ensure system security, there is, and there must necessarily be, less power given to human operators to override the scheme's automated processes. Information, particularly digital information, plays the critical role, not human beings. Although courts have traditionally resisted recognition of machine intelligence,[138] usually to prevent an obvious miscarriage of justice, this approach ignores the fact that computers are performing intelligent functions and making decisions which often cannot be readily overridden by human operators.

Under the scheme, token identity determines a person's right to be recognised as an individual and to transact. If the scheme is sufficiently robust to ensure the integrity of identity authentication at the time of registration and the unfailing accuracy of identity verification at the time of each transaction, then it is of little practical significance whether a court accepts the argument that token identity is the legal person or whether the P2 approach would be followed. A human being must still be involved, albeit as the administrator of the rights and duties attaching to P1, and the individual to whom the identity is attributed in the NIR is the most obvious administrator. That individual is also presumed to present the token identity at the time of a transaction. This assumes the authenticity of the registered identity, particularly token identity. However, if there is a possibility of system error, or fraud (which is at least a possibility because no system is infallible),[139] so that accuracy and integrity of authentication, and/or verification of identity under the scheme is compromised, the practical and legal issues become much more complex and problematic.

---

[137] However, it is certainly not unknown in the law. A corporation, for example, is similarly abstract and artificial.
[138] See, *Davies v Flackett* (1972) Crim L R 708 and *Kennison v Daire* (1985) 38 SASR 404, 416 (O'Loughlin J). See also, *Kennison v Daire* (1986) 160 CLR 129.
[139] Indeed, the United Kingdom Information Commissioner has warned that '[t]he potential for mistakes and errors being introduced during the processing of applications or the maintenance of the scheme should not be

Most significantly, the argument that token identity is invested with legal personality reverses the presumption in the cases of mistaken identity that the contract is with the fraudster rather than with the person impersonated. The impact of token identity therefore has broad ramifications for commercial dealings but individuals face the most immediate and significant consequences.

As discussed in this chapter, under a scheme like the NIS, the individual linked to the token identity as recorded in the NIR is regarded as having entered into the contract. The consequences for that individual may mean that in future special rules will need to be developed so that that individual is not held accountable if his or her token identity is misused by another person. However, this situation highlights the immediate need for the recognition and protection by the State, of the right of an individual to an accurate, functional, unique token identity and to its exclusive use. This right to identity and other consequential rights are considered in chapter 5 and the role of the criminal law in protecting an individual's right to identity is examined in chapter 6. Criminal sanctions have a major role because the misuse is usually with criminal intent but also because at present there is no clear common law action available to an individual in these circumstances.

As a prelude to that discussion and to add practical perspective to the issues explored in this chapter, chapter 4 considers the vulnerabilities inherent in a national identity scheme like the NIS.

---

underestimated.' Information Commissioner, '*Entitlement Cards and Identity Fraud. The Information Commissioner's Response to the Government's Consultation Paper*, 30 January 2003, 4.

4. Digital Identity – Inherent Vulnerabilities

In the movie 'The Net' Angela Bennett played by the actress Sandra Bullock returns to her hotel in Mexico after being hospitalised for several days following an incident in which her purse, containing her passport and credit cards, was stolen. She goes to the Registration Desk to pick up the key to her room.

Angela: 'I need my room key for 206 please.'
The Registration Desk Clerk replies: 'What was the name?'
Angela: 'Angela Bennett.'
The clerk checks the hotel computer and replies: 'No, I am sorry, Angela Bennett checked out last Saturday.'
Angela: 'No, sorry, you don't understand. I am Angela Bennett. I am standing right here. I didn't check out.'
Clerk: 'I am sorry, its not on the computer. Let me check my records.'
Clerk: (*The clerk scrolling through information on the computer screen*) *'No. Angela Bennett, she checked out last Saturday.'*
Angela: 'No, I didn't check out. I would know if I checked out. I didn't check out.'
Clerk: 'According to the computer you checked out. There is nothing I can do for you, ok. I am sorry.'[140]

4.1. Introduction

In an environment in which transactions are not based on personal relationships, an individual's identity must be established by providing information which is verified by comparing it to a referent standard. Under a national identity scheme like the NIS, the referent standard is the NIR, the official identity database.

While the scheme purports to verify identity by connecting it to a person, identity is really verified by matching digital information to digital information.[141] As discussed in chapters 2 and 3, the information recorded in the identity register is matched with the information presented at the time of a transaction. The accuracy of the match and hence the connection between an individual and the registered identity, depends on the rigour and integrity of the

[140] '*The Net'* Columbia Pictures Industries Inc (1995).
[141] This is the case for all the token identity information but when an individual's appearance (as distinguished from a face scan) and handwritten signature is compared with the photograph and/or signature as recorded in the NIR in the case of face to face transactions, a person makes the comparison.

initial registration process, the assumption that the identifying information as recorded remains unchanged, and the rigour and integrity of the verification process at the time of each transaction.

This chapter addresses the specific claims by the IPS as to the operation of NIS, as a prelude to developing the argument that individual rights arise in relation to the emergent concept of identity and the obligation of the State to protect those rights as discussed in chapters 5 and 6. The purpose of this discussion is to provide some background and perspective, not to present a comprehensive scientific or technical dissertation or analysis.

The discussion in this chapter focuses on the use of a photograph and fingerprints because it now appears that the NIS will use only a photograph and fingerprints and that plans for face and iris scans have been abandoned, at present.[142] The chapter outlines the main areas for concern in relation to the NIS, provides some well documented examples of how error can occur, especially in the use of photographs and fingerprints for identification, and highlights the possible repercussions in the context of a scheme like the NIS.

As the discussion in this chapter reveals, although there is reliance on the identifying information to verify identity, none of the identifying information and processes used in the NIS, particularly the use of photograph identification and fingerprint matching, is foolproof. The consequences for an individual are potentially serious, especially considering the security and law enforcement purposes which are typical of a national identity scheme like the NIS. The potential consequences for individuals highlight the importance of establishing a national identity scheme within a regime which recognises and protects basic human rights as

[142] Above, n 22. It now appears that only a photograph, not a face scan, and fingerprints will be used.

discussed in chapter 5. An established human rights regime now exists in the United Kingdom as a consequence of the country's membership of the European community but that type of national regime does not exist in Australia.

This chapter highlights the inherent vulnerabilities of a scheme which depends on comparison of information to verify identity, to illustrate the need for individual rights to be acknowledged and protected. This discussion adds perspective to the preceding discussion of token identity as the legal person in a transaction in chapter 3 and sets the scene for examination in chapter 5 of the individual rights, including the right to token identity, which this thesis argues arise in the context of the NIS as a consequence of the emergent concept of identity.

4.2. The Fallibilities of the Identifying Information

The NIS uses a photograph and a handwritten signature as identifying information but the foundation of the NIS in authenticating and subsequently in verifying identity, is the use of biometrics which under the scheme are fingerprints and as originally proposed, a face scan and iris scans. [143] However, biometrics will only be used for major transactions, usually financial transactions. Routine transactions under the NIS will compare the photograph on record in the NIR (and on the ID card) to the individual.

[143] The proposed ACS also used a photograph and handwritten signature to verify identity but unlike the NIS, biometrics were not used to be used verify identity for transactions.

In the example on the IPS website, at the time of a transaction the check is done by a person who compares the photograph on the ID card with the individual presenting it.[144] Unless the person carrying out the check knows the individual, the matching process is prone to error. According to Michael Bromby and Haley Ness, the most significant factor in accurate identification by a human being is familiarity:

> Recognising familiar faces is a fairly robust process. We can easily recognise people we know in different contexts and view. However, for a previously unfamiliar face 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.[145]

It appears that 'recognition of unfamiliar faces depends on matching or recognising superficial details of the image–picture recognition.[146] In a study in which supermarket cashiers compared real people not known to them to photographs on the credit cards they presented, only 50 percent accurately accepted or rejected the cards. When the card contained a photograph resembling the person presenting it, only 36 percent of the cashiers correctly rejected the card.[147]

---

[144] Identity and Passport Service, *Using the Scheme in Daily Life, Transferring Money*, <http//:/www.identity cards.gov.uk/scheme.html> at 10 May 2006. For the current examples see, Identity and Passport Service, *Using the Scheme in Daily Life* <http://www.ips.gov.uk/identity/how-idcard-daily-providing.asp> at 1 September 2008.

[145] 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> at 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. 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.

[146] Ibid, Michael Bromby and Haley Ness, 7 citing Peter Hancock, Vicki Bruce and A Mike Burton 'Recognition of Unfamiliar Faces' (2000) 4(9) *Trends in Cognitive Science* 330. See also, Jose Kersholt, Jeron Raaijmakers and Mathieu Valeton, 'The Effect of Expectation on the Identification of Known and Unknown Persons' (1992) 6 *Applied Cognitive Psychology* 173. For a more recent article in this area see Sarah Stevenage and John Spreadbury, 'Haven't we Met Before? The Effect of Facial Familiarity on Repetition Priming' (2006) 97(1) *British Journal of Psychology* 79. Research also shows that individuals are better at recognising and discriminating own- race versus other- race faces. For a recent article on this topic see Pamela Walker and Miles Hewstone, 'A Perceptual Discrimination Investigation of the Own-Race Effect and Intergroup Experience'(2006) 20(4) *Applied Cognitive Psychology* 461. See also, Kirsten Hancock and Gillian Rhodes, 'Contact, Configural Coding and the Other–Race Effect in Face Recognition' (2008) 99 *British Journal of Psychology* 45.

[147] 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.

The higher the quality and clarity of the photograph, the more accurate the identification process-providing the individual is known to the identifier.[148] 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.'[149] However, training and experience in identification does not increase the accuracy of identification.[150]

A scheme like the NIS which is based on digital technology does not use familiarity as the basis for either authentication or verification of identity. Consequently, when identification is by comparison, whether of an individual to a photograph, a signature to that on record in the NIR or an individual's biometrics to those in the NIR, the opportunity for fraud, and for mistakes, increases.[151]

Biometrics are promoted as the strength of the NIS and are regarded as immutably connected to the rightful owner. The IPS on its website states that 'biometrics will be 'sealed to' or permanently paired with your biographical information to create completely unique and secure identity data.'[152] The IPS further asserts that:

> A criminal may steal your card, but your unique biometric data cannot be taken from you. Anyone trying to make a major financial transaction, for example, would have their

[148] 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. See, 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. See, 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.

[149] Bromby and Ness, above n 144, 7.

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

[151] Unlike the NIS, the ACS did not use biometrics to verify identity for transactions. Reliance on comparison of a photograph or a handwritten signature as the primary means of identification significantly increases the likelihood of error in verifying identity at the time of a transaction**.**

[152] Identity and Passport Service, *What is the National Identity Scheme* <http://www.ips.gov.uk/identity/scheme-what-produced.asp> at 1 September 2008.

> biometric data checked against that held in the NIR. If they were not the registered cardholder this check would fail.[153]

However, although the IPS maintains that 'your unique biometric data cannot be taken from you,'[154] in fact it can be taken. As Karen McCullagh points out, 'a person's hand or retina prints can be surgically removed–with or without the person's consent.[155] While this is an extreme example, all the identifying information including the biometrics can be copied and intercepted. The use of biometrics, specifically fingerprints, for in-person transactions does make it more difficult to use another person's token identity without detection, but not all transactions under the scheme will be face to face. The NIS contemplates a 'principally on-line verification service,'[156] where biometrics are supplied remotely through an on-line enquiry facility or through an on-line card or biometric reader,[157] making it possible to use biometrics which have been copied or intercepted. As in the case of face to face dealings, if the information presented matches that on record, the identity is verified.

---

[153] Identity and Passport Service, *Benefits to Society* <http://www.ips.gov. uk/identity/benefits -individual-british.asp> at 1 September 2008.

[154] Ibid.

[155] 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> at 27 April 2006. Note, however, that the NIS will use iris scans, not retina scans. Simson Garfinkel also maintains that the danger of mutilation will increase as society increases its reliance on biometrics. See, 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. Nevertheless advances in medical science are making science fiction a reality. For example, until recently face transplants such as those depicted in the movie *'Face Off*,' Paramount Pictures (1997) in which the central characters played by John Travolta and Nicholas Cage surgically swapped faces, were considered science fiction but in 2005 the world's first face transplant was successfully performed on a woman in France. However, a more likely scenario is that an individual may be compelled, under threat, to provide his or her identifying information (and indeed his or her token identity) for a transaction, in much the same way as a person can be forced to hand over his or her card.

[156] Regulatory Impact Assessment, Identity Cards Bill Introduced to House of Commons on 25 May 2005 (UK) para 39 <http//:www.homeoffice.gsi.gov.uk.html.> at 16 May 2006

[157] Ibid, para 23.The card reader and/or biometrics reader used by accredited organisations under the NIS must be approved by the IPS. Fingerprints are obtained by the individual placing his or her fingers on a biometric reader. To obtain a face scan and iris scans, the individual's face is scanned by a camera.

Furthermore, despite assurances as to reliability, none of the biometrics, including fingerprints, proposed for the NIS provide foolproof identification. Mistakes and errors can occur as a result of the conditions under which the biometric is obtained, stored and transmitted.

Live scan technology can produce its own set of problems. When biometrics are required to verify identity for a transaction, the individual is asked to roll his or her fingers on a screen or in the case of iris and facial scans, the individual's eye or face was to be scanned. That scanned image is then sent electronically, to be compared with the scan of the biometric stored in the NIR. The biometric scanned from an individual for verification may be obtained, stored and transmitted under different conditions from the biometric stored in the NIR. Those conditions can affect both the quality of the images and their comparison. Movement during scanning, either deliberately or involuntarily due to infirmity, can dramatically affect the quality of the image.[158] The way in which the scanned print is transmitted and stored for example, using compression technology, and distortion caused by different storage formats, can also affect the quality of the images and their interpretation by a human being or machine. Errors also occur in interpretation of a match.

Of the biometrics proposed for the NIS, fingerprints are thought to have the lowest error rate, though the actual error rate is unknown.[159] Until recently, fingerprint evidence was regarded as

---

[158]'New Fingerprint Technology' <http//:www.news10now.com/content/top_stories> at 28 May 2006. In discussing the advantages and disadvantages of live digital scanning, movement affecting the image is a significant issue. Movement during scanning can result from an individual deliberately being uncooperative but movement may also be involuntary, due illness or infirmity.

[159] Sandy Zabell, 'Fingerprint Evidence' (2005) 13 *Journal of Law and Policy* 143, 167 and 169. The actual error rate is unclear. Zabell states that 'we still do not know the actual rate of error for fingerprint identification in criminal cases. Zabell quotes Donald Kennedy, the Editor-in-Chief of *Science*,'[i]t's not that fingerprint analysis is unreliable … [but] … that its reliability is unverified by either statistical models of fingerprint variation or by consistent data on error rates.' It should be noted that the controversial report sponsored by the United States Federal Bureau of Investigation ('FBI') and prepared by Stephen Meager *et al* (known as the'50 K study') which

having a zero error rate.[160] That claim is now disputed and courts, particularly in the United States,[161] but also in the United Kingdom and Australia, have rejected fingerprint evidence as unreliable. The evidence has been rejected, on the basis of error in matching prints, [162] rather than on the basis of their uniqueness.[163] Although it is generally accepted that the rate of error is probably low, many mistakes have recently come to light.[164] Concern to date has centred on the comparison of inked and latent prints,[165] but the issues are still relevant to the NIS considering that prevention and detection of crime and national security are included in the stated purposes of the NIS.

---

used a database consisting of digital images of 50,000 fingerprints, concluded that the probability of an image being mistaken for any other in the database was 1 in 10. However, the methodology used in the study has been widely criticized and the accuracy of the results is disputed. See, the critique by David Stoney, 'Critique' in Henry Lee and Robert Gaensslen, *Advances in Fingerprint Technology* (2001), 378-383. See also, David Kaye, 'Questioning a Courtroom Proof of Uniqueness of Fingerprints' (2003) 71 *International Statistics Review* 521; Simon Cole, 'Grandfathering Evidence: Fingerprint Admissibility Rulings from Jennings to Llera Plaza and Back Again' (2004) 41 *American Criminal Law Review* 1226 and also Christopher Champod and Ian Evett, 'A Probabilistic Approach to Fingerprint Evidence' (2001) 51 *Journal of Forensic Identification* 101. As an interesting twist to this debate which is of particular interest in relation to the NIS, note Zabell's comment in referring to Professor Kaye's critique that 'it turned out that the 50,000 prints did not, in fact, all come from 50,000 different individuals; in a small number of cases, some of the prints were, in fact, duplicate prints taken from the same individual. These duplicate pairs (although of course still fairly similar) were sufficiently dissimilar to suggest that one might well see comparable pairs of prints exhibiting a comparable level of similarity coming from *different* individuals, provided only that a large enough group of prints were examined.' Zabell notes that the result depends on the particular type of automatic fingerprint identification system being used.

[160] Reportedly, this is the longstanding contention of the United States Department of Justice. See, Andy Goglan, 'How Far should Prints be Trusted?' *New Scientist*, 17 September 2005, 6. The use of deoxyribonucleic acid ('DNA') and documented misidentifications has recently led to increased scrutiny of fingerprint evidence.

[161] Reportedly, there have been at least 22 known instances in the United States. See, Simon Cole, 'More than Zero, Accounting for Error in Latent Fingerprint Identification' (2005) *Journal of Criminal Law and Criminology* 985, 999. There have also been cases in the United Kingdom as reported on *Panorama* <http//:www.bbc.co.uk.html> at 29 May 2006 and in Australia as reported on *Four Corners*. <http://www.abc.net.au/4corners/archives/2002.html> at 10 May 2006.

[162] Ibid Cole, 1030. Cole reports that proficiency tests of fingerprint examiners conducted since 1983 show an aggregate error rate of 0.8 percent. However, individual studies have revealed much more alarming results. In 1995 a proficiency test that for the first time was designed, assembled and reviewed by the International Association for Identification found that 66 percent of examiners tested incorrectly classified latent prints. Twenty two percent of those tested 'substituted presumed but false certainty for truth.' See, David Grieve, 'Possession of Truth' (1996) 46 *Journal of Forensic Identification* 521, 523. See also, Zabell, above n 159, 167.

[163] As first claimed by Galton. See, Francis Galton, *Fingerprints* (1892). See also Stephen Stigler, *Statistics on the Table* (1999), 131. Note, however, that the scientific basis for this conclusion is questionable, prompting one expert Dr David Stoney to state that '[f]rom a statistical viewpoint, the scientific foundation for fingerprint individuality is incredibly weak.' See, Henry Lee and Robert Geansslen, *Advances in Fingerprint Technology* (2001), 329.

[164] See also Zabell, above n 159, 167 and 169. Similar incidents in the United Kingdom have been featured on *Panorama* <http//:www.bbc.co.uk.html> at 29 May 2006 and in Australia as reported on *Four Corners* <http://www.abc.net.au/4corners/archives/2002.html> at 10 May 2006.

One of the most notorious incidents is worthy of mention, especially considering the national security and crime detection and prevention purposes of the NIS and the potential repercussions for individuals. The incident involved Brandon Mayfield a lawyer who lives and works in Portland, Oregon. Three United States Federal Bureau of Investigation ('FBI') officers and an independent expert, all identified Mr. Mayfield's prints at the scene of the Madrid train bombings in 2004. The FBI examiners reportedly concluded that the print was '100 percent positive identification.'[166] By contrast, the Spanish authorities concluded that the match was 'conclusively negative.'[167] Although there was nothing to suggest that Mayfield had travelled out of the United States, the FBI reportedly remained steadfast in their assessment. It was only the perseverance of the Spanish authorities who realising that a mistake had probably been made, eventually traced the prints to an Algerian man, whose deoxyribonucleic acid ('DNA') confirmed his involvement.[168] Mayfield was released after spending two weeks in prison.[169]

How did this mistake occur? It is most likely to be due to human error. Prints are obtained under a range of conditions which may influence the integrity of the information they can provide. At a crime scene, for example, prints may be smudged or incomplete. In the Mayfield case, the FBI compared a digital print obtained from a database with a latent print from the

---

[165] Fingerprints obtained at crime scenes, for example, are called latent prints because they have to be recovered using special techniques such as chemical treatments and/or illumination using ultraviolet light.

[166] Robert Stacey, 'A Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case' (2004) 54 *Journal of Forensic Identification* 706, 710.

[167] Sarah Kershaw, 'Spain and US at Odds on Mistaken Terror Arrest', *New York Times* (New York) 5 June 2004, A1. Reportedly, the Spanish authorities reportedly found seven points of correlation between the fingerprints found at the scene and Mayfield's prints, whereas the FBI found 15 points of correlation.

[168] Tomas Alex Tizon *et al*, 'Critics Galvanized by Oregon Lawyer's Case', *Los Angeles Times* (Los Angeles) 22 May 2004, 13.

[169] David Heath and Hal Bernton, 'Portland Lawyer Released in Probe of Spain Bombings', *Seattle Times* (Seattle), 21 May 2004, 1.

crime scene.[170] However, the explanations given by the FBI for its mistake in the Mayfield case are contradictory and unsatisfactory in light of accepted standards of forensic practice.[171] According to the head of Spanish National Fingerprint, '[t]hey had a justification for everything … but I just couldn't see it.'[172] The explanation he offers contains cautionary lessons relevant not only to identification using fingerprints but to the photographic identification used in the NIS:

> 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 it's curly in the picture. Maybe the woman in the picture had a permanent?[173]

Preconception and perception play a significant role in influencing a person to 'see' what they want to see or expect to see, not necessarily what is there.[174] The distortion which can result is an important factor in any form of identification. If examiners do not work 'blind,' the examination may be influenced by the opinions of colleagues or the preponderance of

---

[170] Zabell, above n 159, 148 and 149.

[171] According to Robert Stacy of the FBI '[t]he error was human error and not a methodological or technology failure.' Stacey, above n 166, 714. The error is explained, if not justified, by use of a poor quality database print and/or a poor quality latent print from the crime scene, though the exact problem is not clear. There is some doubt as to whether the digital print was a second generation print, that is, a copy of a copy and whether the latent print was of sufficient quality for an accurate comparison to be done. These aspects should have prompted the investigators to determine whether distortion was within acceptable limits. See, David Ashbaugh, *Quantitative – Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology* (1999), 146. However from Stacy's report and final recommendations, it seems that perception bias was really the issue–the matching process and its confirmation were not 'blind.'

[172] Kershaw, above n 167.

[173] Ibid. Perception and 'seeing' what one expects or hopes to see can also lead to distortion of reality. Familiar faces are recognised more accurately from internal features–the eyes, nose and mouth, whereas recognition of unfamiliar faces is dominated by external features like shape of the head, hair and ears. For a recent article on this point see, Charlie Frowd, Vicki Bruce, Alex McIntyre and Peter Hancock, 'The Relative Importance of External and Internal Features of Facial composites' (2007) 98 *British Journal of Psychology* 61. See also, Zabell, above n 159,155 where the implications of justifications and explanations in relation to fingerprint evidence are discussed.

[174] Zabell, above n 159,153. Zabell mentions this phenomenon and discusses it as the basis for rigorous standards being imposed by science. For further discussion of the phenomenon see, Michael Risinger *et al*, 'The Daubert /Kumho Implications of Observer Effects in Forensic Science: Hidden Problems of Expectation and Suggestion' (2002) 90 *California Law Review* 1. For a classical text on this subject see, Evon Vogt and Ray Hyman, *Water Witching* (1979).

evidence implicating a suspect.[175] Taking steps to eliminate bias addresses some concerns, but not all.[176]

Although bias can often not be completely eliminated in an examination by a human being, what if human bias were minimised, even eliminated, by automation? Does automation of the fingerprint matching process increase accuracy? The findings are not comforting. In their 2002 report Pankanti, Prabhakar and Jain state that,

> [o]ur results show that (1) contrary to the popular belief, fingerprint matching is not infallible and leads to some false associations, (2) while there is an overwhelming amount of discriminatory information present in the fingerprints, the strength of the evidence degrades drastically with noise in the sensed fingerprints, (3) the performance of the state-of- the- art automatic fingerprint matchers is not even close to the theoretical limit and (4), because automatic fingerprint machines based on minutia use only a part of the discriminatory information present in fingerprints, it may be desirable to explore additional complementary representations of fingerprints for automatic matching.[177]

Advances in technology do not necessarily eliminate bias. In the Mayfield case, the FBI used its automated system, Integrated Automated Fingerprint Identification System ('IAFIS'). Sandy Zabell explains that IAFIS generated a print so highly correlated to Mayfield that three senior examiners concluded that Mayfield had to be the source. 'This example demonstrates that, when searching tens of millions of inked prints the fingerprint community has no real idea of just how close a near miss can be.'[178] As Zabell observes,

> [w]hen fingerprint identification errors have been discovered in the past, the fingerprint community has almost invariably attributed them to incompetent individuals rather than problems or limitations with the methodology itself.'[179]

---

[175] Ibid, n 159, 174. Zabell concludes that '[i]n fact there is no reason why *all* verifications should not be blind and–for the reasons discussed earlier in this paper- every reason why they should.'

[176] Safeguards include using a second examiner to review the initial identification (preferably as a blind verification), ensuring the competence of all examiners, requiring a high number of matching points and having an independent expert examine the match/mismatch. Cole found, however, that that each of these safeguards failed in all of the cases of mistaken fingerprint identification he studied. See also, Cole, above n 161

[177] Sarath Pankanti, Salil Prabhakar and Anil Jain,'Transactions on Pattern Analysis and Machine Intelligence' (2002) 24(8) Institute of Electrical and Electronics Engineers *Transactions On* 1010 <http://www.doi.ieee computersociety.org/html> at 10 May 2006.

[178] Zabell, n 159,175.

But there is no 'methodology', in the sense of a universally accepted and objective set of protocols that can be applied to a set of prints to establish identity of the source.[180] Indeed, Simon Cole correctly argues that the assertion that fingerprint evidence is valid because fingerprints are unique to the individual is fundamentally fallacious. That argument, he says, is akin to saying that eye witness identification is infallible because every human face is unique.[181] As Zabell points out,

> [i]dentification of any kind involves the extraction and analysis of features; the fundamental issue is not the "uniqueness" of the object under scrutiny (be it the human face, the friction ridge patterns of the human finger, or the sequence of bases in human DNA), but the accuracy of the process used to extract features and analyze them.[182]

So what about the other biometrics originally planned for the NIS – iris and facial scans? As mentioned earlier in this chapter and in chapter 2, implementation difficulties have reportedly resulted in implementation plans for these scans being deferred.[183] While facial recognition software has advanced considerably recently and is continuing to improve, like all such technology, it is not free from error and this is the important point for this thesis. In the context of a scheme like the NIS, and the ACS, even if the accepted error rate is relatively low, a low error rate can still produce a significant number of mistakes with potentially serious consequences, especially for an individual.

For example, the accepted error rate for automated facial scanning is 10 percent,[184] although advances in technology are reducing error rates, and an error rate of 2 percent has been

---

[179] Ibid, 168.
[180] Ibid, 177.
[181] See Cole, above n 161.
[182] Zabell, above n 159, 176-177.
[183] Above n 22.
[184] One report states the error rate of 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> at 29 March 2007.

reported in Australia under controlled conditions.[185] Similarly, the error rate for fingerprint matching is considered relatively low, but to put this in perspective, consider for example, a 2 percent error rate for a population of 50 million people, which is the estimated number of individuals who will eventually be registered under the NIS.[186] An error rate of 2 percent results in 1,000,000 people being affected in the United Kingdom;[187] and of course, any error rate is unacceptable if it results in an individual being unable to use his or her token identity to transact, being held accountable for transactions made another person, or being wrongly accused of a crime.[188]

4.3. Conclusion

The validity and reliability of the identifying information used in the NIS depends on the rigor of the processes used to collect, update, store, and use that information. There is no doubt that the logistics involved in establishing and maintaining a scheme like the NIS on an on-going basis are considerable. However, while the process for identity authentication at the time of registration and the maintenance of up to date information in the NIR are certainly areas of potential weakness, the identification used in the scheme is inherently fallible.

---

[185] 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> at 27 April 2006. Reportedly, an error rate of 2 percent was achieved in trialling 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. See, London School of Economics and Political Science and the Enterprise Privacy Group, '*The Identity Project. An Assessment of the UK Identity Cards Bill and its Implications'* Interim Report, March 2005, 49.

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

[187] Under the ACS, 16.7 million adults were to be registered over two years. See,Australian Government, Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007, *x*. In Australia, a 2 percent error rate potentially amounts to 340,000 incidents of incorrect identification in that population.

All the identifying information used in the NIS, and proposed for the ACS, has acknowledged error rates. Comparison of appearance to the photograph which will be the method most commonly used to verify identity for transactions under the NIS and which was to form the basis of the ACS, has the highest error rate if there is not a history of personal acquaintance. And the matching of biometrics which form the basis of identification under the NIS is not infallible.

Errors including false positives can have serious consequences in the context of a national identity scheme, particularly for an individual. This is especially so if the scheme has security and crime detection and prevention objectives like the NIS, but even a scheme like the ACS is used for law enforcement. Indeed, the inevitability of a national identity scheme like the ACS eventually being established in Australia, highlights the need for a national human rights regime in that country. This need is illustrated in the next chapter which considers the individual rights, specifically the right to privacy and the right to identity, which this thesis argues must arise as a consequence of the new concept of identity. The recognition and protection afforded to those rights in the United Kingdom as a member of the European community, provides a sharp contrast to the position in Australia.

---

[188] As may occur if some of his or 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 on the ID card or in the NIR.

5. Digital Identity – Consequential Individual Rights

'On the third day Winston went to the vestibule of the Records Department to look at the notice board. One of the notices carried a printed list of the members of the Chess Committee, of whom Syme had been one. It looked almost exactly as it had looked before-nothing had been crossed out-but it was one name shorter. It was enough. Syme had ceased to exist: he had never existed.'[189]

5.1. Introduction

This chapter examines the right to identity which this thesis argues arises in specific form in relation to digital identity in the context of a scheme like the NIS, and its relationship to other rights, most notably the right to privacy. In the context of the NIS, the right to identity is the right to be recognised and to function as an individual under the scheme and it takes specific form as the right of an individual to an accurate, functional, unique token identity. This right arises because under the scheme, token identity is an individual's transactional identity and it is the gateway to, and gatekeeper of, the other Schedule 1 information which makes up an individual's database identity. This chapter argues that this right to identity is emergent.

The right to privacy is relatively well established with the consequence that it has dominated jurisprudence and legal scholarship. This focus on privacy has obscured the significance of the right to identity, especially in the context of a scheme like the NIS**.** The right to identity is conceptually very close to the right to privacy in that they both relate to individual autonomy but they are nevertheless distinct rights. They are different in nature and they are infringed in different ways.

As explained in this chapter, the right to identity is infringed by the untrue or false use of indicia of identity, whereas the right to privacy is infringed by the association of an individual

with personal facts, contrary to the wishes of the individual. In the context of the NIS therefore, the right to identity is the right of the individual to an accurate, functional token identity and to its exclusive use, whereas right to privacy protects the other Schedule 1 information which makes up an individual's database identity.

Apart from being different in nature, the right to identity and the right to privacy also differ in the extent to which they can be subordinated to the public interest. Unlike the right to privacy, this thesis argues that the right to identity in the context of a scheme like the NIS, is of such a fundamental nature that its interference cannot be justified on public interest grounds. The argument developed in this chapter is that, in the context of a national identity scheme, the right to identity therefore provides more protection than the right to privacy. And the protection provided by the right to identity is more appropriate than the protection provided by the right to privacy, considering the role and nature of token identity under the scheme and the consequences for the individual if token identity is inaccurate, dysfunctional or is able to be used by another person.

This chapter argues that in view of the emergent concept of digital identity and its consequences for an individual, particularly in the context of a national identity scheme, the right to identity should be recognised and protected. The protection afforded by the right to identity is important especially in view of token identity's pivotal role under the scheme as discussed in chapters 2 and 3. The need for protection is given added significance considering the inherent vulnerabilities of the identifying information examined in chapter 4.

---

[189] George Orwell, *Nineteen Eighty–Four* (1949), 154.

Just as the emergent concept of digital identity is part of a broader concept of identity, the right to digital identity under the NIS is part of a broader right to identity. Although the right to identity in this broad sense is not considered in this thesis, the right to identity protected under the *Convention of the Rights of the Child* is considered to show that a right to identity arises at birth and that it is comprised of similar elements to the concept of identity under the NIS. Token identity under the NIS largely consists of information which is established at birth, so there are strong similarities with the elements of identity protected by the *Convention on the Rights of the Child*. The rationale for protection of identity under the *Convention on the Rights of the Child* (because of the prospect of the creation of false identities and the ensuing consequences for individuals) also resonates with the need to protect identity, particularly token identity, in the context of a scheme like the NIS.

In the context of the NIS, the emergent right to identity, that is, the right to have an identity under the NIS, arises on registration when the individual is accepted into the scheme. The NIS generally applies to minors from the age of 16 years, as well as to adults.[190] So, in the case of a minor, the right to identity is protected by Article 8 of the *Convention on the Rights of the Child*. However, in the United Kingdom, the right to identity of adults, as well as minors, is protected under the *ECHR*. The *ECHR* is the focus of the discussion in this chapter because the European Court has specifically stated that a right to identity is protected by Article 8(1) of the *ECHR*.[191]

While privacy can provide some protection to the other Schedule 1 information which makes up database identity, this chapter shows that privacy does not clearly protect an individual's token identity from unlawful interference and its misuse by another person. Indeed, the *Data*

[190] This is typical. The Belgium E-ID scheme, for example, also applies to children from 12 years of age.

Protection Act and the *Data Protection Directive* can operate to screen errors caused by fraud and system error, from scrutiny. An individual's right to privacy is also generally subject to the public interest whereas, as this chapter argues, in the absence of extraordinary circumstances, an individual's right to identity should not be subordinated to the public interest. Consequently, interference with an individual's right to identity, that is, the right to be regarded as a unique individual under the scheme, cannot be justified on the basis that it is, for example, an unfortunate, or indeed an inevitable, consequence of a scheme which has broader societal objectives. As a result, unauthorised removal or change of an individual's identity or its misuse by another person cannot ordinarily be justified on the basis that it is 'in accordance with the law' or 'necessary in a democratic society' under Article 8(2) of the *ECHR*. In presenting this argument, the right to identity in the context of the NIS, that is, the right to token identity, is distinguished from other associated rights arising as a consequence of the scheme, such as the right to register, the right to use the registered identity for particular transactions, and the right to privacy.

The *Identity Cards Act* and the NIS are used as the basis for the discussion in this chapter but many of the same issues potentially arise in relation to similar schemes including the proposed ACS, should it be established in Australia in the future. There are strong similarities between the law of United Kingdom and Australia but significantly, Australia does not have a national equivalent to the United Kingdom's *Human Rights Act,* and the *Australian Constitution* does not contain a bill of rights.

---

[191] *Peck v United Kingdom* [2003] All ER 255, (2003) 36 EHRR 719, [2003] EMLR 287.

The United Kingdom human rights regime, although located within the European regime, is a potential model for Australia.[192] Two Australian jurisdictions have recently enacted legislation which is based, inter alia, on the *Human Rights Act* [193] and the other Australian jurisdictions may enact similar legislation in the future,[194] although a national approach is required if a national identity scheme is established. Although the United Kingdom approach is not without its critics, it provides valuable perspective regarding the impact of a national identity scheme on individual rights. This perspective is especially valuable because *ECHR* claims have very different objectives and hence different requirements as to procedure and standards of proof, to common law claims.

Essentially, common law claims compensate a claimant for damage caused, whereas *ECHR* claims are designed to uphold minimum human rights standards. This is an important point in the context of the NIS because at present there is not a common law cause of action for breach of identity. In any event, proof and quantification of damage are likely to be very difficult essentially because of the nature of this concept of identity. In the United Kingdom, however, an individual whose identity has been incorrectly recorded in the NIR or which has been misused under the NIS, can pursue an *ECHR* claim against the government and entities using the scheme,[195] on the basis that the individual's right to identity has not been adequately protected. The case law on Article 8 of the *ECHR* discussed in this chapter illustrates how the

---

[192] As Carolyn Evans and Simon Evans observe '[i]t is likely that the most influential of the regional human rights courts for the development of Australian human rights law will be the European Court of Human Rights (European Court). The European Court is the longest-established regional human rights court and has the most prolific jurisprudence.' They also comment that '[i]t may be that, as human rights Acts become widespread across Australia, the common law will begin to change in response as judges become more used to applying rights standards…' Carolyn Evans and Simon Evans, *Australian Bills of Rights* (2008) 156, 214.

[193] See, the *Human Rights Act 2004* (ACT) and *the Charter of Human Rights and Responsibilities Act 2006* (Vic).

[194] Plans for a charter of rights by the Western Australian and Tasmanian government are on hold pending the outcome of the National Human Rights Consultation established by the federal government to seek the views of the Australian community on how human rights and responsibilities should be protected in the future.

[195] S 6(3) *Human Rights Act* states that 'public authority' 'includes any person certain of whose functions are of a public nature.'

interests of the individual are balanced with societal interests in considering whether interference with an *ECHR* right is justifiable and illustrates the need for a similar approach in Australia, should a national identity scheme be established.

This chapter begins by distinguishing identity from privacy. The origins and nature of the right to identity in the *Convention on the Rights of the Child* are then considered and the argument that a specific right to identity in the context of the NIS should be recognised is presented. The protection afforded by that right to identity is contrasted with the protection afforded by the right to privacy as it applies to database identity including token identity, having regard to the *Human Rights Act*, the *ECHR*, the Data Protection Act and the *Data Protection Directive.*

5.2. Identity Distinguished From Privacy

Identity is conceptually very close to privacy, but although they share the same conceptual roots, privacy and identity relate to different interests. They are, however, often considered as one, with identity being subsumed into privacy. The following comments of the United Kingdom Information Commissioner in relation to the NIS, shows how identity and privacy are often amalgamated, with the result that the importance of identity is obscured by the focus on privacy:

> We must recognise that we may risk turning our society from one where the need to prove identity is commensurate with the service on offer, with complete anonymity being a real option in many circumstances to one where the highest level of identity validation becomes the norm for the most mundane of services, one where we run the risk of the unique personal number being used to track our interactions with the state and others, and to have all this recorded on a central register under its control. Of course nothing in the government's current proposals is so draconian. But we must appreciate that, whilst we may be reassured that benign administrations will live up to their promises about

> limitations on use, we will be creating a potentially powerful infrastructure. Our close European neighbours can account for how this can be misused at catastrophic social cost.[196]

Identity is closely related to privacy in that both relate to autonomy and specifically to an individual's right to self-determination in relation to information relating to him or her.[197] However, privacy in the context of the NIS is essentially about an individual's control over the collection, disclosure, and use of his or her personal information.[198] By contrast, identity is about autonomy in the sense of being recognised and regarded as a unique individual which in the context of the NIS, specifically relates to the ability of a person to be recognised and to transact as a unique individual under the scheme.

Neethling's Law of Personality[199] ('*Neethling*') provides further insight into the nature of identity. Identity is an interest which is much more developed under South African law and it is heavily influenced by the European concept of identity, particularly under German and Dutch legal doctrine. Although its origins, and to an extent, its nature[200] differ from the emergent concept of digital identity, there are broad similarities. According to *Neethling*,

> [i]dentity as an interest in personality, can be defined as a person's uniqueness or individuality which defines or individualises him as a particular person and thus distinguishes him from others. Identity is manifested in various indicia by which that particular person can be recognised; in other words, facets of his personality which are characteristic of or unique to him, such as his life history, his character, his name, his creditworthiness, his voice, his handwriting, his appearance (physical image), etcetera. A person has a definite interest in the uniqueness of his being and conduct being respected by outsiders. Therefore a person's identity is infringed if any of these indicia are used without authorization in ways which cannot be reconciled with his true image.[201]

---

[196] United Kingdom Information Commissioner, *The Identity Cards Bill–The Information Commissioner's Concerns* (June 2005) <http://www.ico.gov.uk/ eventual.html> at 10 May 2006.

[197] Above n 191.

[198] Including knowledge of when and where the information is being collected, who is collecting and using it, how it is being used and will be used in the future; as well as the individual's rights of correction and notation in respect of the information.

[199] J Neethling, J Potgeiter and P Visser, *Neethling's Law of Personality* (2005).

[200] Some aspects of the right to identity under South African law are similar to the rights of celebrities under United States law to protection of economic interests in their personalities. See, Neethling ibid, 36.

In the context of a national identity scheme like the NIS, collectively the information which comprises token identity 'defines or individualises' a person 'as a particular person and thus distinguishes him from others.'[202] Under the scheme, an individual's uniqueness is determined by the information which collectively comprises his or her token identity. The token identity registered under the scheme is an individual's transactional identity and it is used to access the more extensive information which makes up the individual's database identity. Token identity is therefore the identity by which the individual is known under the scheme and the individual has, to use Neethling's words, a definite interest in its uniqueness.

In an insightful passage, *Neethling* distinguishes privacy from identity:

> In contrast to identity, privacy is not infringed by the untrue or false use of the indicia of identity but through an acquaintance with (true) personal facts regarding the holder of the right contrary to his determination and will.[203]

This is an important distinction which highlights the difference between the role of token identity under the NIS and the other Schedule 1 information which makes up database identity. It also highlights the distinction between the right to identity and the right to privacy in the context of the scheme and the need to articulate and separate the right to identity from the right to privacy.

An individual's right to identity is infringed by the 'untrue or false use' of his or her token identity. By contrast, the right to privacy is the right of the individual to be informed of the recording of the other Schedule 1 information in the NIR and, where appropriate, to correct it

---

[201] Neethling, above n 199, 36. This statement also accords with the definition of 'identity' in the *Concise Oxford Dictionary*, that is, 'absolute sameness' but the definition also includes 'individuality, personality.'

[202] The information which, with token identity, constitutes database identity is indicia of identity but in a broad sense. Database identity relates to an individual's life history. The view expressed in *Neethling* is that an individual's life history is a facet of an individual's personality which is characteristic of or unique to that individual. See Neethling, above n 199, 36.

[203] Neethling, above n 199, 37.

and to be informed of its use, including its disclosure. In the United Kingdom, the rights of the individual in relation to the personal information which makes up the other Schedule 1 information are prescribed by the *Data Protection Act.* That Act gives effect, with some change, to the standards set by the European *Data Protection Directive*.[204]

5.3. The Right to Identity under the Scheme

The right to identity under the NIS, as postulated by this thesis, is more than just control of personal information. It is the recognition that each individual has an inalienable 'interest in the uniqueness of his being.'[205] In the context of a national identity scheme which requires that identity be established for transactions, the right to identity is about an individual's right to be recognised, and to transact, as a unique individual–in effect to be considered a unique entity under the scheme.

The *Identity Cards Act* imposes some obligations on individuals, mostly requirements to notify changes and errors in the 'registrable facts,'[206] and some limitations on the government's power to record and disclose information. However, considering that the registered identity is *the* identity which is recorded by the government, and which is officially recognised in the United Kingdom, this thesis argues that additional implicit individual rights in relation to that identity, and government obligations in relation to those rights, must arise.

---

[204] The *Data Protection Act* states that it was passed to apply 'Directive 95/46/EC of European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.' The 10th Preamble to the Directive states that ' the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law.' Art 1(1) states that the 'object of the Directive' is that '[i]n accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'

[205] Neethling, above n 199, 36

On registration, the individual is accepted into the scheme and from that time, considering the presumptions of accuracy and authenticity on which the scheme is based, the individual has the right to an accurate database identity and to an accurate, functional and unique token identity. Most importantly, given the nature of the scheme and that it is based on 'one person: one identity,'[207] the right to identity in the context of the scheme must include the individual's exclusive use of his or her token identity.

Accuracy and exclusivity, are considered in more detail later in this chapter in relation to human rights, and are further considered in chapter 6 in relation to protection, but for the moment, the right to identity under the NIS needs to be placed in context having regard to the broader concept of identity.

When the scheme becomes fully operational and eventually compulsory, the identity of an individual as recorded in the NIR will become more influential and more pervasive. The identity which is the subject of this thesis will then be more significant and will be a large component of an individual's identity. However, when the scheme is fully operational although registered identity will be a relatively large component, it will still be just one part of a United Kingdom resident's identity because identity in a broader context includes aspects, such as racial, cultural, sexual and familial identity. As discussed in chapter 2, identity can also be conceptualised more broadly as Solove's 'digital person,' who is 'composed in the collective computer networks of the world.'[208]

---

[206] S 1(5). Recall that 'registrable facts' are defined to include 'identity' and the other sch 1 information which comprises database identity.
[207] Wadham, Gallagher, Chrolavicius, above n 30, 127.

The impact of database identity, including token identity, in relation to an individual's identity in a wider context and the application of the right to identity arising in the context of the NIS, can be depicted diagrammatically:

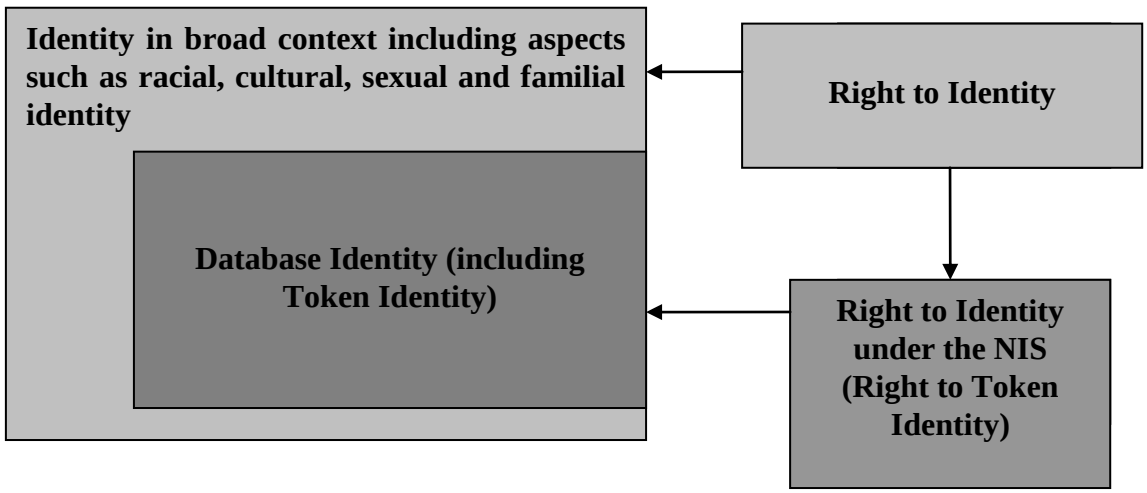

Fig.11.

Under a scheme like the NIS, the right to identity takes specific form as the right to token identity, because token identity is an individual's transactional identity and it is the gateway to the other Schedule 1 information which makes up the individual's database identity.

5.4. An Express Right to Identity

The *Convention on the Rights of the Child* expressly includes the right to identity. This treaty has been ratified by the United Kingdom[209] so it is part of international law although it has not yet been fully incorporated into domestic law. The inclusion of the right to identity in Article

---

[208] Solove, above n 48, 1.

[209] The United Kingdom ratified the *Convention on the Rights of the Child* on 16 December 1991 and it came into force on 15 January 1992. Australia ratified the *Convention on the Rights of the Child* on 17 December 1990 and it came into force on 16 January 1991.

8[210]of this treaty is significant because it shows that an express right to identity exists. The elements of identity specified in Article 8 also comprise some of the same information which constitutes digital identity under the NIS [211] and identity is clearly distinguished from privacy which is covered under Article 16.[212]

Article 8 specifically refers to the right to identity and to elements of an individual's identity. Although 'identity' is not defined, Article 8(1) specifies that:

> States Parties undertake to respect the right of the child to preserve his or her *identity, including nationality, name and family relations* as recognised by law without unlawful interference.[213] (emphasis added)

Article 8(2) further states that:

> Where a child is illegally deprived of some or all of the elements of his/her identity, States Parties shall provide appropriate assistance and protection, with a view to speedily re-establishing his or her identity (emphasis added).

The concept of identity in Article 8(1) includes 'name and family relations' and 'nationality.' This list is not exhaustive but the specific inclusion of these elements is significant considering the information which comprises token identity under the NIS and that most of that information is required to be registered at birth under Article 7(1).[214]

---

[210] This article and the other Articles referred to in this thesis have been ratified by both the United Kingdom and Australia without reservation.

[211] Although nationality is not part of token identity under the NIS, nationality is expressly included in database identity. See sch 1 pt 3(a) *Identity Cards Act*. The *Identity Cards Act* applies to specified categories of residents and not just citizens.

[212] Art 16 *Convention on the Rights of the Child* states that: 'No child shall be subjected to arbitrary and unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation.' Art 18(2) states that: 'The child has the right to the protection of the law against such interference or attacks.'

[213] Art 29(1)(c) which deals with the education of the child also mentions identity but it is identity in a different context and in a narrower sense– cultural identity.

[214] Art 7(1) *Convention on the Rights of the Child* provides that: 'The child shall be registered immediately after birth and shall have a right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.'

Article 8 was included in the *Convention on the Rights of the Child* as a result of a proposal by Argentina following a campaign by the Abuelas de Plaza de Mayo, the grandmothers of 'The Disappeared' in Argentina, for formal recognition of the right to identity.[215] The Abuelas alleged that their children and grandchildren were systematically removed from their families in the 1970s by the military junta and given a new legal identity as the children of other people. In concerns which resonate with concerns about the NIS, the Abuelas considered that Argentina's adoption laws, at that time, concealed children's true identities and enabled false identities to be created for them.[216]

The *Convention on the Rights of the Child* confirms the existence of a right to identity under international law and the nature of that right and its origin are significant in the context of this thesis. Nevertheless the *Convention on the Rights of the Child* only applies to minors so it has limited application to the NIS, whereas the European Court has stated that a right to identity of application to adults and children is protected under the *ECHR*.[217]

5.5. Right to Identity under European Human Rights Law

The *ECHR* is incorporated into United Kingdom domestic law by the *Human Rights Act*. The *Human Rights Act* provides that '[i]t is unlawful for a public authority[218] to act in a way which

---

[215] The original proposal was: 'The child has the inalienable right to retain his true and genuine personal, legal and family identity. In the event that a child has been fraudulently deprived of some or all the elements of his identity, the State must give him special protection and assistance with a view to establishing his true and genuine identity as soon as possible. In particular, this obligation of the State includes restoring the child to his blood relations to be brought up.' See, Sharon Detrick, 'The United Nations Convention on the Rights of the Child. A Guide to the "Travaux Preparatoires" ' (1992), 292.

[216] Their campaign resulted in Argentina recognising a constitutional right to identity and adopting an open adoption system. See, Lisa Avery, A Return to Life: The Right to Identity and the Right to Identify Argentina's 'Living Disappeared' (2004) 27 *Harvard Women's Law Journal* 235.

[217] Above n 191.

[218] 'Public authority' is not defined in the *Human Rights Act* but s 6(3) states that 'public authority' 'includes any person certain of whose functions are of a public nature.' While it is clear that government departments and authorities like the IPS are public authorities under the Act, the situation is less clear for bodies that perform a

is incompatible with a Convention right.'[219] Section 3(1) of the *Human Rights Act* provides that '[s]o far as is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with Convention rights.'

Non-compliance with the *ECHR* does not strike down the legislation but non-compliance must be notified when a Bill is introduced to Parliament,[220] and may be notified when legislation is interpreted by a court.[221] This process has the effect of raising the awareness of Parliamentarians and the legal profession, including the judiciary, of the human rights implications. Most importantly, it can alert the public to non-compliance and under the European human rights regime, a claim can be pursued by an individual before a domestic court and the European Court.[222]

ECHR claims have different objectives and features from common law claims, as recently summarised by Lord Brown:

---

mixture of public and private functions. This has implications for private sector bodies using the NIS because *ECHR* rights are directly enforceable only against public authorities. For a recent case in which the House of Lords considered whether a private sector body was a public authority for the purposes of the *Human Rights Act* see *YL v Birmingham City Council* [2007] UKHL 27. The majority concluded that a private nursing home operating on a profit basis did not perform a function of a public nature in providing accommodation and care for a publicly funded resident. The majority was clearly concerned that public law rights might interfere with private law contractual rights and the commercial interests of private enterprise. See, Stephanie Palmer, 'Public, Private and the Human Rights Act 1988: An Ideological Divide' (2007) *Cambridge Law Journal* 559, 567.

[219] S 6(1).

[220] Under s 19 the Minister in charge of the Bill in either House of Parliament must make a statement that the Bill's provisions are compatible with the Convention; or that although he or she is unable to make a statement of compatibility, the government nevertheless wishes the House to proceed with the Bill. Subordinate legislation may be invalid to the extent of the inconsistency unless 'the primary legislation prevents removal of the incompatibility.' This latter point is relevant to the *Identity Cards Act*, considering that it empowers the Secretary to make regulations in many key areas. See, for example, s 10(5) *Identity Cards Act.*

[221] S 4(2) *Human Rights Act*.

[222] In the United Kingdom, an individual can rely on the rights enshrined in the *ECHR* in domestic proceedings and before the European Court. S 8(1) and s 8(6) *Human Rights Act* provides that a Court or tribunal 'may grant such relief within its powers as it considers just and appropriate.' There is scope for a court in the United Kingdom to award damages, but under the *Human Rights Act* it is limited. S 8(3) provides that no damages are to be awarded unless necessary for just satisfaction. See, sub-ss 8(2) – (4). The power of the European Court to award just satisfaction under Art 50 *ECHR* is much wider: 'If the court finds that a decision or a measure taken by a legal authority or any authority of a High Contracting Party is completely or partially in conflict with the obligations arising from … the convention, and if the internal law of the said party allows only partial reparation

> Where civil actions are designed essentially to compensate claimants for their losses, convention claims are intended rather to uphold minimum human rights standards and to vindicate those rights. That is why time limits are markedly shorter…It is also why s 8 (3) of the Act provides that no damages are to be awarded unless necessary for just satisfaction. It also seems to me to explain why a looser approach to causation is adopted under the convention than under English tort law. Whereas the latter requires the claimant to establish on the balance of probabilities that, but for the defendant's negligence, he would not have suffered his claimed loss… under the convention it appears sufficient generally to establish merely that he lost a substantial chance of this.[223]

The observance of minimum human rights standards is the most important consideration for a scheme like the NIS especially considering the legal nature of token identity as examined in chapter 3 and the inherent fallibilities of the identifying information as discussed in chapter 4. The nature of the emergent concept of identity also means that a direct common law cause of action may be difficult to establish at this time. Copyright does not protect the individual's rights in his or her digital identity under the scheme and the individual is not necessarily protected as a result of the recent and remarkable extension of the law of confidence in the United Kingdom[224] because that action is primarily directed at protecting the individual's privacy. The nature of digital identity also means that damage can be difficult to establish and quantify.

---

to be made for the consequences of a decision or measure, the decision of the court shall if necessary, afford just satisfaction to the injured party.'

[223] *Van Colle v Chief Constable* [2008] 3 All ER 977, 1018.

[224] See, *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457 ('*Campbell*'). The development of privacy law in Australia has taken a similar path to the United Kingdom although in relation to a tort of privacy. The rationale for privacy protection has been expressed by the High Court of Australia in similar terms to the courts in the United Kingdom but on the basis of fundamental values rather than fundamental rights. The leading High Court of Australia decision is *Australian Broadcasting Commission v Lenah Game Meats* (2001) 208 CLR 199 ('*Lenah*') which opened the door to the possibility of an action for invasion of privacy. Following the decision in *Lenah*, Senior Judge Skoien of the District court of Queensland held in *Grosse v Purvis* [2003] QDC 51 that there is a tort of invasion of privacy. The requirements for the cause of action set out by His Honour are strikingly similar to the formulation established in the United Kingdom in *Campbell.* For the invasion to be actionable, His Honour stated that there must be a willed act by the defendant which intrudes on the plaintiff's privacy or seclusion in a manner considered highly offensive to a reasonable person of ordinary sensibilities which causes detriment to the plaintiff. The detriment must be mental, psychological, emotional harm or distress, or which prevents or hinders the plaintiff from doing an act which he/she is lawfully entitled to do. Whether a tort for invasion of privacy currently generally exists under Australian law remains uncertain but for a recent Victorian decision which closely followed the reasoning in *Campbell* see, *Doe v ABC* [2007] VCC 28.

5.5.1. Right to Identity under Article 8

Article 8 of the *ECHR* is entitled 'Right to Respect for Private and Family Life.' 'Private life' has been interpreted by the European Court as including the right to identity.

Article 8(1) states that '[E]veryone has the right to respect for his private and family life, his home and his correspondence' and Article 8(2) provides that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others.[225]

The meaning of 'private life' in Article 8 was considered by the European Court in *Peck v United Kingdom* ('*Peck*')[226] The case considered the public television broadcast of CCTV footage showing Peck (a young man who was in a state of severe depression and intending to commit suicide) walking alone down a street carrying a knife. The Court commented that Article 8 protects 'a right to identity:'

> Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name, sexual orientation, and sexual life are important elements of the personal sphere protected by Article 8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'…[227] (emphasis added)

Peck did not elaborate further on the right to identity and of course the case predates the emergent concept of digital identity. However, the Court's statement invokes protection of the

---

[225] Compare Art 7 *Charter of Fundamental Rights of the European Union* (Official Journal of the European Communities 2000/C 364/01) 18 December 2000, which is entitled 'Respect for private and family life' and simply states that: 'Everyone has the right to respect for his or her private and family life, home and communications.'

[226] Above n 191.

[227] Above n 191, para 57 citing *PG and JH v United Kingdom* ECHR 2001-IX.

'private sphere' advocated by Charles Reich.[228] Reich calls 'the individual sector,' the 'zone of individual power' necessary for the healthy development and functioning of the individual and 'absolutely essential to the health and survival of democratic society.'[229] This protection of the 'private sphere' derives its moral force from the liberal ideal of autonomy. Any interference with an individual's self-determination in that sense, impacts on the autonomy of society as a collective, and on the values which underpin democracy, a view which is highly influential in European jurisprudence. A right to identity is part of that personal sphere and this thesis argues that the right to token identity under the NIS is now also part of that sphere.

While the other Schedule 1 information which makes up database identity is essentially private information, token identity is comprised of information which is mostly public. Token identity is protected under Article 8(1) not because it is private in the sense of being confidential but because Article 8 protects individual autonomy. In the context of the NIS, the autonomy protected by Article 8 is the autonomy of the individual to use his or her token identity to transact.

Under the scheme, token identity is used by the individual to establish business relationships with public and private sector entities. As the court in *Peck* states, Article 8 'protects the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature.'[230] In the context of the NIS, this is the right of an individual to an identity which enables him or her to transact under the scheme. It is the right of the individual to his or her transactional identity which in the context of the NIS is the right to an accurate, functional unique token identity and to its exclusive use.

---

[228] Charles Reich 'The Individual Sector' (1990-1991) 100 *Yale Law Journal* 1409.
[229] Ibid, 1442.
[230] Above n 191, para 57

5.5.2. The Nature of Right to Identity under Article 8

In the context of the NIS, the right to identity is the right to be recognised and to be treated as a unique individual under the scheme and this thesis argues that unilateral interference with that right cannot usually be legitimately justified under Article 8(2) of the *ECHR.* In this regard the right to identity differs from the right to privacy which is also protected under Article 8 because the right to privacy is often subordinated to the public interest especially where there are security and crime protection and detection objectives. By contrast, this thesis postulates that an individual's right to identity should not be subordinated to the public interest except in the most extraordinary of circumstances. Indeed, considering the consequences for an individual and the broader societal implications of the alteration or removal of an individual's identity, it is difficult to imagine a situation where the public interest can legitimately be considered to override an individual's right to his or her identity.

It is important, though, to distinguish the right to identity from other associated rights which arise as a consequence of a national identity scheme, such as the right to register which has greater significance before the scheme becomes compulsory, and the right to use the registered identity for particular transactions.

The right to register under the NIS is subject to prerequisites such as residency, age and usually, the requirement to register in person. Subject to these requirements, an individual has a right to register. One can envisage, for example, that a person under the age of 16 years may assert that he or she has a right to register and that the age requirement is an infringement of his or her rights. The right to register under the NIS is a different claim to the right to identity under the *Convention on the Rights of the Child* which under Article 8(1) is the right of the child to '*preserve* his or her identity, including nationality, name and family relations as

recognised by law without unlawful interference.'(emphasis added). Recall also that Article 8(2) further states that 'Where a child is *illegally deprived* of some or all of the elements of his/her identity States Parties shall provide appropriate assistance and protection, with a view to speedily re-establishing his or her identity'(emphasis added). Establishing a minimum age for registration of an identity under the scheme does not necessarily interfere with these rights as conferred under the *Convention on the Rights of the Child*. In these circumstances, the interests of the individual in registering under the NIS would, and should, be balanced against the public interest objectives of the scheme. However, when a minor registers under the scheme, if the registered token identity is inaccurate, dysfunctional or is able to be used by another person, then this thesis agues that there is a breach of the child's right to identity. The minor would then have a claim for breach of Article 8(1) of the *Convention on the Rights of the Child* which is in effect an unconditional right, as well as for breach of Article 8 of the *ECHR* which under Article 8(2) takes into account public interest considerations.

Similarly, after registration, use by an individual of his or her token identity for some transactions may be restricted or even curtailed on public interest grounds such as where fraud is suspected.[231] The individual may claim that such a restriction is an infringement of his or her rights under Article 8(1) of the *ECHR* but such a restriction would, and should, be balanced against broader societal interests under Article 8(2) of the *ECHR*.

These associated rights are fundamentally different in nature from an individual's right to identity under the NIS in that the individual's right to identity is a fundamental human right. In the context of the NIS, that right emerges on registration because at that time the

[231] Tags can be associated with token identity. In the case of suspected fraud for example an alert or 'stop' may be posted. Although these tags can be attached to token identity they are not part of token identity. They are part of database identity.

prerequisites for registration are met, the required checks have been completed and the presumptions of accuracy and authenticity on which the scheme is founded, apply. At that time, the individual has the right to his or her registered identity and specifically, to an accurate, functional, unique registered token identity and to its exclusive use. Unlike the other associated rights and the right to privacy, this right of an individual to his or her registered identity cannot legitimately be curtailed, nor should it be made conditional, other than in extraordinary circumstances.

The distinction between the limitations on a right like privacy and the right to identity is highlighted by the case of a person who has been convicted of a crime and is incarcerated. It is clear that in these circumstances, an individual's right to privacy does not prevent him or her being under surveillance in prison. Public safety considerations enable the prisoner to be kept under observation, and the loss of privacy is potentially total.[232] By contrast, this thesis argues that even when incarcerated a prisoner has a right to identity and in a democracy that right to identity cannot legitimately be unilaterally removed, or altered, or made conditional on public interest grounds. The prisoner may be prevented from using his or her registered token identity for some transactions[233] but that is an entirely different matter from unilaterally removing or changing a person's identity or denying an individual the right to have a recognised identity.

The enduring nature of identity which is based on birth information and the rights of the individual in respect of that identity are evident when considered in the context of a witness

[232] One can readily envisage circumstances in which the public interest justifies placing a prisoner under 24 hour surveillance, monitoring all incoming and outgoing communication and compelling the provision of samples for DNA and other analysis, for example.

[233] If the individual is prevented from using his or her token identity for all transactions, however, that would, in effect, be a denial of his or her right to identity under the scheme.

protection program. Even if an individual is assigned a new identity under the program, the assignment must be with the individual's consent and cooperation. Under a witness protection program, name and date and place of birth may be changed in the Register of Births, Still-Births, Deaths and Marriages, though witness protection legislation typically provides that the original details not be obliterated. Although the original record is screened from public view, it is retained and future restoration of the original identity is possible.[234]

Indeed, other than in a situation in which the original registration of identity under the NIS is tainted by fraud or error, it is difficult to envisage circumstances where removal or change of an identity could be considered 'in accordance with the law' and 'necessary in a democratic society' under Article 8(2) as interpreted by the European Court and domestic courts in the United Kingdom. The line of inquiry followed by a court will be first to determine whether there is infringement of a right protected by Article 8(1). It is then a question of whether the infringement is justified as being in accordance with the law. If the infringement is within Article 8(2), say for national security or for crime detection or prevention, then the question is whether the infringement is necessary in terms of its proportionality.

In a situation where the registration of identity is incorrect because of the individual's fraud for example, there is not an infringement of the right to identity under Article 8(1) in the first place. The person's real identity is not removed or changed. The error caused by the fraud is merely rectified. However, if the error is that of the system and it affects the accuracy and integrity of the individual's registered token identity then there is an interference with that individual's right to identity under Article 8(1). This thesis argues that that infringement

[234] See, for example, in Australia s 19 and s 11 *Witness Protection Act 1994* (Cth). In the United Kingdom, see sub-ss 82(2) and 82(3*) Serious Organised Crime and Police Act 2005* (UK) c 15 which is not as clear as the Australian legislation but which still contemplates restoration.

cannot be justified on the basis that it is an unfortunate, and an inevitable, consequence of a scheme which has public interest objectives including national security and crime detection and prevention. An individual's right to identity in the context of the NIS, that is, the right to an accurate, functional, unique token identity and to its exclusive use, will not be subordinated to the public interest under Article 8 of the *ECHR* in this situation. Unlike the right to privacy, the right to identity protects the rights of innocent individuals in these circumstances.

5.6. The Protection Provided By the Right to Privacy

While the right to identity and the right to privacy both provide protection to the information which comprises an individual's identity under the scheme, each right applies in a different way. Each right also applies to different parts of the information which comprises an individual's identity under the scheme and the protection afforded by each right also differs.

The other Schedule 1 information is clearly personal information and is subject to the provisions of the *Data Protection Act* which gives effect to the right to privacy in the United Kingdom and the *European Data Protection Directive* on which the Act is based. The right to privacy protects that information and the *Data Protection Act* and the *European Data Protection Directive* confer general rights on an individual to access his or her entry on the NIR, to correct or notate the record, and to be informed of the disclosure and use of his or her personal information as recorded in the NIR. However, these rights are subject to significant exceptions in the interests of national security, crime detection and prevention and commercial impact. Although the legislature attempts to balance the rights of the individual with the need for information, in many respects the *Data Protection Act* subordinates

individual interests to public and commercial interests.[235] The overall result is that an individual's right of access, correction and to be informed of the use and disclosure of the personal information which comprises his or her entry in the NIR are relatively weak compared to the power of government to collect, use and disseminate information.

Furthermore, as discussed below, it is not clear that the information which comprises an individual's token identity is subject to the *Data Protection Act* or the *European Data Protection Directive.* By contrast, the right to identity clearly applies to token identity which is the information in the NIR in greatest need of protection in terms of its accuracy and its functionality. Unlike the right to privacy, in the context of the NIS, the right to identity protects an individual's right to have a unique token identity and to use it exclusively and, as discussed, the right to identity is not as readily subordinated to the public interest as the right to privacy.

It is against this background that this section examines the protection afforded by the right to privacy[236] to the information that comprises an individual's entry in the NIR. The protection afforded by privacy is limited in three key respects. First, the *Data Protection Act* and the *European Data Protection Directive* do not clearly apply to token identity. Secondly, while the right to privacy does protect the other Schedule 1 information which makes up an individual's database identity, in balancing the rights of the individual against the public

---

[235] See, for example, the exceptions in Pt IV and the exceptions on grounds of practicality in the data protection principles in sch 1 *Data Protection Act*.

[236] The European *Data Protection Directive* gives effect to the right to privacy. The Directive stipulates that 'personal data' must be collected 'fairly and lawfully' for 'specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.' Data collected must be 'adequate, relevant and not excessive' in relation to the purposes of collection and/or further processing. The data must be accurate, kept up to date and 'every reasonable step must be taken to ensure that data which are inaccurate or incomplete ...are erased or rectified.' The data must also not be kept in a form 'which permits identification of data subjects for any longer than necessary.' 'Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.' See, Art 6(a)-(e) *Data Protection Directive*.

interest, the latter is more likely to prevail than in a case involving the right to identity. Thirdly, in circumstances where an individual uses false biographical information to register under the scheme, the *Data Protection Act* and the *Data Protection Directive* can operate to facilitate the fraud. When each of these limitations is considered in detail below, it becomes clear that the right to privacy only applies to some of the information which comprises an individual's identity under the NIS, and that the individual only has privacy rights in respect of that information in some circumstances.

For example, if as a result of system error, another person is able to use an individual's registered token identity, that use infringes the individual's right to identity in the context of the NIS. As argued in this thesis, the right to identity cannot be abrogated on public interest grounds other than in extraordinary circumstances and the government cannot rely on the public service objectives of the scheme and dismiss such an error is an unfortunate but inevitable consequence of the scheme's design and operation.

By contrast, the right to privacy has limited application, and is largely ineffective in protecting an individual's transactional identity in the context of a national identity scheme like the NIS. If the individual instead asserts that the misuse has violated his or her right to privacy, there is firstly doubt whether privacy applies to an individual's token identity, especially under the *Data Protection Act* and the *Data Protection Directive.* Article 8 of the *ECHR* has been interpreted by the court as protecting an individual's right to privacy when there is systematic collection of information likely to affect an individual's reputation and less intrusive measures could be used but this right applies to the other Schedule I information, not token identity. Although that collection and use of personal information is usually not considered to be justified under Article 8(2) of the *ECHR*, an individual's privacy rights may be subordinated

to the public interest at a time of increased security concerns. Moreover, while privacy protects the other Schedule 1 information, where it is not clear that the individual is the data subject (as may be the case in the event of fraud, for example), the individual may not be able to rely on the rights of access to, and correction of, the record as provided by the *Data Protection Act* and the *Data Protection Directive*, with the consequence that errors may not be quickly discovered.

5.6.1. Token Identity is not Clearly Protected by Privacy

The *Data Protection Act* defines 'personal data' as:

> data[237] which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller,[238]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.[239] (emphasis added)

For the purposes of the European *Data Protection Directive*, 'personal data' is similarly defined as:

> …any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;[240] (emphasis added)

---

[237] 'Data' is defined in s 1 (1) (a) of the *Data Protection Act* to include 'information which is being processed by means of equipment operating automatically in response to instructions given for that purpose.' S 1(1) pts (b) – (e) extend the definition to recorded information and specifically includes 'recorded information held by a public authority.' S 1(1) *Data Protection Act* defines 'public authority' to mean 'public authority as defined by the Freedom of Information Act.'

[238] Under s 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.'

[239] See, s 1(1). The Australian *Privacy Act* defines 'personal information' in s 6 (1) in similar terms but refers to identity rather than identification.

[240] Art 2(a). The Data Protection Principles established by the *Data Protection Directive* are generally applied in the United Kingdom by the *Data Protection Act*. The *Data Protection Act* gives effect to the Directive and generally the Act follows the Directive but where there are differences, the latter usually provides more protection for the individual. In the event of clear inconsistency or ambiguity, the courts give direct effect to the Directive and will do so in applying Article 8 *ECHR*. The European Court has consistently asserted the supremacy of European Community law over domestic law. The Courts in the United Kingdom have accepted this position since the House of Lords decision in *R v Secretary of State for Transport ex parte Factorame* (No 2) [1991] 1 AC 603, though at times the English courts appear to stretch the bounds of reason to find that domestic

These definitions clearly contemplate a link between information like that constituting token identity[241] and a wider body of information such as that which makes up database identity.[242] The definition also contemplates a set of information like token identity as the gateway to the other information which constitutes an individual's database identity. Even though 'any information' can conceivably cover just token identity and even individual components of it, like an individual's name for example,[243] the definition clearly covers the personal information that constitutes database identity but not necessarily token identity.

The information which collectively constitutes an individual's database identity under the *Identity Cards Act* is within the definition in the *Data Protection Act* and the Directive, even on the narrow interpretation adopted in *Durant v Financial Services Authority*[244] ('*Durant*') in which the Court of Appeal held that the mere mention of a name in a document does not necessarily make it 'personal data.' The Court considered that the person who is the data subject must be the focus of the information, the information must be sufficiently biographical, and most importantly in the context of the present discussion, it must affect the

---

legislation is in accordance with the Directive, as occurred in *Durant v Financial Services Authority* [2003] EWCA Civ 1746, for example.

[241] And,a number that represents token identity. The number is used to reduce the time that is spent on a transaction conducted by telephone or internet, for example. When the number is entered, it brings up the information which collectively constitutes the individual's token identity. For a detailed discussion see, Australian Government, *Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007*, 25. A number was also planned for the NIS but this feature has been downplayed over the past few years.

[242] Compare the definition of 'personal information' in s 6(1) *Privacy Act* which is framed in terms of 'identity' not identification. 'Personal information' is defined as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose *identity is apparent, or can reasonably be ascertained, from the information or opinion.'* (Emphasis added). So the link between token identity and the broader body of information which makes up database identity, is clearer under the Australian legislation.

[243] See *Lindqvist v Sweden* [2003] ECR I-12971, 24 where the Court stated that '[t]he term undoubtedly covers the name of a person in conjunction with telephone coordinates or information about his working conditions or hobbies.' See also, *Roberson v Wakefield Metropolitan District Council and Another* [2002] 2 WLR 889, para 34 where in considering name and address under Art 8 of the *ECHR*, the court stated that rather than focusing only on the information, consideration should be given to what is known and anticipated about the use to which it will be put.

data subject's privacy.[245] The other Schedule 1 information, which includes for example, residential status and residency details,[246] personal reference numbers such as passport number for example, and security information, meets the criteria. An individual can also be identified from some of this information, even when it is considered in isolation from token identity.

However, the information which collectively constitutes token identity faces a couple of difficulties in meeting the *Durant* requirements. Name, gender, data and place of birth, date of death, signature and appearance may not be considered to affect the data subject's privacy. This information is necessarily public. Only the biometrics used in the NIS are not generally in the public domain in the sense that they are not usually recorded on publicly available registers.[247]

A fingerprint, facial contours and even features of the iris may be observable to the naked eye, but the precise measurements which are included in the recorded biometric are not publicly

---

[244] [2003] EWCA Civ 1746.

[245] While the motivations for the decision are understandable and it may indeed be the correct decision on the facts, its narrow interpretation of 'personal data' in section 1(1) flies in the face of European Community law, which has adopted a much wider approach. See for example, *Österreichischer Rundfunk v Austria*, [2003] ECR 4989, para 64. Cf *R v Rooney* [2006] EWCA Crim 1841 ('*Rooney*') Although *Rooney* may appear to contradict *Durant,* the reasoning is not necessarily inconsistent, nor does it necessarily reveal that the wider European approach is now being followed by courts in the United Kingdom. Rooney was convicted of an offence under s 55 of the *Data Protection Act* of disclosing personal information about individuals without the data controller's consent. On appeal, the defendant argued that disclosing information that the individuals lived in a specific town did not amount to disclosure of personal data as defined in the Act because it did not sufficiently identify the individuals or their address. However, the Court of Appeal upheld the conviction, finding that the 'information contained personal data' as required under s 55. The Court stated that in disclosing the information it was not necessary to identify the individual because the recipient of the information already knew the identity of that individual.

[246] In sch I *Identity Cards Act*, residential address is classified as 'personal information' as is name, gender date and place of birth, that is, the biographical information which constitutes token identity but s 1(5) distinguishes address and the other sch 1 information from 'identity.'

[247] Biometrics are not usually recorded on public registers and are not obvious to the casual observer as in the case of a person's face (as contrasted with a face scan), for example. The other information, that is, name, gender, date and place of birth and death is recorded on public register and can also be obtained from public sources such as notices in newspapers and even from tombstones. An individual's signature can also be obtained from publicly available documents. Although an image of a biometric like a fingerprint, can be observed during transmission for example, fingerprints, face and iris scans are not observable in the sense that the relative measurements of the features cannot be seen without the necessary equipment and interpretation skills.

available.[248] Unlike the other token identity information, the biometrics may therefore be considered private in that they are not recorded on a public register, nor can they usually be seen by a casual observer.[249] By their nature, biometrics can also be distinguished from the other token identity information. Assuming accuracy, biometrics are physiological measurements, that is measurements of physical characteristics of a person (albeit at a particular time), whereas the other elements of token identity can be said to be acquired by a person mostly at birth. However, even if the biometrics can be said to be private in nature on the basis of their intimate connection with the individual,[250] like the other token identity information, biometrics are not likely to be considered sufficiently biographical in nature. The token identity information may not meet this requirement even when considered as a set.

More stringent protection may possibly be available under the *Data Protection Act* if the information is 'sensitive' as defined in section 2.[251] Information is generally considered to be sensitive if it relates to the data subject's racial, or ethnic origin, political opinions, religious beliefs, trade union membership sexual life, alleged commission of an offence and/or

---

[248] Although, as technology becomes more sophisticated, biometrics are becoming easier to collect from public places.

[249] It may be argued that this is just a consequence of history and technical evolution. Name and signature for example, like biometrics, are also not obvious to a casual observer. Their use by a person makes them public. Historically, the establishment of key elements of identity such as name and handwritten signature, necessarily depended on public use and recognition; and that approach is still evident in the concept of identity established under the *Identity Cards Act*.

[250] For a case that discusses fingerprints see, *R v Chief Constable of South Yorkshire Police ex parte LS and Marper* [2002] 1 WLR 3223 where it was common ground that the taking of fingerprints and DNA samples is an interference under Art 8(1) even though the invasion of bodily integrity is minimal. It was also common ground that the use of the information derived from them, is interference because the information is regarded as intrinsically private. However, the majority of the court held that in the circumstances of the case the interference caused by retention of the samples was justified under Art 8(2).

[251] Under both the *Data Protection Act* and the *Data Protection Directive*, 'explicit consent' of the data subject is required for the processing of 'sensitive personal data.' See Art 8 *Data Protection Directive* and sch 3 para 1 *Data Protection Act.* The Directive and the Act do, however, permit processing when necessary to 'protect the vital interests of the data subject *or another person'* when consent of the data subject cannot be obtained or is unreasonably withheld. (emphasis added) See, Art 8(2)(c) *Data Protection Directive* and para 3, sch 3 *Data Protection Act.* The question is whether 'vital interests' are involved. The Act also permits processing that is necessary for the administration of justice and for the exercise of any functions conferred on a person by an enactment. See, sch 3 para 7 *Data Protection Act. Data Protection Act.* See, also Art 8(4)-(6) *Data Protection Directive*. Recall also that Art 8(7) *Data Protection Directive* states that: 'Member States shall determine the

proceedings for any offence. However, in the United Kingdom it also includes information as to the data subject's 'physical or mental health or condition.'[252]

The biometrics used in the NIS may possibly be considered information about the data subject's 'physical ...condition,' so as to afford additional protection to the processing[253] of biometric information. Considering the crucial role biometrics play in both authentication and verification of identity under the scheme, biometrics are indeed especially sensitive for individuals. Under the NIS, biometrics 'unequivocally'[254] connect an individual to his /her token identity and hence to his /her database identity. It may also be argued therefore that all the information which collectively constitutes identity should be considered as an indivisible set, and afforded additional protection as 'sensitive information.' However, while it may be appealing to consider biometrics and indeed, token identity as sensitive information under the *Data Protection Act*, the inclusion of 'physical' in the United Kingdom legislation is an anomaly.[255] Bearing in mind that domestic legislation is to be interpreted in line with the Directive,[256] clearly the original intention was to give extra protection to health information.[257] Even considering the expansive and surprising interpretation of 'health information' within Article 8(1) of the Directive by the European Court of Justice in *Bodil Lindqvist,*[258] to

---

conditions under which a national identification number or any other identifier of general application may be processed.'

[252] See s 2(e) *Data Protection Act*.

[253] 'Processing' is widely defined in s 1(1) *Data Protection Act* to mean "obtaining, recording, or holding" and specifically covers 'organization, adaptation, or alteration,' 'retrieval, consultation, or use,' and disclosure by 'transmission, dissemination or otherwise making available,' and also 'alignment, combination, blocking, erasure or destruction.' See, pts (a)-(d).

[254] Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/schemehtml>at 10 May 2006. For a more recent statement to the same effect, see Identity and Passport Service, *What is the National Identity Scheme* <http://www.ips.gov.uk/identity/scheme-what-produced.asp> at 1 September 2008.

[255] Cf the definition of 'health information' s 6(1) Australian *Privacy Act.*

[256] See *Von Colson and Kamann v Land Nordrhein-Westfalen* (Case 14/83) [1984] ECR 1891, *Marleasing SA v La Commercial International de Alimentatcion SA* (Case C-106/98) (1990) ECR 1-4135 and *Wagner Miret v Fondo de Guarantia Salaria* (Case C-334/92) [1993] ECR 1-6911.

[257] Art 8(1) *Data Protection Directive* refers to "health or sex life." See, Douwe Korff, *EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws* (2002), 85.

[258] EU Court of Justice Dec C101-01. See, *Lindqvist v Sweden* [2003] ECR I- 12971.

categorise fingerprints, a face scan and iris scans, let alone token identity, as health information would certainly be a strained interpretation.

In summary, it is clear that the *Data Protection Act* and the *Data Protection Directive* apply to the other Schedule 1 information which makes up database identity. However, it is unclear, and in fact doubtful, that the Act and Directive apply to token identity when it is considered separately from that other Schedule 1 information. Because the right to privacy does not clearly apply to token identity, even the relatively limited protection provided by the rights of access, correction and notation, and in some circumstances to be informed of the use and disclosure of that information, do not necessarily apply to token identity. This outcome is not surprising considering that the information which comprises token identity is largely in the public domain but it does not take into account that, as a collective, that information takes on distinct legal character and performs specific functions under the NIS, especially at the time of a transaction.

5.6.2. The Protection Afforded to Database Identity

As discussed in chapter 2, the information recorded in an individual's entry in the NIR is augmented on an on-going basis. Information collected when an individual's record in the NIR is accessed by organisations using the scheme to verify identity, becomes part of an individual's database identity. Opinions and notes added to the record also become part of database identity. Even information which appears to be largely administrative and innocuous such as 'validation information'[259] and especially 'records of provision of information'[260] can

[259] 'Validation information' includes steps taken and information obtained in identifying the applicant and verifying information provided in connection with an application to be registered on the NIR and for ensuring that the entry is 'complete, up-to-date and accurate.' See, sch 1 pt 7 *Identity Cards Act.*

give the impression that an individual is being investigated and is under suspicion. All the information adds to the narrative about an individual and to his or her reputation in the context of the scheme. Inaccuracy as a result of errors or gaps in the information can affect how an individual is regarded by the system and by other people.

While the right to identity can be invoked to protect an individual's registered token identity from inaccuracy and use by another person, the other Schedule 1 information recorded about an individual in the NIR, is more appropriately protected by the right to privacy. The right to privacy relates to undesired collection disclosure and use of personal information, about an individual, whereas the right to identity applies to the untrue or false use of indicia of identity, that is token identity. An individual's right to privacy is infringed by the association of personal facts, contrary to the wishes of the individual.

The right to privacy entails rights of access to the individual's entry in the NIR, rights of correction and of notation and the right to be informed of, and to an extent, control the use and disclosure of the information. As the following review of the decisions of the European Court reveal, in balancing the privacy interests of the individual against the broader public interest in accordance with Article 8(2) of the *ECHR*[261] the power of the State is curtailed when an

---

[260] This information is specified as 'particulars of every occasion on which information contained in an individual's entry has been provided to a person,' 'particulars of every person to whom such information has been provided on such an occasion' and 'other particulars, in relation to such an occasion, of the provision of the information.' See sch 1 pt 9 *Identity Cards Act*.

[261] The other Article referred to in relation to privacy is Art 10 which covers the countervailing right to freedom of expression. This Article is often considered in balancing broader public interests with an individual's right to privacy. In relation to information such as that which makes up database identity, the European Court has stated that,'[t]he court observes that the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish to impart to him. Art 10 does not, in circumstances such as those of the present case, confer on the individual a right of access to a register containing information on his personal position, nor does it embody an obligation on the government to impart such information to the individual.' See, *Leander v Sweden* (1987) 9 EHRR 433. *Gaskin v United Kingdom*, (1990) 12 EHRR 36 confirmed this view, stating that '[t]he Court holds, as it did in *Leander v. Sweden*, that 'the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him. Also in the circumstances of this case, Article 10

individual's reputation is besmirched and where other less intrusive means could be used to achieve the public interest objectives.

In considering the application of Article 8, in relation to privacy, the court in *Peck* stated that, '[p]rivate life considerations may arise once any systematic or permanent record comes into existence of such material from the public domain.'[262] Systematic collection and storage by the government infringes Article 8(1) and the European Court has held that, '[t]hat is all the truer where such information concerns a person's distant past'[263] and where some of the information on record is 'false and is likely to injure the applicant's reputation.'[264]

---

does not embody an obligation on the State concerned to impart the information in question to the individual.'(sic) It is also now settled that neither Article 8 nor Article 10 takes precedence over each other. See, *In re S (a child)* [2005] 1 AC 593.

[262] Above n 191, para 57, citing *PG and JH v United Kingdom* ECHR 2001-IX, paras 57 and 59 where the Court stated that '[t]he monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life (see, for example, *Herbecq and Another v Belgium*, applications Nos 32200/96 and 32201/96, Commission decision of January 14, 1998, DR 92-A, p.92). On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations. Accordingly, in both the *Rotaru* and *Amann* judgments (to which the P.G. and J.H. judgment referred) the compilation of data by security services on particular individuals even without the use of covert surveillance methods constituted an interference with the applicants' private lives (*Rotaru v Romania* [GC], No.28341/95, §§43-44, ECHR 2000-V, and *Amann v Switzerland* (2000) 30 EHRR 843,65-67).' In *Amann v Switzerland* the European Court reiterated 'that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. See, *Amann v Switzerland* (2000) 30 EHRR 843, 69. The subsequent use of the stored information has no bearing on that finding.' These decisions have recently been confirmed by the European Court in *Segerstedt –Wiberg v Sweden* (2007) 44 EHRR 2.

[263] *Rotaru v Romania* (28341/95) 8 BHRC 449 where an intelligence service file on the applicant listed him as a University student when he was still at school, specified a different faculty from the one he subsequently joined and wrongly classified him as a member of an extreme right-wing organization. Some of the information had been gathered more that 50 years earlier.

[264] Ibid, para 43. A provision similar to Art 8 of the *ECHR* can be found in Art 9 of the French *Code Civile* which states that: 'Everyone has the right to respect for his private life.' J Hauch writes that it protects 'the right in one's name, one's image, one's voice, one's intimacy, one's honour and reputation, one's own biography, and the right to have one's transgressions forgotten.' See, J Haunch, 'Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris' (1994) 68 *Tulane Law Review* 1238, n 89 citing the Judgment of 15 May 1970, Cour d'appel de Paris, 1970 DS Jur 466, 468. See also, E Picard, 'The Right to Privacy in French Law' in B S Markes (ed) *Protecting Privacy* (1999) 49, 51-52. Art 9 has also been interpreted by the French courts as extending to the health of an individual, his or her close family, private repose and leisure, parental and marital status, family life and intimate interpersonal relations and sexual orientation, way of life in general, inner emotions, political and religious beliefs and significantly (especially in the context of database identity, including token identity) true names and residences. See J. Haunch, 'Protecting private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris' (1994) 68 *Tulane Law Review* 1238, 1247, n134; 1247, n 137; 1248, n 139-142 and n 145; 1254, n 181 and 1246,125. Article 9 has also been

The main consideration is the unnecessary collection and storage of information like the information which collectively comprises database identity. However, to establish 'interference' under Article 8(1) it may also be necessary for the information to be disclosed to a third party.[265] Disclosure to a public authority without the individual's consent as permitted under the *Identity Cards Act,*[266] is an interference within the meaning of Article 8 (1).[267]

Having established threshold interference under Article 8(1), it then becomes a question of whether there is justification under Article 8(2). The *Identity Cards Act* and the NIS clearly contemplate that the data protection principles should apply to the information in the NIR–to an extent. The wording of Article 8(2), particularly in relation to necessity, is closely followed in the *Identity Cards Act* in the sections which authorise provision of information recorded in an individual's entry in the NIR without the individual's consent.[268]

Section 17 of the *Identity Cards Act* permits the Secretary of State to provide information recorded in an individual's entry to a range of security and law enforcement bodies. Most of the subsections authorise disclosure 'in the interests of national security,' 'for the prevention or detection of crime' or when 'necessary in the public interest.'[269] 'Something necessary in

---

held to extend to the deceased, most notably President Mitterrand. See, E. Picard, 'The Right to Privacy in French Law' in B S Markes (ed) *Protecting Privacy* (1999), 49, 80-81.

[265] See, *Amann v Switzerland* (2000) 30 EHRR 843, para 69, and *Leander v Sweden* (1987) 9 EHRR 433, para 48.

[266] See, ss 17-21.

[267] See, *Österreichischer Rundfunk v Austria* [2003] ECR 4989, 74. Also note that in *X v Federal Republic of Germany* Appl. No. 5877/72 YBXVI (1973) 328,388 the fact that information collected about an individual who did not have a criminal record, was not disclosed to anyone was a crucial factor in the finding that Article 8 was not infringed.

[268] See, s 18 which authorizes disclosure of information including (under sub-s (4) information falling within para 9, sch 1) to 'a person' for criminal proceedings and investigations under the statutes specified in that section. See also, s 20 which permits disclosure to a public authority where there is no authorisation under ss 17-19. S 20(2) specifies that it must be 'necessary in the public interest.'

[269] S 17(3)(c) authorises provision of information to a chief officer of police 'for other purposes specified by order made by the Secretary of State' but sub-s (7) requires that it 'must be necessary in the public interest.' S 7(8) requires that a draft of the order or of regulations must be approved by resolution of each House of Parliament.

the public interest' is defined in section 1(4) to cover national security and prevention and detection of crime as stated in Article 8(2). The definition in the *Identity Cards Act* also extends to enforcement of immigration controls, enforcement of prohibition of unauthorised employment[270] and 'for the purpose of securing the efficient and effective provision of public services.'

However, disclosure under section 19 is not specifically restricted to national security, crime and public interest purposes. The section deals with information 'which appears to the Secretary' to be inaccurate or incomplete and authorises disclosure of the individual's entry 'in respect of the matters to which the inaccurate or incomplete information related.'[271] It also seems that disclosure under section 17(5) is not specifically restricted to national security, crime and public interest purposes. It authorises information not falling within paragraph 9 of Schedule 1[272] to be provided to a government department 'for purposes connected with the carrying out of any prescribed functions of that department or of a Minister in charge of it.'[273] Disclosure of information comprising database identity, including token identity, under these provisions may therefore not be justified under Article 8(2), having regard to the right to privacy, let alone to the right to identity.

Provision of information under sections 17 and 19 is subject to compliance with 'requirements imposed by or under section 21.' Section 21 empowers, but does not require, the Secretary to

---

[270] Immigration and labour controls also raise issues of restriction of movement and employment within the European Community. See, Colin Harvey and Robert Barnidge, 'Human Rights, Free Movement, and the Right to Leave in International Law (2007) 19 (1) *International Journal of Refugee Law*, 1 and Frances Conte, 'Sink or Swim Together: Citizenship, Sovereignty, and Free Movement in the European Union and the United States' (2007) 61 *University of Miami Law Review* 331.

[271] 'The reference to providing information about an individual for verification purposes' in s 19 is widely defined in s 19(4).

[272] This paragraph is entitled 'Records of provision of information.'

make regulations specifying the categories of persons who are entitled to apply for the provision of information under sections 17-20, persons to whom information may be provided including provision to 'another person,' and conditions that may be imposed. Section 21(2) states that the Secretary *may* by regulations impose 'requirements that must be satisfied before information is provided under sections 17-20.' (emphasis added)[274] but does not contain any more detail. The discretion given to the Secretary in making regulations and the apparently limited nature of those regulations is of concern and may not be justified under Article 8(2) of the *ECHR*.

The phrase 'in accordance with the law' in Article 8(2) of the *ECHR* has been interpreted by the European Court to imply conditions which go beyond the existence of a legal basis in domestic law and requires that the legal basis be 'accessible' and 'foreseeable.'[275] What this means is clarified in *Malone v The United Kingdom* ('*Malone*'):[276]

> The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention …The phrase thus implies-and this follows from the object and purpose of Article 8-that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph (1) …Especially, where a power of the executive is exercised in secret, the risks of arbitrariness are evident…[277]

The European Court considers the consequences for an individual whose rights are infringed by legislation like the *Identity Cards Act* and a scheme like the NIS, and the specified

---

[273] S 17(7) requires that the power for the Secretary to make an order or regulations 'authorising the provision of information to a person' must only be exercised in circumstances when the provision is 'necessary in the public interest.' However, it is not clear that an order or regulations are required for disclosure under s 17(5).

[274] However, s 21(1) only permits 'identifying information' which is the individual's biometrics, face and iris scans, photograph and signature to be provided to a person if the Secretary is 'satisfied that it would not have been reasonably practicable for that person to have obtained that information by other means.'

[275] *Amann v Switzerland* (2000) 30 EHRR 843, para 57.The expression in 'accordance with the law' in Art 8(2) of the *ECHR* requires that the interference must have some basis in domestic law. Moreover, the law in question must be accessible to the individual concerned and its consequences for him or her must also be foreseeable.

[276] (1985) 7 EHRR 14.

[277] Ibid para 67.

precautions taken to safeguard those rights. In *Amann v Switzerland* ('*Amann*'),[278] for example, a Swiss businessman was 'fortuitously' caught by telephone surveillance of calls from the Union of Soviet Socialist Republics embassy, and a card relating to him was held in the national security card index. The Court found that the primary object of the legislation under which the surveillance was conducted was the surveillance of persons suspected or accused of criminal activity,

> …or even third parties presumed to be receiving information from or sending it to such persons …but the Act does not regulate in detail the case of persons monitored fortuitously… In particular, the Act does not specify the precautions which should be taken with regard to those persons.[279]

The Court concluded that the interference was not 'in accordance with the law' since 'Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration.'[280]

This finding relates to 'foreseeability' in Article 8 (2), in relation to which the court in *Malone* stated that:

> Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.[281](emphasis added)

Peck also addresses this point:

> In cases concerning the disclosure of personal data, the court has also recognised that a margin of appreciation should be left to the competent national authorities in striking a fair

[278] (2000) 30 EHRR 843.
[279] Ibid para 61.
[280] Ibid, para 62.
[281] Above n 276, para 67.

> balance between the relevant conflicting public and private interests. However, this margin goes hand in hand with European supervision (Funke v France, judgment of February 23, 1993, Series A No.256-A, §55) and the scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference (Z.v Finland, judgment of February 25, 1997, Reports of judgments and Decisions 1997-I, §99).[282]

In findings which are directly relevant to the protection of information recorded under the NIS, the court found in that case that the CCTV surveillance footage of Peck was 'in accordance with the law'[283] in that it was permitted by domestic law.[284] The court also accepted the role of CCTV in preventing crime but the crucial question was whether the interference in Peck's 'private life' was 'necessary in a democratic society.'[285] In addressing this question, the court noted that the footage did not disclose the commission of an offence, and went on to state:

> The Court has also noted, on the one hand, the nature and seriousness of the interference with the applicant's private life (para [63] above). On the other hand, the Court appreciates the strong interest of the State in detecting and preventing crime. It is not disputed that the CCTV system plays an important role in these respects and that that role is rendered more effective and successful through advertising the CCTV system and its benefits. [286]

---

[282] Above n 191,para 77. The Court went on to state that '[t]he above-cited *Z v Finland* judgment related to the disclosure in court proceedings without the applicant's consent of his health records including his HIV status. The court noted that the protection of personal data was of fundamental importance to a person's enjoyment of his or her right to respect for private life and that the domestic law must therefore afford appropriate safeguards to prevent any such disclosure as may be inconsistent with the guarantees in Art.8 of the Convention. In so finding, the court referred, mutatis mutandis, to Arts 3 §2 (c), 5, 6 and 9 of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (European Treaty Series No.108, Strasbourg, 1981). It went on to find that the above considerations were 'especially valid' as regards the protection of the confidentiality of information about a person's HIV status, noting that the interests in protecting the confidentiality of such information weighed heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued. Such interference could not be compatible with Art.8 of the Convention unless it was justified by an overriding requirement in the public interest. Any State measures compelling disclosure of such information without the consent of the patient and any safeguards designed to secure an effective protection called for the most careful scrutiny on the part of the court.'

[283] Art 8(2) ECHR.

[284] Above n 191, paras 66-67, where the Court found that the interference with the applicant's private life was in accordance with the law because it fell within s 163 *Criminal Justice and Public Order Act 1994* (UK) c 33 and s 111 of the *Local Government Act 1972* (UK) c 70. 'Accordingly, the court considers that the disclosure did have a basis in law and was, with appropriate legal advice, foreseeable (*The Sunday Times v The United Kingdom* (No.1), judgment of April 26, 1979, Series A No.30, §49). It also regards the disclosure as having pursued the legitimate aim of public safety, the prevention of disorder and crime and the protection of the rights of others.'

[285] Art 8(2) ECHR.

[286] Above n 191, para 79.

However, the Court considered that other options were available that could achieve the same objectives[287] and found that under the circumstances, 'the disclosure constituted a disproportionate and therefore unjustified interference with his private life and a violation of Article 8 of the Convention.'[288]

As to whether the same view will be adopted by a court in relation to the NIS, there are a number of considerations. The scheme can infringe on an individual's 'private life', as interpreted by the European Court and the broader body of information which comprises database identity is clearly protected by the right to privacy. However, the stated public interest purposes of the NIS which include national security and crime prevention and detection, as well as 'securing the efficient and effective provision of public services,'[289] will be balanced against the impact on individual privacy. Moreover, as far as data protection is concerned, disclosure of information under section 19, and probably also under section 17(5) of the *Identity Cards Act*, is not clearly specified to be limited to interference necessary to protect national interest. This aspect, coupled with the discretion given to the Secretary in these provisions and in relation to the making of limited regulations, could result in an infringement not being justified under Article 8(2). Such a finding would also mean that the *Identity Cards Act* and the *Data Protection Act* are incapable of satisfying the proportionality requirements of the Directive.

The right to privacy therefore generally provides reasonable protection in relation to the other Schedule 1 information recorded in the NIR because the balancing of individual interests against broader societal interests usually keeps the power of the State in check. However, at a

---

[287] Including obtaining the applicant's consent, or ensuring that the images were masked.

[288] Above n 191, para 87. For a recent decision in the same vein see, *Copeland v United Kingdom* [2007] 45 EHRR 37.

time of heightened security concerns such as may exist immediately following a terrorist attack for example, the public interest objectives of a scheme like the NIS may be considered to outweigh the impact on an individual's right to privacy.

5.6.3. Who is the Data Subject?

There is another issue which can arise under the NIS that affects the protection afforded by privacy to the other Schedule 1 information which comprises database identity. Consider a situation in which the biographical information of an individual is used by another person to register a false identity under the NIS. At the time of registration, the latter's biometrics are then 'sealed to or permanently paired'[290] with biographical information which is not authentic to him.[291]

If the fraudster is subsequently required to provide biometrics to establish his identity either for transactional purposes or as part of an investigation, the biometrics will match those recorded in the NIR. One would expect the British authorities to counter that this person could

---

[289] S 1(4).

[290] Identity and Passport Service, What is the National Identity Scheme? <http//:www.identitycards.gov.uk/scheme.html> at 10 May 2006. See also, Identity and Passport Service, What is the National Identity Scheme? <http//:www.ips.gov.uk/identity/scheme-what-produced.asp> at 1 September 2008.

[291] It is also conceivable that biometrics obtained from an individual could be attached to the record of another individual as a result of processing error, system error or even through unauthorized manipulation of information in the NIR. Considering the number of registrations required under the scheme and the on-going updating that will be required, data processing errors are certainly possible and are probably likely. Biometrics can also be relatively easily obtained from a database or during transmission. If a fingerprint, iris or facial scan is obtained, it can be replicated. 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. Indeed, the replica can then be attached almost invisibly so as to verify identity when using a biometric reader. Increasingly, readers are designed to detect blood flow but this can also be replicated. If the biometric is verified using the Internet, deception can be even easier. For further discussion of these aspects see, Clare Sullivan, 'The United Kingdom Identity Cards Act 2006-Proving Identity?' (2006) 3 *Macquarie Journal of Business Law* 259.

not be registered in the first place but the possibility of a false identity being created and used in this way has been acknowledged by the Home Secretary.[292]

This situation can have serious consequences, considering the purposes of the scheme. Section 1(3) specifies the purposes of the NIS as,

> ...to facilitate, by maintenance of a secure and reliable record of registrable facts about individuals in the United Kingdom–
>
> (a)the provision of a convenient method for such individuals to prove facts about themselves to others who reasonably require proof; and
> (b)the provision of a secure and reliable method for registrable facts about individuals to be ascertained or verified wherever that is necessary in the public interest.

When these purposes are considered in terms of identity, the implications become apparent.The first purpose is to provide a convenient method for an individual to prove his/her identity.[293] This purpose has the unintended consequence of assisting the perpetrator in the scenario above, in proving the false identity. As to the second stated purpose, section 1(4) states that 'something is necessary in the public interest if and only if it is' in the interests of national security, for prevention or detection of crime, to enforce immigration controls, to enforce prohibition on unauthorised working or employment or for 'securing the efficient and effective provision of public services.' This requirement seems to be specifically designed to cover the conditions for the processing of personal data without the consent of the data subject, as set out in the *Data Protection Act*.[294]

---

[292] Home Secretary, *IPPR Speech* 18 November 2004 <http//:www.identitycards gov.uk.html> at 16 May 2006. The Home Secretary maintained though that '[t]here can't be 2 people with the same biometric on the same database claiming to be the same person.'

[293] Recall that 'identity' is included in the definition of 'registrable fact in relation to an individual' in s 1(5) *Identity Cards Act*. S 1(7) *Identity Cards Act* states that: 'In this section references to an individual's 'identity' are references to 'his full name,' 'other names by which he is or has previously been known', date and place of birth, date of death and 'external characteristics of his that are capable of being used for identifying him.'

[294] See, para 5(d), sch 2 *Data Protection Act*. The 'consent' of the data subject is not required if the processing is necessary 'for the exercise of any other functions of a public nature exercised in the public interest by any person,' though the processing is probably also covered by parts (b) and (c) of para 5 of sch 2. See also, sch 3 para 2(1) which permits processing of 'sensitive personal data' to comply with law 'in connection with employment.' Most importantly, sch 4 para 4 permits transfer of data when 'necessary for reasons of substantial

An individual whose biometrics are recorded in the NIR is 'a living individual who can be identified' in accordance with the definition of 'data subject.' Section 1(1) of the *Data Protection Act* defines the 'data subject' as 'an individual who is the subject of personal data.' Recall that 'personal data' is defined in section 1(1) to mean 'data which relate to a living individual who can be identified' from the data/information and that under Article 2 of the *Data Protection Directive* refers to 'an identified or identifiable natural person' as the data subject.[295]

If identification for the purposes of the definition of 'data subject' in the *Data Protection Act* and the *Data Protection Directive* depends on the biometrics, the fraudster will be considered a data subject under both the Act and the Directive and probably, *the* data subject under the *Data Protection Act.*[296] Even if all the biographical information recorded relates to another person, that person may not be considered the subject of that personal data/information. This is especially so under the *Data Protection Act* following the controversial, narrow interpretation adopted in the *Durant*.[297] The decision in that case was clearly influenced by the need to protect disclosure of information relating to an individual without that person's consent 'unless it would be reasonable in all the circumstances for him to have it without that consent,[298] and the decision has been criticised. However, the result is that conflicting rights are likely to be decided in the fraudster's favour, at least initially. That person's biometrics are

---

public interest.' Neither 'public interest,' nor 'substantial public interest' is defined in the *Data Protection Act*. See also, the *Data Protection Directive*.

[295] In Australia, s 6 *Privacy Act* defines 'individual concerned, in relation to personal information or a record of personal information' to mean 'the individual to whom the information relates.' The Australian *Privacy Act* does, however, define 'personal information' in terms of 'identity' although 'identity' is not defined.

[296] This is also the case in Australia under the *Privacy Act.*

[297] Above n 244.

[298] Above n 244,7. The Court of Appeal was influenced by the fact that Durant was attempting to obtain information previously denied him as part of the discovery process during litigation, as well as by the need to protect third parties. See also, s 7(4) *Data Protection Act*.

recorded in the NIR and biometrics are regarded as unique identifiers under the scheme. Constraints are also imposed on the data controller complying with a request by a person to be informed as to whether his or her personal data is being processed if compliance involves disclosure of information relating to another person.[299]

Irrespective of whether this situation is the result of fraud, negligence or system malfunction, the individual whose biographical information is recorded may not be considered to have the rights of a data subject under the *Data Protection Act* and the Directive. Those rights include the right to know whether the data controller is processing any of his or her personal data, and to be told what information is being processed, its source, why it is being processed; and to whom the information is, or may be, disclosed.[300] As discussed, the individual also has rights to correct and notate the record. However, in a classic 'catch-22' situation, the exercise of these rights depends on the individual knowing what personal information is being processed and how it is being processed.[301] In effectively screening this information from scrutiny, the *Data Protection Act* and the *Data Protection Directive* can prevent or at least delay its discovery.

It is important to note that in this situation, the right to identity does not protect the individual. An individual does not have an exclusive right to components of identity such as name, date of birth or photograph. Individual rights to biometrics like fingerprints and face or iris scans in this context are also not yet recognised. Misuse of some of this information by another person

---

[299] See, for example, s 7 (4), sch 2 paras 5 and 6, and sch 3 paras 3 and 4 *Data Protection Act.* See also, s 7(3) *Data Protection Act* While there are a number of sections in the *Data Protection Act* which can be invoked, in the absence of grounds for suspicion of identity fraud, or even when there is a suspicion but there is doubt about who is the perpetrator and who is the victim, the situation can place the data controller in a very difficult position. The same issues apply in Australia under the *Privacy Act*.

[300] S 7(1). See also, *Durant* above n 244, 7.

[301] See the comments of Laddie J in *Johnson v Medical Defense Union Ltd* [2005] WLR 750, 19. See also, *Johnson v The Medical Defense Union* [2007] EWCA 262.

is therefore not use of an individual's identity and it does not amount to interference with the right to identity. The important point, however, is that although neither the right to identity nor the right to privacy effectively protect the information in this situation, the *Data Protection Act* and the Directive can operate to facilitate its misuse by another person.[302]

5.7. Conclusion

To date, legal scholarship and jurisprudence have focused on the law of privacy to protect personal information. However, the protection provided to an individual by the right to privacy is inadequate and inappropriate in the context of identity under the NIS.

The NIS is subject to the *Data Protection Act* and the *Data Protection Directive*, but the *Identity Cards Act* gives considerable discretion to the government particularly in relation to information disclosure, and is largely silent as to individual protections and rights. The problem is compounded by the fact that the *Data Protection Act* and the Directive do not clearly protect token identity and, indeed, can operate to shield fraud, negligence and system malfunction from scrutiny. Moreover, if an individual invokes his or her right to privacy in relation to the other Schedule 1 information, the interests of the individual must be balanced against those of the broader community.

---

[302] As can the Australian *Privacy Act*. Lynn LoPucki makes a similar point in relation to privacy under United States law and its impact on identity crime in that country. See, Lynn M, LoPucki, 'Did Privacy Cause Identity Theft?'(2002-2003) 54 *Hastings Law Journal* 1277. See also Lynn M, LoPucki, 'Human Identification Theory and the Identity Theft Problem' (2001- 2002) 80 *Texas Law Review* 89. See also, Daniel Solove, Identity Theft, Privacy and the Architecture of Vulnerability (Enforcing Privacy Rights Symposium)' (2003) 54 *Hastings Law Journa*l, 1227, Daniel Solove, 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure' (2003) 53 *Duke Law Journal* 967 and Daniel Solove, 'Power and Privacy: Computer Data Bases and Metaphors for Information' (2001) 53 *Stanford Law Review* 1393.

This thesis argues that in the context of the NIS, the right to identity is the right of an individual to an accurate, functional, unique token identity and to its exclusive use. As argued in this chapter, the right to identity, if recognised in the context of the NIS, provides greater protection and more appropriate protection, to an individual's registered token identity than the right to privacy.

Unlike privacy, the right to identity clearly protects token identity. The public interest may be considered to outweigh individual privacy interests under Article 8(2) of the *ECHR*, especially at a time of increased security concerns. However, infringement of an individual's right to identity especially in the context of a national identity scheme like NIS is unlikely to be justified under Article 8(2) except in extraordinary circumstances, because to do so gives the State power to disenfranchise an individual–in effect, to render him or her, a non-person under the scheme.

This aspect and its consequences for an individual illustrate the need for a national identity scheme like the NIS and the ACS to be established within a national human rights regime that recognises and protects individual rights including the right to identity as well as the right to privacy. The *ECHR* offers additional protection to an individual in a situation where the State has considerable power to affect the way an individual is regarded and how he or she is treated under the scheme. This point is particularly important for Australia.

Under the *ECHR*, the legal protection provided by domestic law is a significant consideration in determining whether an *ECHR* right is respected. The protection which can be provided to the emergent concept of identity, and especially to token identity, under private law is currently limited, essentially because of the nature of digital identity. As a result, the

protection afforded to token identity and to identity information by the criminal law becomes especially significant. The European Court has observed in relation to Article 8 that 'effective deterrence against grave acts…where fundamental values and essential aspects of private life are at stake, requires efficient criminal law provisions.'[303]

Although a United Kingdom resident clearly has redress against the government for a breach of his or her human rights, this is just one facet of the overall situation. If, for example, a fraudster uses an individual's token identity, or undermines the integrity of the scheme by using false identity information, criminal law sanctions and attendant victim's rights, including compensation, should apply. The protection of identity and identity information by the criminal law in the United Kingdom and in Australia is therefore considered in the next chapter.

[303] *MC v Bulgaria* (2005) 40 EHRR 20, para 150. This case concerned a rape that occurred in a domestic situation but the sentiments of the court can apply to any grave act where fundamental rights are at stake: The full statement made by the court is that '[p]ositive…obligations on the State are inherent, in the right to effective respect for private life under Article 8: these obligations may involve the adoption of measures even in the sphere of relations of individuals between themselves. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is in principle within the State's margin of appreciation, *effective deterrence against grave acts* such as rape, *where fundamental values and essential aspects of private life are at stake, requires efficient criminal law provisions*. Children and other vulnerable individuals, in particular, are entitled to protection.'(emphasis added).

6. Digital Identity – Protection

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 crime, 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 are going to do it to you. I am not Ruth Marx. They invented her and put her on the computer with my thumbprint.'[304]

6.1. Introduction

This chapter considers the protection afforded by the criminal law to token identity. The analysis builds on the examination of the functions and legal nature of token identity in chapters 2 and 3, the examination of the inherent vulnerabilities of the identifying information in chapter 4, and the human rights implications considered in chapter 5. Against this background, the protection afforded to an individual's token identity in the context of a national identity scheme assumes considerable significance.

The argument in this chapter is that dishonest misuse of an individual's registered token identity by another person should be considered theft of identity. This approach accurately describes the nature of the wrong and the consequences for the individual whose identity is misused by another person. Unlike the general fraud offences, theft designates that individual as the victim of the crime.

[304] '*The Net*' Columbia Pictures Industries Inc (1995).

The general fraud offences apply to a range of fraudulent activities and apply in the context of a national identity scheme where an individual's token identity is dishonestly used with intent to make a financial gain or loss.[305] However, although these offences are wide ranging, in the context of such a scheme, token identity is used for many types of transactions, not just those of a financial nature. The argument in this chapter is that the wrong is the unlawful use of an individual's registered token identity by another person. That misuse should be the offence, regardless of whether the use is with intent to make a financial gain or cause a financial loss.

The new offences in the *Identity Cards Act* address fraud at the time of registration, but they do not cover misuse by another person of an individual's token identity after registration. Consequently, there is a gap in the protection currently provided by the law which can be filled by the theft offence. Treating misuse of another individual's token identity as theft rather than fraud recognises that the essence of the offence is appropriation of identity and that the individual is the primary victim of that wrong.

Section 1(1) of the United Kingdom *Theft Act* sets out the basic definition of theft:

> A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and "thief" and "steal" shall be construed accordingly. [306]

This thesis argues that misuse of an individual's registered token identity by another person for a transaction is capable of meeting all of the elements required for theft. Central to this argument is that token identity is a form of intangible property. Misuse by another person constitutes an appropriation with intent to permanently deprive the individual of his or her

---

[305] See for example, s 2 *Fraud Act* which makes it an offence to dishonestly make a false representation with intent to make or cause a loss. S 5(2)(a) defines 'gain' and 'loss' in terms of 'money or other property.'
[306] The theft offence in the Australian federal *Criminal Code* contains the same elements. See, s 131.1(1).

ownership of that property in that the misuse is a dealing in disregard of the individual's right to exclusive use and control of his or her token identity.

This chapter takes issue with the view recently reiterated by the Model Criminal Law Officers Committee ('MCLOC') in its Final Report on Identity Crime that,

> [t]he phrase 'identity theft' is a misnomer, as identity theft does not actually deprive a person of their identity. The offence of theft or larceny traditionally involves an appropriation of the personal property of another with the intention to deprive him or her of that property permanently. Wrongfully accessing and using a person's personal information or forging proof of identity documents, without taking any physical document or thing, would not deprive the person of the ability to use that information.[307]

In the context of a scheme like the NIS this view is fallacious. Deprivation of use is not a requirement for theft and the view of the MCLOC is based on the long-held assumption that information is just information, so that its appropriation cannot possibly cause permanent deprivation. But as this thesis contends, an individual's transactional identity under the NIS is more than just information. As discussed in previous chapters, token identity has specific functions under the scheme which give it legal character. It is against that background that this chapter argues that registration gives token identity the characteristics of property which is capable of being misappropriated-and damaged.

Recognising that token identity is property also enables the offence of criminal damage to apply to misuse in circumstances where a person intends to cause damage or is reckless. The offence of criminal damage can fill an important gap considering the enduring harm which results from misuse of an individual's token identity by another person and because unlike theft, dishonesty is not a requirement for the offence. This chapter argues that misuse of an

---

[307] Model Criminal Law Officers' Committee of the Standing Committee of Attorneys- General, '*Final Report Identity Crime,'* March 2008, 14. The MCLOC instead conceptualised 'identity theft' as fraud or deceit and recommended that new model identity crime offences cover dealing in, or possessing, identification information with the intention of committing, or facilitating the commission of, an indictable offence.

individual's token identity by another person causes harm which can, and should, be considered criminal damage to property and that the offence should extend to damage to intangible property as is the case in South Australia.[308]

The discussion in this chapter is directly relevant to the NIS but it has implications for Australia in relation to any future national identity scheme and its impact on human rights. Following on from chapters 4 and 5, the NIS is used as the model for the analysis, but the issues are also applicable to a scheme like the ACS, especially considering the similarities between the criminal law of the United Kingdom and Australia.

The federal *Criminal Code* is the relevant national legislation in Australia. For constitutional reasons, the *Criminal Code* is limited to offences against the Commonwealth. In the event of a national identity scheme being established in Australia, token identity would be established by Commonwealth legislation. As property established by Commonwealth legislation, token identity would be covered by Commonwealth theft law,[309] so for the purposes of this discussion, the provisions of the *Criminal Code*, including section 131.1 which deals with theft of property belonging to a Commonwealth entity,[310] is considered to apply to an individual's token identity registered under a national identity scheme. The relevant offences in the United Kingdom are basically the same as the offences in the *Criminal Code*. However, specific reference is made to the South Australian legislation which is also based on the English law but contains modifications that are especially relevant to this discussion.

---

[308] S 85(3) *Criminal Law Consolidation Act.*
[309] In any event, if`legislative amendment is required to extend clearly to an individual's identity registered under the scheme, such an amendment is within the incidental powers under s 51 *Australian Constitution*.
[310] See, s 131.1(1)(b). S 131.1 is a slightly modified version of the United Kingdom theft offence in the *Theft Act*.

Bearing in mind the inherent vulnerabilities of the identifying information examined in chapter 4, the analysis begins by considering how it is possible for an individual's token identity to be used by another person for a transaction under the scheme, and the nature of the wrong and the harm caused by that misuse. The nature of the wrong is relevant to theft and criminal damage but harm is most relevant to criminal damage which is examined later in this chapter, after theft.

The examination of theft distinguishes identity fraud from identity theft using the emergent concept of digital identity in the context of the NIS and having regard to the nature of the wrong, and the resulting harm to the individual as the primary victim. The elements of the theft offence are then considered in relation to misuse of an individual's token identity.

The analysis concludes by examining criminal damage which is closely related to theft but which in the United Kingdom and under the Australian federal *Criminal Code* is limited to tangible property. The South Australian offence, which applies to intangible property, is therefore considered in relation to the damage caused by misuse of token identity, as a suitable legislative model for the United Kingdom and for the Australian federal *Criminal Code* which currently confine criminal damage to tangible property.

6.2. The Wrong and the Harm Caused by Misuse of Token Identity

As discussed in chapters 2 and 3, registration and the verification process under the NIS transforms the information which constitutes token identity, so that, as a set, it becomes an individual's transactional identity. The token identity presented at the time of transaction,

singles out an identity and authorises the system to deal with that identity. Token identity acts as the metaphorical key.

Misuse of an individual's token identity by another person for a transaction is made possible by the verification process under the scheme. Identity is verified when the required token identity information as presented matches the record in the NIR. Recall from the discussion in chapters 2 and 3 that not all the registered token identity information will necessarily be used to verify identity at the time of a transaction. The token identity information used will depend on the nature of the transaction and the requirements of the transacting entity.

As mentioned in chapter 3, usually name, gender, date and place of birth and one item of the identifying information will be required. Depending on the transaction, the identifying information used can be appearance in comparison with the head and shoulders photograph, comparison of the handwritten signature and/or comparison of one or more biometrics. Routine transactions conducted in-person will usually require a match with the photograph or a signature. Use of biometrics makes misuse more difficult (although not impossible) but biometrics will only be used for significant financial transactions under the NIS.[311] Indeed some transactions, most notably remote transactions conducted by telephone or using the internet, may not use any of the identifying information. Answers to pre-designated questions may be used to check identity, but as discussed in chapter 1, their purpose is really to check that the token identity is in the right hands. This additional information is not part of token identity.

[311] Identity and Passport Service, *Using the Scheme in Daily Life, Transferring Money,* <http//:/www. identity cards.gov.uk/scheme.html> at 10 May 2006. For a recent statement see also, Identity and Passport Service, *Using the Scheme in Daily* Life <http://www.ips.gov.uk/identity/how-idcard-daily-providing.asp> at 1 September 2008 Identity and Passport Service, *Using the Scheme in Daily Life, Transferring Money,* <http//:/www. identity

Use of the token identity of individual A by another person B, for example, exploits the presumption that the token identity is presented by A, but as argued in chapter 3, the transaction is between the transacting entity and the token identity A. Token identity is the legal person in a transaction, not the individual to whom it is connected in the register, nor the person who presents it at the time of the transaction. The situation can be depicted diagrammatically:

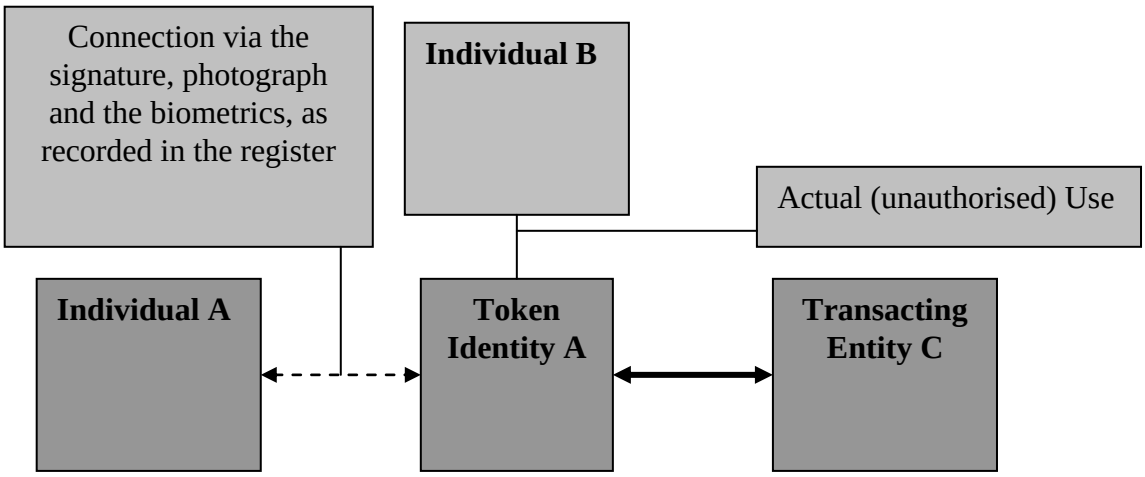

Fig. 12.

Assuming absence of conspiracy between B and A (and C), if B presents A's token identity as his or her own, A is the primary victim. In this situation, B has presented A's token identity and the transacting entity C will seek to enforce the transaction against A as the obvious, presumed administrator of token identity A. This is particularly so if biometrics are not used for the transaction but even if biometrics are used, there is no indication that the biometric actually presented at the time of a transaction will be recorded, nor that the record will be retained for future comparison. Without such a record, the biometric presented cannot

---

cards.gov.uk/scheme.html> at 10 May 2006. For a recent statement see also, Identity and Passport Service, *Using the Scheme in Daily* Life <http://www.ips.gov.uk/identity/how-idcard-daily-providing.asp> at 1 September 2008.

subsequently be compared to the biometric in the NIR, nor to the individual suspected of using the token identity for the transaction.

The wrong is the use of A's token identity by another person and the wrong occurs at the time of the misuse. The wrong is primarily to the individual whose token identity is used by another person, although there are collateral wrongs to C and broader societal implications which extend to the transacting entity, the State as administrator of the scheme, and indeed to all users who rely on the integrity and accuracy of the scheme.

Harm also occurs when the token identity is used by another person for a transaction but the nature of token identity and its functions under the NIS mask the true effects of the misuse. While harm it not necessary for theft, the harm caused by the misuse reveals the impact on the individual as the primary victim and the harm caused to token identity is directly relevant to the offence of criminal damage which this thesis argues should also have application to intentional or reckless misuse.

The intangible nature of token identity means that its use by another person is not likely to be noticed by the victim in the same way that a wallet or identity card is missed, for example. Nevertheless, the enduring nature of the information which comprises token identity and its unique association with an individual under the scheme[312] means that misuse of an individual's token identity by another person impairs that unique and exclusive association.

[312] Even if a victim can use a new token identity as a result of name change, for example, the new identity can be traced back to the original name. Under sch 1 pt 9 *Identity Cards Act* includes 'other names by which he is or has been known' are recorded in the NIR.

The misuse does not necessarily render the token identity useless to the individual either during misuse, nor afterwards. Use by another person will not prevent the individual from using his or her token identity for other transactions, unless misuse is suspected and a 'stop' is imposed by the system. Such action will also only be temporary, although system security will usually require that the individual continue to provide additional information such as a PIN or answers to designated questions in order to use his or her token identity. The need for these extra requirements illustrates the damage caused.

The misuse also affects the individual's database identity and his or her broader 'digital reputation.' When the system verifies identity for a transaction, that verification is recorded in the individual's entry in the NIR, while details of the transaction are recorded in the database of the transacting entity. This is the case for all transactions, irrespective of whether they are with a government or a private sector entity. Consequently, the use of the individual's token identity for a transaction becomes part of the individual's database identity under the scheme,[313] whereas the transactional details become part of Solove's 'digital person.' Of course, the record should be corrected when the individual is cleared of any involvement and, as discussed in chapter 5, the individual has rights of access, correction and notation under the *Data Protection Act*. However, in the meantime, information entered into government and private sector databases may have been sold or otherwise distributed. Distribution can be so fast and widespread that the rights of the individual under the *Data Protection Act* are virtually useless.

[313] Recall that public sector databases are generally accessible under the scheme.

6.3. Identity Theft Distinguished from Identity Fraud

Recall that as discussed in chapter 5, according to *Neethling*, '[a] person's identity is infringed if *the indicia* of identity are *used* without authorization in ways which cannot be reconciled with his true image.'[314] (emphasis added). Under a national identity scheme, the set of information which is an individual's identity for the particular transaction is indicia of identity.

This thesis argues therefore that identity theft is the dishonest use of an individual's token identity for the particular transaction. Theft therefore only applies to a token identity transaction, that is, a transaction which is with a transacting entity under the scheme. Recall that such a transaction may be between an individual and a government department or agency or a private sector entity, but does not include dealings of a social or domestic nature. Eventually, when the scheme is fully established, most commercial transactions entered into by an individual with public and private sector businesses will be token identity transactions.

As discussed, the token identity information required depends on the particular transaction but typically will comprise, name, date and place of birth, gender and identifying information such as comparison of photograph, signature or biometrics. For example, a transaction may require name, date and place of birth, gender and say, photo comparison, to establish identity. If a person dishonestly uses another individual's name, date and place of birth and photograph (whether on the ID card or as recorded in the NIR) for the transaction, this chapter argues that use of that set of information constitutes theft of the individual's token identity and is identity theft as defined in this thesis.

By contrast, identity fraud is essentially deception as to any database identity information including token identity information. Use of another name and date and place of birth may be fraudulent but it is not theft of identity as defined in this thesis. Name, gender, and date and place of birth, even when considered as a set, will usually not conclusively identify an individual, especially in a large population. It is likely, for example, that there is more than one person named Peter Smith who is male and who was born in London on 1 October 1970. As discussed in chapter 5, none of those individuals has an exclusive right to use that name or to that date and place of birth, and use of the information by one of them, even as a set, does not infringe the right to identity of any of the others under the scheme because that information does not constitute the indicia of identity under the NIS.

While adding a current address to the set of information narrows the field significantly, the *Identity Cards Act* separates 'identity' from residential address/es,[315] probably because an individual's address is likely to change over the course of a lifetime. If address is regarded as a de facto inclusion in the set of information which constitutes token identity, then arguably the set of information comprising an individual's name, gender, date and place of birth and address could be considered indicia of identity. However, that set of information cannot be considered to be the indicia of identity under the NIS, unless it is the set required to establish identity for a transaction under the scheme.

Use of just the identifying information of another individual is also insufficient to constitute theft. Consider for example, the situation depicted in *The Net,* where Angela Bennett's

---

[314] Neethling, above n 199, 36.
[315] See, s 1(5) *Identity Cards Act.*

fingerprints and photo are recorded with the name, address and social security number[316] of another person, Ruth Marx, to create a false identity. If this situation arises as a result of data manipulation as occurred in *The Net*, the activity is usually caught by specific computer crime offences which include hacking,[317] unauthorised modification of computer material[318] and, depending on the circumstances, unauthorised access with intent to commit or facilitate the commission of further offences.[319] However, the more likely scenario in the context of the NIS, is that a person will register using biographical information which relates to another person but will provide his or her own identifying information.

On registration, that biographical information is 'sealed to or permanently paired'[320] with the fraudster's identifying information. In this situation, the registration is fraudulent but the fraudster does not use another person's identity. Use of a name, and date and place of birth, which happen to correspond to that of another individual does not amount to dishonest use of that individual's token identity under the scheme so as to constitute identity theft. The use is fraudulent but it is not identity theft. Similarly, the subsequent use by of that registered token identity is fraudulent but it is not identity theft as defined in this thesis.

Identity theft is more restricted in its application than identity fraud. If a perpetrator dishonestly uses less than the full set of registered token identity information which constitutes an individual's identity for a particular transaction, or uses only the other Schedule 1 information, that use is not theft of identity. Furthermore, dishonest use of fictitious identity

---

[316] Address and a number like a social security number or passport number are part of the other sch 1 information which comprises an individual's database identity, but not token identity, under the NIS.
[317] S 1(1) *Computer Misuse Act 1990* (UK) c 18 ('*Computer Misuse Act'*). See also s 478.1 Australian federal *Criminal Code.*
[318] S 3(1) *Computer Misuse Act.* See also s 477.2 and s 478 Australian federal *Criminal Code.*
[319] S 2(1) *Computer Misuse Act.* See also s 477.1 Australian federal *Criminal Code.*

information may be identity fraud but it cannot be identity theft because an individual's transactional identity is not used. To constitute theft, the transactional identity used must be of a person who has been born, although that person does not still have to be alive, as long as the identity is registered under the scheme.[321]

The distinction between identity fraud and identity theft can be summarised diagrammatically:

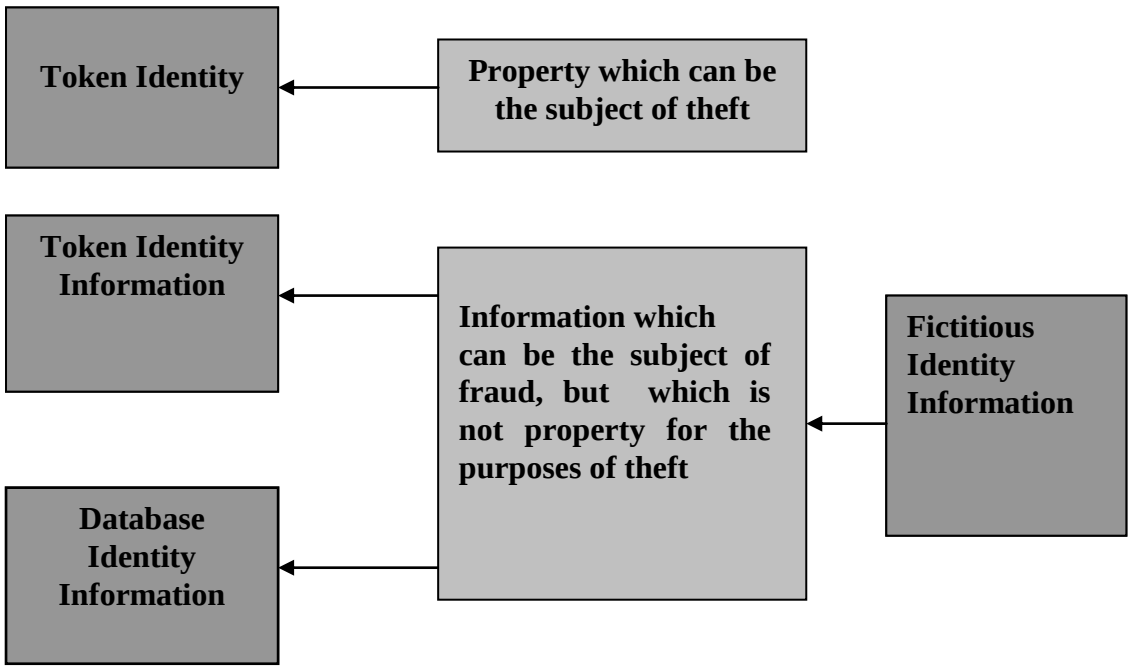

Fig. 13.

6.4. Is Identity Theft Really Theft?

Alex Steel maintains that 'nothing of practical value is gained by extending theft to include intangible property and that misuse of intangible property is best dealt with either by fraud or

[320] Identity and Passport Service, *Biometrics* <http//:www.identitycards.gov.uk/scheme.html> at 10 May 2006.For recent version of this statement see, Identity and Passport Service, '*What is the National Identity Scheme?'* <http//:www.ips.gov.uk /identity/scheme-what-produced.asp> at 1 September 2008.
[321] Recall that token identity includes date of death. See, s 1(7) *Identity Cards Act.*

sui generis offences.'[322] However, this chapter argues that dishonest use of an individual's token identity by another person is more than fraud and that in the context of a scheme like the NIS, there is much to be gained by extending theft to intangible property like token identity.

The current fraud and sui generis offences do not address the essential nature of the misuse by another person of an individual's registered token identity which as this chapter agues, is an appropriation. Most importantly, the offences do not acknowledge the immediate wrong to the individual caused by the misuse. Fraud offences in the United Kingdom for example, are financial offences which typically require the offender to intend to 'make a gain for himself or another' or 'to cause loss to another or to expose another to risk of loss,' [323] whereas theft is framed in terms of the violation of the rights of the individual in respect of his or her property.

Specific types of offences such as the computer offences under the *Computer Misuse Act*,[324] have limited application to the types of misuse which can be expected in the context of the NIS. Use of an individual's token identity by another person does not necessarily involve

[322] Alex Steel, 'Intangible Property as Theft,' (2008) 30 *Sydney Law Review* 575.

[323] See, ss 2 and 5 *Fraud Act.* 'Gain' and 'loss' are defined as a gain or loss in money or 'other property'. 'Property' for the purposes of the *Fraud Act* offences is defined in same terms as the *Theft Act*. See, s 5(2*) Fraud Act* and s 4(1) *Theft Act.* An individual's token identity is property within that definition so the offence of fraud by false pretence can apply if a person uses another person's name and date and place of birth to register, because he or she makes a false representation in order to gain a registered token identity. In Australia, see also, s 134.2 *Criminal Code* which refers to 'financial advantage.'

[324] Pt 10.7 *Criminal Code* includes computer offences which are similar to the offences in the United Kingdom *Computer Misuse Act*. Legislation in the other Australian jurisdictions contains similar provisions. See for example, Pt 4A South Australian *Criminal Law Consolidation Act*.

modification of data,[325] nor modification or impairment of electronic communication[326] and, arguably, access is not unauthorised as required by section 1(1) of the *Computer Misuse Act*.[327] Even the new offences in the *Identity Cards Act*, which are indicative of the type of new offences that can be expected in the event of a national identity scheme, do not make misuse of an individual's token identity by another person an offence. They only apply to offences at the time of registration, not to misuse of registered identity. Sections 25 and 28 in particular, are directed at the use for registration of information which is fabricated or which relates to another person. The other sections in the suite of offences relate to scheme administration and are primarily directed at employees and contractors. Section 27 makes it an offence to disclose confidential information and section 29 makes it an offence to tamper with the NIR. The offence under section 29 is similar to the offence in section 1 of the *Computer Misuse Act* except that section 29 includes recklessness.

Indeed, so called specific 'identity theft' legislation like that enacted in Australia, and the model identity crime provisions recommended for Australia by the MCLOC, do not make identity theft or identity fraud, as defined in this thesis, an offence per se. Instead, the offence

---

[325] See, s 3 *Computer Misuse Act*. This is also the situation in Australia. See, pt 10.7 *Criminal Code* particularly the definition of 'modification' in s 476.1(1) which is defined as:

'(a) the alteration or removal of the data: or

(b) an addition to the data.'

Similarly, under State legislation like pt 4A South Australian *Criminal Law Consolidation Act,* for example, use by another person's token identity for a transaction is clearly not unauthorised modification of data under s 86C, nor is it an unauthorised impairment of electronic communication under s 86D.

[326] In Australia, see for example, ss 476.4 and 474.6 *Criminal Code*.

[327] To be guilty of the offence of unauthorised access under s 1 the offender must 'cause the computer' to perform a function to secure access which is unauthorised. S 17(1)(c) and s 17(3) define access to include use of a program that causes the computer to perform a function. Although widely defined, in the context of the NIS, access is not unauthorised, and a person does not cause the function–it is a function of the token identity. Nevertheless, in specific circumstances, the offence under s 1 can apply to misuse of an individual's registered token identity by another person. The same comment applies to the equivalent offence under s 476.2(1) Australian *Criminal Code* which provides that access to data in a computer by a person 'is unauthorised if the person is not entitled to cause that access.' Other specific offences in the Australian federal *Criminal Code* like the offences in relation to 'National Infrastructure' such as using a telecommunications network with intent to commit a serious offence in s 474.14 and under s 1(1) *Regulation of Investigatory Powers Act 2000* (UK) c 23 may also apply in some circumstances, although proving the intent element may be difficult. The important point

is the use of another person's 'personal identification information,'[328] 'intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence.'[329] In framing the offences in this way, the objective is early intervention, with the aim of preventing what is regarded as the more serious offence.[330] It is a common approach,[331] the rationale being that identity crime is often committed as a preliminary step to a serious crime. However, the result is that none of the current or proposed Australian 'identity theft' offences make the immediate wrong to the individual an offence, unless there is intent to commit or facilitate 'a serious criminal offence' which in section 144 of the South Australian *Criminal Law Consolidation Act* for example, is defined as an indictable offence or a prescribed offence. Labelling these offences 'identity theft'[332] and 'identity crime'[333] can therefore be misleading.

Section 144 applies to use of 'personal identification information' not to use of another individual's identity. Section 144A(a) defines 'personal identification information' as including:

> (i) information about the person such as his or her name, address, date or place of birth, marital status, relatives and so on;

---

is, however, that although these offences may be invoked in some circumstances, they do not fit misuse of token identity like theft, or indeed, criminal damage.

[328] See, s 144A(a) *Criminal Law Consolidation Act*. South Australia uses 'personal identification information' whereas the Queensland offence and the recommended model are based on 'identification information' but the substance of the definitions is the basically the same.

[329] See, for example, s 144A *Criminal Law Consolidation Act* which defines 'serious criminal offence' to mean
'(a) an indictable offence; or
(b) an offence prescribed by regulation for the purposes of this definition;'
The intention of 'committing or facilitating the commission of an indictable offence,' is required for the Queensland offence, and for the recommended model offences. See, s 408D *Criminal Code 1899* (Qld). See also, the offence provisions recommended by the MCLOC. above n 307, 25.

[330] In line with this rationale, s 144E specifically excludes attempt offences by providing that '[A] person cannot be convicted of an attempt to commit an offence against this Part.'

[331] It has been adopted for a range of offences in Australia. See, for example, the offence of using a telecommunications network with intent to commit a serious offence in s 474.14 *Criminal Code* and the offence of possession or control of data with intent to commit a computer offence in s 478.3 *Criminal Code.* It is also widely used in other jurisdictions. See for example, the *Identity Theft and Assumption Deterrence Act 1998*.18 USC 1028(a)(7) which prohibits the knowing use, transfer, or possession, without authorization, of a 'means of identification' of another person with the intent to commit, or to aid or abet, or in connection with any unlawful activity that constitutes any offence under federal law or any felony under state or local law in the United States.

[332] Pt 5A of the South Australian *Criminal Law Consolidation Act* is entitled 'Identity theft.'

[333] The title of the model offences recommended by the MCLOC is 'Recommended model identity crime offences.' See, MCLOC, above 307, 25.

(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;
(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);
(viii) a series of numbers or letters (or a combination of both) intended for use as a means of personal identification;'

This definition is very wide. It certainly includes elements which comprise token identity under the United Kingdom scheme (and under the proposed Access Card Bill). However, a defined concept of identity for transactional purposes is not evident in the provision.[334]

Moreover, dishonest misuse of an individual's token identity by another person is not an offence under section 144 unless there is intent to commit or facilitate an indictable or prescribed offence. Proving that additional element of the offence can be difficult, whereas dishonest misuse can be established relatively easily.

The misuse should be appropriately and accurately labelled, as theft, and specifically as identity theft. As Andrew Ashworth observes, the concern lying behind fair labelling or representative labelling, as it was originally termed,[335] is that 'widely felt distinctions between kinds of offences and degrees of wrongdoing are respected and signalled by the law, and that offences are subdivided and labelled so as to represent fairly the nature and magnitude of the law-breaking.'[336] As Ashworth notes, labelling is important for reasons of 'proportionality' to provide 'maximum certainty' and he touches on the importance of legal definitions reflecting

[334] The closest formulation is in pt (a)(i) but the expansion of the set of information to include 'relatives' and the addition of 'so on' extends the information beyond token identity into the additional information which comprises database identity.
[335] Andrew Ashworth, 'The Elasticity of Mens Rea' in C. F. H. Tapper (ed), *Crime, Proof and Punishment: Essays in Memory of Sir Rupert Cross* (1981) 45, 53.
[336] Andrew Ashworth, *Principles of Criminal Law* (5th ed, 2006), 88.

'common patterns of thought in society.'[337] This reasoning has been supported by recent research which shows that description and differentiation are the two most important considerations in the accurate labelling of offences.[338] A description which accurately describes the offence is the most important consideration for the general public, whilst a label which clearly differentiates the nature of the offence is the most important consideration for people working within the criminal justice system.[339] The label 'identity theft' correctly applied, readily differentiates the offence from fraud which can apply to a wide range of criminal behaviour with many different victims and different consequences, which influence sentencing, rehabilitation and parole as well as victim compensation, for example.

Consequently, contrary to Steel's assertion, there is a significant gap in the protection currently provided to an individual's registered token identity. This gap can be addressed by regarding the dishonest use of an individual's token identity by another person for a transaction, as theft of the individual's identity and labelling it as identity theft. Doing so acknowledges the true nature of the offence as a dishonest misappropriation of the individual's rights in his or her token identity and the immediate impact on the individual as the legitimate rights holder.

6.5. Identity Theft is Theft

Recall that section 1(1) of the United Kingdom *Theft Act* provides that:

> A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and "thief" and "steal" shall be construed accordingly.[340]

---

[337] Ibid, 88-89.
[338] James Chalmers and Fiona Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 217, 246.
[339] Ibid.
[340] The theft offence in the Australian federal *Criminal Code* contains the same elements. See, s 131.1(1).

If a person dishonestly uses the identity of another individual, or even just some parts of it, to obtain property such as money, the elements of the offence are usually easily made out. However, as discussed, in the context of a scheme like the NIS, the wrong and the harm to the individual occurs at the time his or her token identity is used by another person for a transaction and this thesis argues that that misuse is capable of meeting all of the elements required for theft.

6.5.1. Token Identity is Property belonging to the Individual

Theft clearly extends to intangible property. Section 4(1) of the *Theft Act* defines 'property' as including 'money and all other property whether real or personal including things in action and other intangible property.' For the purposes of theft, property is regarded as belonging to the person who has control of it or who has a proprietary right in it. Indeed, section 5(1) states that '[p]roperty shall be regarded as belonging to any person having *possession or control* of it, or having in it *any proprietary right or interest* (not being an equitable interest arising only from an agreement to transfer or grant an interest).'(emphasis added)[341]

The nature of token identity, its functions under the NIS, its contingent connection to the individual as recorded in the NIR and the control of the registered token identity accorded to that individual by the scheme, give token identity the characteristics of intangible property belonging to the individual within the meaning of sections 4(1) and 5(1) of the *Theft Act*.

[341] The Australian equivalent contains very similar definitions. See, s 130.1 and s 130.2(1) *Criminal Code*.

When considered separately, the components of token identity do not have the characteristics of property, nor do they invariably identify an individual. An individual does not own his or her name, and date and place of birth, for example. Even jurisdictions which protect some of the components, do not regard them as property, nor the individual as their owner. The right to publicity recognised in the United States for instance, protects the unauthorised use of a celebrity's name, image, and even voice.[342] When considered separately these components can identify the individual because, as a consequence of the celebrity's public profile, the name, image or voice is distinctive, but the right is essentially personal, not proprietary. However, on registration under the NIS, the information which makes up token identity assumes the essential characteristics of property. On registration, as a set, it becomes property that is then capable of being controlled as required by section 5(1). Assuming the absence of fraud or system error at the time of registration, the registered token identity then belongs, as defined in section 5(1), to the individual to whom it is attributed in the NIR.

The conceptualisation of property as a relationship between people based on individual autonomy where property 'describes the individual's protected sphere, asserted against the collective,'[343] is well established in international legal scholarship and jurisprudence.[344] The

---

[342] The law in some European jurisdictions provides similar protection to persons who do not have a public profile but as a personal, not a proprietary right.

[343] Laura S Underkuffler, *The Idea of Property* (2003), 52. See also, Laura S Underkuffler, 'On Property' (1990) *Yale Law Journal* 127 and Robert W. Gordon, 'Paradoxical Property' in John Brewer and Susan Staves (eds) *Early Modern Conceptions of Property* (1996) 95, 101 where Gordon traces the history of property back to rights like liberty and states that ''[p]roperty' is still to this day heard as unequivocally expressive of autonomy and liberty.'

[344] See, C Edwin Baker, 'Property and its Relation to Constitutionally Protected Liberty' (1986) 134 (4) *University of Pennsylvania Law Review*, 741, 742-75 which describes property as 'an aspect of relations between people' where 'property rights are a cultural creation and a legal conclusion.' Baker lists the functions of property as 'the welfare function to secure individuals' claims on those resources that a community considers essential for meaningful life,' 'the personhood function ...to protect people's control over unique objects and specific spaces that are intertwined with their present and developing individual personality or group identity'; the 'protective function' which is to protect individuals against forms of unjust exploitation by other individuals or the government, the 'allocative function' to secure resources individuals need for their productive or consumptive activities and the allied 'sovereignty function.' In a similar vein, see also, Joseph William Singer, *Entitlement: The Paradoxes of Property* (2000), 146 and the seminal work, Thomas C. Gray 'The Disintegration of Property' in J. Roland Pennock and John W. Chapman (eds) *Nomos XX11: Property* (1980).

important considerations are relationship and control, as recognised by the majority of the Full Court of the High Court of Australia in *Yanner v Eaton* [345] which cites the influential work of Kevin Gray:[346]

> The word 'property' is often used to refer to something that belongs to another. But in the *Fauna Act*, as elsewhere in the law, 'property' does not refer to a thing; it is a description of a legal relationship with a thing. It refers to a degree of power that is recognised in law as power permissibly exercised over the thing. The concept of "property" may be elusive. Usually it is treated as a 'bundle of rights.' But even this may have its limits as an analytical tool or accurate description, and it may be, as Professor Gray has said, that 'the ultimate fact about property is that it does not really exist: it is mere illusion.' Considering whether, or to what extent, there can be property in knowledge or information or property in human tissue may illustrate some of the difficulties in deciding what is meant by 'property' in a subject matter….
>
> Nevertheless, as Professor Gray also says,
> An extensive frame of reference is created by the notion that 'property' consists primarily in control over access. Much of our false thinking about property stems from the residual perception that 'property' is itself a thing or resource rather than a legally endorsed concentration of power over things and resources.[347]
>
> …Because 'property' is a comprehensive term it can be used to describe all or any of many different kinds of relationship between a person and a subject matter.[348]

Although these views of the High Court are obiter dicta,[349] they provide as Gray states, a frame of reference. Most importantly in the context of this thesis, they present a realistic conceptualisation which takes into account modern forms of intangible property such as token

---

[345] (1999) 201 CLR 351.The appellant, an Aboriginal man was charged with breaching s 54(1)(a) of the *Fauna Conservation Act 1974* (Qld) ('*Fauna Act'*) after killing two crocodiles using a traditional form of harpoon. Section 54(1)(a) makes it an offence to hunt certain fauna, including crocodiles, without first obtaining a licence or permit. The appellant argued that under s 211 of the *Native Title Act 1993* (Cth) he was entitled to exercise his native title right to hunt upon land of which he is a traditional owner without seeking prior authorisation.

[346] Kevin Gray is Drapers' Professor of Law at the University of London at Queen Mary and Westfield College.

[347] (1999) 201 CLR 351, para 18, quoting Kevin Gray, 'Property in Thin Air', (1991) 50 *Cambridge Law Journal* 252, 299. The judgement also refers to Jeremy Bentham, stating that 'Bentham recognised this long ago. Bentham pointed out that 'in common speech in the phrase 'the object of a man's property,' the words 'the object of' are commonly left out; and by an ellipsis, which, violent as it is, is now become more familiar than the phrase at length, they have made that part of it which consists of the words 'a man's property' perform the office of the whole.' See, *An Introduction to the Principles of Morals and Legislation*, ed by W Harrison (1948), 337, n 1.'

[348] Ibid, paras 17-20.

[349] Gleeson CJ, Gaudron, Kirby and Hayne JJ concluded that the 'property' conferred on the Crown is not accurately described as 'full beneficial, or absolute, ownership.' 'Taken as a whole the effect of the *Fauna Act* was to establish a regime forbidding the taking or keeping of fauna except pursuant to licence granted by or under the Act.' The majority went on to find that '[t]he *Fauna Act* did not extinguish the rights and interests upon which the appellant relied. Accordingly, by operation of s 211(2) of the *Native Title Act* and s 109 of the *Constitution*, the *Fauna Act* did not prohibit or restrict the appellant, as a native title holder, from hunting or fishing for the crocodiles he took for the purpose of satisfying personal, domestic or non-commercial communal needs.' Ibid, paras 30 and 40.

identity.[350] They recognise that property is a relationship and that it can be a relationship based on an abstraction or a thing.

Under the NIS, there is a relationship between the individual and his or her registered token identity which necessarily requires the individual's control or power over access. Under the scheme, the individual controls the use of his or her token identity for transactions and hence access to his or her record in the NIR to verify identity at the time of a transaction. The premise of one person: one identity underpins the scheme and as discussed in chapter 5, part of the individual's right to identity in the context of the scheme, is the right of the individual to a unique identity and to its exclusive use. A broader relationship between the individual and others also exists, whereby the relationship between an individual and his or her token identity is recognised and respected. Central to this relationship is the individual's control over his or her registered token identity for transactional purposes.

Under the scheme, there is necessarily a general duty on other members of society not to interfere with an individual's token identity and the individual's exclusive use, which is in line with Hans Kelsen's view that,

> [t]he typical right to a thing (or real right) …is the property right. Traditional science of law defines it as the exclusive dominion of a person over a thing and thereby distinguishes this right from the right to claim, which is the basis only of personal legal relations. This distinction, so important for civil law, has an outspoken ideological character.
>
> Since the law as a social order regulates the behavior of individuals in their direct or indirect relations to other individuals, property too, can legally consist only in a certain relation between one individual and other individuals. This relation is the obligation of

[350] Alienability is often assumed to be a distinguishing feature of property. For example, in *National Provincial Bank v Ainsworth* [1965] AC 1175, Lord Wilberforce stated that property 'must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability.' In Australia, however, assumption by third parties' is clearly not an essential feature of property as Kitto J of the High Court of Australia pointed out in *National Trustees Executors & Agency Co of Australasia Ltd v FCT* (1954) 91CLR 540, 583. 'It may be said categorically that alienability is not an indispensable attribute of a right of property according to the general sense which the word 'property' bears in the law.' And alienability is not a feature of recently recognised concepts of property. The property rights recognised by the High Court of Australia in *Mabo v Queensland [No 2]* (1992) 175 CLR 1, for example, do not include alienability.

> these other individuals not to disturb the first one in his disposition over a certain thing. What is described as the exclusive 'dominion' of an individual over a thing is the legally stipulated exclusion of all others from the disposition over this thing. The dominion of the one is legally merely the reflex of the exclusion of all others.[351]

Like Kelsen, Morris Cohen also maintains that a 'property right is a relationship not between an owner and a thing but between owner and other individuals in reference to things. A right is always against one or more individuals.'[352]

As to rights and duties as incidents of ownership of property, Stephen Munzer explains that,

> [t]he idea of property–or, if you prefer, the sophisticated or legal conception of property – involves a constellation of Hohfeldian elements, correlatives and opposites; a specification of standard incidents of ownership and other related but less powerful interests; and a catalogue of "things" (tangible and intangible) that are the subject of these incidents. Hohfeld's conceptions are normative modalities. In the more specific form of Honoré's incidents, these are the relations that constitute property. Metaphorically, they are the "sticks" in the bundle called property.[353]

According to Anthony Honoré, for full ownership in a thing to be recognised, an individual must have most, though not necessarily all, of what he refers to as incidents of ownership.

These incidents spring from the relationship and according to Honoré consist of the right to possess the property, the right to use the property, the right or power to manage how the property is used, the right to income from the property, the right to capital, to security from interference, the right of transmissibility, the right to absence of term, the duty to prevent harm, liability to execution and the incident of residuarity.[354] As discussed below, this thesis

---

[351] Hans Kelsen, *Pure Theory of Law* (Max Knight trans, 1970), 131.
[352] Morris Cohen, 'Property and Sovereignty,' (1927) 13 *Cornell Law Quarterly*, 12. See also Charles Reich, 'The New Property' in C.B. Macpherson (ed) *Property Mainstream and Critical Positions* (1978), 177.
[353] Stephen Munzer, *A Theory of Property* (1990), 23.
[354] Anthony Honoré, 'Ownership' in AG Guest, *Oxford Essays in Jurisprudence* (1967), 107. In examining the concept of ownership evident in most legal systems, Honoré, found these 11 incidents (nine rights, one duty and one liability).

asserts that in relation to his or her registered token identity, the individual has most of the 11 rights and duties listed by Honoré.[355]

Although the *Identity Cards Act* provides that if an ID card is issued it 'remains the property of the person issuing it,'[356] the Act is silent as to the ownership of the information which comprises token identity. Nevertheless, just as the card can be stolen from the individual as cardholder, this thesis argues that the information which collectively constitutes token identity can be stolen. On registration, the power to possess and control the collection of information which constitutes his or her token identity is conferred on the individual.

Possession according to Honoré, is the right to have exclusive physical control. Honoré states that there are two aspects to this control: the right to be put in control and the right to remain in control.[357] Both aspects are present in relation to an individual and his or her token identity. Registration puts the individual in control of the registered token identity and gives the individual the right to remain in control of that property, within the constraints of the scheme.[358] Embedded in this right to control is the right that others cannot unilaterally and unlawfully interfere with it.[359] Honoré states that [i]t is of the essence of the right to possess that it is in rem in the sense of availing against persons generally' and that,

---

[355] This thesis asserts that an individual has seven of the 11 incidents of ownership listed by Honoré. As discussed in this chapter, in addition to the right to possess and the right to use his or her registered token identity, the individual has the right to manage it, the right to its security, the right to immunity from the termination without justifiable cause and arguably the incident of residuarity applies. The individual also has a duty not to use the token identity to cause harm. The other incidents listed by Honoré such as the right to capital, right to income, and liability to execution for example, are incidents of specific forms of property. They do not apply to token identity primarily because of its intangible nature and because it is currently an emergent form of property.

[356] S 6(3)(d). It seems, therefore, that the card is government property.

[357] Honoré, above n 354, 113.

[358] The notion that information can be possessed is certainly not an alien notion under modern criminal law. S 478.3 *Criminal Code* for example, makes it an offence to possess or control data with intent to commit a computer offence.

[359] Honoré, above n 354, 114.

> [t]he protection of the right to possess, and so of one essential element in ownership, is achieved only when there are rules allotting exclusive physical control to one person, rather than another, and that not merely on the basis that the person who has such control at the moment is entitled to continue in control.'[360]

As argued in chapter 5, an individual has the exclusive right to his or her unique identity under the scheme and in that sense therefore the individual has exclusive 'dominion' over his or her registered token identity. To maintain the integrity of the scheme, an individual's dominion over his or her registered identity must be protected from interference or disturbance and be respected by others.

In addition to the right to possess and the right to use, the individual also has the right to manage, also listed by Honoré, in that the individual has the right to determine how his or her token identity is used, within the constraints of the scheme, and the right to security in the sense that the individual should be assured that he or she will remain in control of the token identity and will not be forced to give it up. The individual also has the right to immunity from termination without justifiable cause, of his or her rights to the token identity.

As to duties, the individual must not use the token identity in a way that harms other members of society and Honoré maintains that the owner must also prevent others from using the property in a way that harms others. The incident of residuarity may also apply. Ownership rights may expire or be abandoned at which time rights to the token identity vest in someone else. In the context of token identity, that 'someone else' may be an executor or it may be the State.

---

[360] Ibid.

Token identity is therefore fundamentally different from the confidential information in the exam paper which was held in *Oxford v Moss*[361] not to be intangible property capable of being stolen.[362] In this case, a student dishonestly obtained the proof of an examination paper, read it and then returned it. Token identity is also fundamentally different from the other more detailed information which makes up the rest of an individual's database identity. Like the exam paper in *Oxford v Moss*, the other Schedule 1 information is just information. Depending on the circumstances, unauthorised access to that other information which makes up database identity may amount to an offence but it is not property which can be the subject of theft.

6.5.2. Appropriation of an Individual's Registered Token Identity

Appropriation for the purposes of the law of theft requires that the thief acts as though he owns the property. Section 3(1) of the *Theft Act* defines 'appropriation' as:

> Any assumption by a person of the rights of an owner amounts to an appropriation, this includes, where he has come by the property (innocently or not) without stealing, any later assumption of a right to it by keeping or dealing with it as owner.

Section 1(2) states that '[i]t is immaterial whether the appropriation is made with a view to gain, or is made for the thief's own benefit.' Assumption of any one of the rights of the owner is sufficient to constitute an appropriation.[363]

---

[361] (1978) 68 Criminal Appeal Reports 183.

[362] Although the decision was stated by the Court to turn on the question of whether information is property, the reasoning concentrates on whether information can be stolen. Oxford v Moss really decided that the unauthorised reading of the proof of an exam paper by a student was not an appropriation of intangible property with intent to permanently deprive because in reading the proof, the student did not remove or change the information it contained, (although arguably it did lessen its value as an assessment tool), so the defendant was not guilty of theft. Although not articulated by the Court, there is also the question of whether a criminal conviction for theft was justified in these circumstances.

Honoré's incidents of ownership map out the specific ownership rights (and duties) which this thesis asserts arise under the scheme and which are appropriated when the token identity is used by another person for a transaction. Specifically, in using an individual's token identity for a transaction, an offender assumes the individual's right to possess and use the token identity as discussed above. The offender also assumes the individual's right to manage the registered token identity and the offender's use also clearly violates the individual's right to security in respect of that identity.

6.5.3. Intention to Permanently Deprive the Owner of his or her Token Identity

The question is then whether the appropriation is made with intent to permanently deprive the individual of his or her token identity. Section 6 (1) of the *Theft Act* states that:

> A person appropriating property belonging to another without meaning the other to permanently to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the others rights; and a borrowing or lending of it may amount to so treating it if, but only if, the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal.

J.C. Smith argues that the intention to use the property as one's own is not sufficient to amount to theft:

> It adds nothing to "appropriates" since appropriation consists in an assumption of the right of the owner. The words, "dispose of," are crucial and are, it is submitted, not used in a sense in which a general might "dispose of" his forces but rather the meaning given by the Shorter Oxford Dictionary: 'To deal with definitely; to get rid of; to get done with, finish. To make over by way of sale or bargain, sell.'[364]

However, Smith's view is not borne out by legislative intent in enacting section 6, nor by subsequent judicial interpretation.

---

[363] *R v Gomez* [1993] AC 442 and *R v Hinks* [2001] 2 AC 241. As Steel observes, '[t]his leaves appropriation as a very broad term which requires only the assumption of any one property right associated with the victim.' Steel, above, n 322, 579.

Smith states that section 6(1) was intended[365] to cover the situation in *R v Hall*[366] (‘*Hall*’) in which the defendant was convicted of theft. Like a person who dishonestly uses another person’s token identity for a transaction, Hall dealt with the property as his own and he misrepresented its true ownership. He did not dispose of the property in the sense advocated by Smith. Hall did not change the property in any way, nor did he remove it from the possession of the true owner.

An employee of a tallow chandler, Hall pretended that the property, butcher’s fat, belonged to a third party in order to obtain payment for it from the owner, his employer. The fat (which had been marked by the owner because he suspected that Hall was stealing from him) remained at the owner’s premises. Hall moved the fat from the ‘upper room’ to the candle room and placed it on the scales with the intention of selling it to his employer as fat belonging to a local butcher Mr Robinson, and pocketing the proceeds. Parker B stated that ‘[i]n this case there is the intent to deprive the owner of dominion over his property…’[367]

Similarly, in *DPP v Lavender*[368] (‘*Lavender*’), the court considered that to focus on the words ‘to dispose of’ in section 6 and applying a dictionary definition to them was too narrow an approach. The words ‘if his intention is to treat the thing as his own to dispose of regardless of the other’s rights’ have to be read together. The court following the statements of the Privy Council in *Chan Man-sin v Regina,*[369] considered that a disposal under section 6 includes dealing.

---

[364] J C Smith ‘The Law of Theft’ (8th ed, 1977), 80.
[365] Ibid, 76.
[366] [1848-49] Law Times 383.
[367] The decision in *Hall* turned on the intention to deprive. As Lord Denman CJ observed, ‘[t]he taking is admitted, the question is, whether there is intention to deprive the owner entirely of his property. How could he deprive the owner more effectively than by selling it? To whom he sells it does not matter.’
[368] [1994] Crim LR 297.
[369] [1988] 1 WLR 196.

In *Lavender,* a tenant secretly took two doors from his landlord's premises to replace the damaged doors in his rented flat. The tenant made no overt pretence as to ownership of the doors. His intention was to leave the doors in the flat after his lease terminated in about a year. However, in assuming possession of the doors, the tenant violated the owner's rights. and applying the second limb of section 6(1), the court stated:

> So we think the question in the instant case is did the respondent intend to treat the doors as his own in dealing with the council regardless of their rights? The answer to this question must be yes. There can be no doubt that what the respondent did was regardless of the council's right. Those rights included the right not to have the doors at 25 Royce Road removed, and to require the tenant at 37 Royce Road to replace or pay for the damaged doors. In dealing with the doors regardless of those rights, when he consciously did, the respondent manifested an intention to treat them as his own.[370]

Both *Hall* and *Lavender* concerned tangible property but the basic principles apply to intangible property like token identity. The common factor in the reasoning used is that the defendant was considered to have stolen the property even though it was not removed from the possession of the owner and the nature of the property was not altered by the offender's actions. In both these cases, the defendant exerted control over the property in violation of the owner's rights and in doing so, usurped the owner's rights of control and exclusive use, although the defendant did not dispose of the property in the sense of getting rid of it. Likewise, a person who dishonestly uses another person's token identity for a transaction exerts control over the token identity and thereby, encroaches upon, and indeed usurps, the owner's rights[371] even though the token identity is not disposed of in the sense used by Smith.

---

[370] CO/2779/92 Unpaginated transcript (Tuckey J) See also, [1994] Crim LR 297, 298 where the commentary on *Lavender* states that '[t]he proper question was whether the respondent intended to treat the doors as his own, regardless of the Council's rights. The answer was yes, the respondent had dealt with the doors regardless of the Council's rights not to have them removed, and in so doing had manifested an intention to treat the doors as his own.'

[371] The South Australian offence which otherwise closely follows the *Theft Act*, expressly frames the intent requirement in terms of encroachment on the owner's proprietary rights. S 134(2) *Criminal Law Consolidation Act* states that:

'A person intends to make a serious encroachment on an owner's proprietary rights if the person intends—

(a) to treat the property as his or her own to dispose of regardless of the owner's

6.5.4. Dishonestly Appropriating Token Identity

If the other elements of the offence are established, it then becomes a question of whether the misappropriation was dishonest.

The *Theft Act* does not define 'dishonesty'[372] but in *R v Feely* the Court of Appeal held that dishonesty involves 'moral obloquy' and whether the accused is dishonest is a question of fact for the jury, applying 'current standards of ordinary decent people.'[373] This approach was modified by the Court of Appeal in *R v Ghosh* where the Court of Appeal emphasised that dishonesty refers to the knowledge and belief of the accused. The court doubted whether the court in *Feely* intended to establish an objective test and reframed it as a two step test:

> In determining whether the prosecution has proved that the defendant was acting dishonestly, a jury must first of all decide whether according to the ordinary standards of reasonable and honest people what was done was dishonest. If it was not dishonest by those standards, that is the end of the matter and the prosecution fails.
>
> If it was dishonest by those standards, then the jury must consider whether the defendant himself must have realised that what he was doing was by those standards dishonest. In most cases, where the actions are obviously dishonest by ordinary standards, there will be no doubt about it. It will be obvious that the defendant himself knew that he was acting dishonestly. It is dishonest for a defendant to act in a way which he knows ordinary people consider to be dishonest, even if he asserts or genuinely believes that he is morally justified in acting as he did.[374]

---

rights; or
(b) to deal with the property in a way that creates a substantial risk (of which the person is aware)—
(i) that the owner will not get it back; or
(ii) that, when the owner gets it back, its value will be substantially impaired.'

[372] S 130 Australian federal *Criminal Code* defines 'dishonesty' for the purposes of Chapter 7 which deals with offences relating to 'the proper administration of government' as:
' (a) dishonest according to the standards of ordinary people; and
(b) known by the defendant to be dishonest according to the standards of ordinary people.'
South Australia also defines 'dishonesty' in s 131 of the *Criminal Law Consolidation Act*:
' (1) A person' s conduct is *dishonest* if the person acts dishonestly according to the standards of ordinary people and knows that he or she is so acting.
(2) The question whether a defendant's conduct was dishonest according to the standards of ordinary people is a question of fact to be decided according to the jury's own knowledge and experience and not on the basis of evidence of those standards.'

[373] *R v Feely* [1973] 1 QB 530, 538 (Lawton LJ).

[374] [1982] QB 1053, 1064.

The belief of the defendant must be genuine. It need not be reasonable, although that is a relevant consideration in determining whether the belief is genuine.[375] In the context of the NIS, use of an individual's registered token identity by another person will usually clearly be dishonest.

Section 2(1) of the *Theft Act* sets out three situations in which appropriation of property is not regarded as dishonest based on the defendant's belief.[376] Under part (a) of section 2 (1), theft is not committed if a person appropriates the property believing that he/she has the legal right to deprive the owner of that property. Under part (b), if the accused believes that he/she has consent if the owner knew of the appropriation and circumstances, the use is not theft; and similarly the use is not theft under part (c) if the accused believes 'that the person to whom the property belongs cannot be discovered by taking reasonable steps.[377] Part (b) covers the situation most likely to arise in the context of the NIS, that is, where a friend or family member uses an individual's token identity for a transaction.

A misappropriation must be dishonest for it to be theft. However, under the NIS, use by another person of an individual's token identity undermines the underlying assumptions of the scheme and compromises the scheme's integrity even if the use is not regarded as dishonest.

---

[375] *R v Waterfall* [1970] 1 QB 148.
[376] The Australian federal *Criminal Code* contains a similar provision. See, s 131.2.
[377] Cf s 131 (4) *Criminal Law Consolidation Act* in South Australia, which follows s 2(1) of the *Theft Act* in spirit, but is expressed in simpler terms:

> '(4) A person does not act dishonestly if the person—
> (a) finds property; and
> (b) keeps or otherwise deals with it in the belief that the identity or whereabouts of the owner cannot be discovered by taking reasonable steps; and
> (c) is not under a legal or equitable obligation with which the retention of the property is inconsistent.
> (5) The conduct of a person who acts in a particular way is not dishonest if the person honestly but mistakenly believes that he or she has a legal or equitable right to act in that way.
> (6) A person who asserts a legal or equitable right to property that he or she honestlybelieves to exist does not, by so doing, deal dishonestly with the property.'

Consequently, special arrangements will be required in cases of incapacity, for example. However, the system can be designed so that the token identity of specific people such as next of kin or a designated carer are linked to the individual through a documented authorisation process, to avoid a situation where, in effect, the designated person represents that he or she is the incapacitated individual by presenting the latter's token identity.

6.6. Criminal Damage

Where, however, the use is reckless but not dishonest, this thesis argues that the offence of criminal damage which is closely related to theft, can and should, apply. Indeed, much of the argument for the application of the offence of criminal damage draws on the same associations as theft.

Considering the damage which can be caused by the misuse by another person of an individual's token identity as examined earlier in this chapter, the offence of criminal damage should extend to token identity. The offence applies to deliberate acts and recklessness. Dishonesty is not required but the act must be without lawful excuse. Section 1(1) of the *Criminal Damage Act 1971* (UK) c 48 ('*Criminal Damage Act'*) provides that:

> A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.

Currently, the *Criminal Damage Act* in the United Kingdom currently only applies to tangible property[378] but there is no reason in principle why criminal damage and theft cannot apply to

[378] See the definition in s 10(1) United Kingdom *Criminal Damage Act*. The *Computer Abuse Act* provides in s 3(6) that '[f]or the purposes of the *Criminal Damage Act* 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.' The Australian *Criminal Code* does not presently contain an equivalent offence but the criminal damage offence recommended in the Model Criminal Code only

the same forms of property. In South Australia, for instance, the criminal damage offence extends to damage to intangible property.[379] The offence closely follows the United Kingdom provision but is capable of applying to new forms of property like token identity. Section 85(3) of the *Criminal Law Consolidation Act* provides that:

> Where a person —.
>
> (a) intending to damage property of another, or being recklessly indifferent as to property of another is damaged; and
>
> (b) without lawful authority to do so, and knowing that no such lawful authority exists,
>
> damages, or attempts to damage, property of another, the person shall be guilty of an offence.

Part (b) of section 84(1)) states that 'to damage in relation to property includes – to make an alteration to the property that depreciates its value.' 'Owner of property' is defined to mean 'a person wholly entitled to the property both at law and in equity.'[380]

As discussed earlier in this chapter, when an individual's token identity is misused by another person, the use does not necessarily render the token identity useless. It can still be used by the individual albeit with a PIN or answers to additional designated questions. However, although it does not appear to be affected, primarily because of its intangible nature, the token identity has nevertheless been damaged. Its use by another person has altered it by compromising its integrity and its exclusivity to the individual and the need to use additional security measures illustrates the damage. In a statement which is particularly relevant to the special nature of the

---

applies to tangible property. See Model Criminal Code Officers Committee the Standing Committee of Attorneys- General, *Model Criminal Code Report, Chapter 4, Damage and Computer Offences* (2001), 8.

[379] S 5(1) *Criminal Law Consolidation Act*. defines 'property' to mean 'real or personal property whether tangible or intangible…'

[380] S 84(1).

damage resulting from the use of an individual's token identity by another person, Walters J in *Samuels v Stubbs*,[381] stated that in considering 'damage' in the South Australian offence:

> One must be guided in a great degree by the circumstances of each case, the nature of the article and the mode in which it is affected or treated …the word…is sufficiently wide to embrace, injury, mischief or harm done to property ...in order to constitute "damage" it is unnecessary to establish such definite or actual damage as renders the property useless or prevents it from serving its normal function.[382]

This statement has direct relevance to an individual's token identity and the harm which is done to it by its misuse by another person. Just as stomping on a policeman's cap was considered in *Samuels v Stubbs* to be criminal damage because it caused a 'temporary, functional derangement,'[383] misuse of an individual's token identity by another person also causes functional derangement. Unlike the policeman's cap, however, token identity is not necessarily restored to its original condition after the misuse and the functional derangement may not be temporary.

The misuse compromises the link between the individual and his or her token identity as recorded in the NIR so additional security procedures will be required to verify identity for a transaction. As mentioned earlier in this chapter, these procedures usually involve the requirement to use a PIN or to provide other additional information at the time of a transaction. The purpose of this additional information is to determine that the token identity is in the right hands but the routine requirement for this new or additional information at the time of a transaction, changes the individual's ability to use his or her token identity for a transaction under the scheme. So, while the core token identity information is unchanged, the

---

[381] (1972) 4 SASR 200, 203.
[382] Ibid. See, also *R v Whiteley* (1993) 93 Crim App R 25. in which the Court of Appeal held that hackers who added and deleted files on a computer network caused criminal damage under s 1(1) of the United Kingdom Criminal Damage Act 1971. The court found that damage need not be tangible and that there could be damage even though it was only perceptible by using a computer. The unauthorised deletion and addition of files altered magnetic particles which court held were tangible property.
[383] Ibid.

misuse changes its usual function at the time of a transaction. Presentation of only the required token identity information without complying with the additional system security requirements will not be sufficient to enable a transaction under the scheme.

The Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General ('MCCOC') observed that the definition of damage in section 84(1) enables the offence to 'extend to some conduct which appears far removed from anything which would ordinarily count as damage.'[384] However, while the offence extends to conduct which historically has not been considered criminal damage, new developments like the NIS and the emergent concept of digital identity, make such an extension necessary.

Token identity is an individual's transactional identity. In the context of the NIS it is the means by which an individual is known by the system and can function under the scheme and when the NIS is fully operational and compulsory it will be essential for most transactions. It is, by its nature, intimately connected with the individual. Its connection to the individual extends beyond any other group of information currently in use, in terms of its intimacy and its significance to the individual and indeed, to users of the scheme. That connection comes from the information which comprises token identity but the connection is cemented by registration under the NIS. The nature of the information which constitutes token identity therefore means that the harm that results from its misuse by another person is fundamental and enduring.

Currently in the United Kingdom, although the damage need not be tangible for the offence of criminal damage, the property damaged must be tangible. However, while that is the situation

now, the law can, and should, develop to deal with new forms of damage to new forms of property. Like the theft offence, the criminal damage offence can be extended, by legislative amendment, to apply to intangible property like token identity.

If stomping on a policeman's cap in *Samuels v Stubbs* and the addition and deletion of files on a computer network were considered criminal damage in *R v Whiteley*,[385] then it is arguable that misuse by another person is a derangement that disrupts the intended functional connection between an individual and his or her token identity. Like the policeman's cap, token identity may appear to 'bounce' back to its original state but that does not change the fact that its integrity has been compromised because the intended integral connection between the individual and his or her token identity has been disrupted. When considered in the context of a scheme like the NIS, if ever there was an example of intangible property that *should* be covered by the criminal damage offence, it is token identity.

6.7. Conclusion

While Steel maintains that nothing of practical value is gained by extending theft to include intangible property,[386] in the case of token identity, such an extension addresses a critical gap in the protection currently provided to token identity under the criminal law in the United Kingdom and in the future, under an Australian scheme.

The new offences in the *Identity Cards Act* address the gap in relation to fraud at the time of registration but they do not cover misuse of an individual's token identity after registration.

---

[384] Model Criminal Code Officers Committee the Standing Committee of Attorneys- General, *Model Criminal Code Report, Chapter 4, Damage and Computer Offences* (2001), 17.
[385] See, above n 382.
[386] Steel, above n 322

The offences under the United Kingdom *Fraud Act* apply if another person's registered token identity is used with intent to make a financial gain or cause a loss. However, the basic wrong, that is, misuse of another person's token identity for a transaction is not an offence. Even the so called 'identity theft' provisions in South Australia do not apply to identity theft or even to identity fraud as defined in this thesis.

Other offences such as the computer offences in the *Computer Misuse Act* and the telecommunications offences such as those in the Australian *Criminal Code* may apply in some circumstances, but they generally have limited application to the type of abuse that can be expected under a national identity scheme. Use of an individual's token identity for a transaction does not necessarily involve hacking or data or program manipulation.

Under a national identity scheme like the NIS and the ACS, misuse of an individual's token identity should be a criminal offence. As this study shows, an individual's token identity is more than just information. The NIS transforms the components of token identity from information into a set which, on registration, assumes the basic characteristics of property which is capable of being the subject of theft and criminal damage.

Dishonest use of an individual's token identity by another person is not just fraud. Its use by another person is an appropriation of property. In using the token identity of another person for a transaction, the offender assumes, and thereby usurps, the individual's right to the exclusive use of his or her registered token identity and to control its use. Dishonest use of an individual's token identity fits well within the requirements of the theft offence under section

1 of the United Kingdom *Theft Act* and its equivalent in the Australian *Criminal Code*,[387] and considering the nature of the wrong and its impact on the individual it should be regarded, and labelled, as theft.

Similarly, in relation to the offence of criminal damage, although the impact of the misuse is widespread, the individual is the primary victim in terms of damage to his or her identity. The misuse does not just cause temporary inconvenience, it is an invasion of the individual's rights which affects the individual's database identity and damages his or her token identity. When misuse of an individual's token identity is intentional or reckless and without lawful authority, it should be treated as criminal and so labelled.

Digital identity is an important new concept and token identity is particularly important because of its functions under the scheme, its legal character, and its connection with an individual. It is, by its nature, susceptible to misuse which in the context of a national identity scheme like the NIS and the ACS, can have profound, far- reaching consequences for the individual as well as for users of the scheme and for the government as scheme administrator, and in its law enforcement role. Token identity is, therefore, especially deserving of protection and, as discussed in chapter 5, under the United Kingdom's national human rights regime, token identity must be adequately protected.

In determining whether an individual has a right of action for violation of his or her human rights, the protection provided by the State will be considered. Considering the nature and objectives of the NIS and the transactional role of token identity, the protection provided by the criminal law to token identity is particularly important. Moreover, while fraud offences

[387] Although as discussed, s 2(1)(b) *Theft Act* requires amendment, and s 6 could be amended to specifically

protect the interests of third parties and broader societal interests, only the theft offence protects the interests of an individual in his or her identity under the scheme. The offence of theft protects individual autonomy by protecting the individual's right to exclusive use of his or her registered token identity for a transaction.

Of course, the argument advanced in this chapter that token identity is property can be applied to give an individual, private law proprietary rights in his or her registered token identity. However, the more important point is that irrespective of whether private law proprietary rights develop, where misuse is dishonest, or it is intentional or reckless and causes damage, it should be considered criminal. The criminal law provides protection which is otherwise not available and describing the offences as theft and criminal damage, as appropriate, captures 'the moral essence of the wrong in question, by reference to the best moral conception of that essence in society as it is today.'[388]

include intent to seriously encroach on the owner's proprietary rights as has been done in South Australia.

[388] Jeremy Horder, 'Re-thinking Non Fatal Offences against the Person' (1994) *Oxford Journal of Legal Studies* 335.

7. Digital Identity – Conclusion

'The Last Enemy transports us to a Britain of the not-too-distant future, where personal information has become the weapon of a surveillance state against its own citizens, and where a super-database called 'TIA–Total Information Awareness' appears to fuse state of the art technology with a rather draconian reinterpretation of the art of the state.'[389]

'The Last Enemy is an emotional odyssey about a man in search of the truth of what happened to his brother, and to his society. It's a cautionary tale about technology, with identity cards, biometric tests and armed police becoming an everyday presence in our lives.'[390]

7.1. Introduction

The Last Enemy has not yet aired in Australia but early in 2008 it caused a sensation in England when it was screened on the BBC. The series depicts Britain transformed into a security state by a major terrorist attack. Identity cards are strictly required and citizens are watched, so the government can catch the terrorists before they strike again.

The tag line from The Last Enemy is 'tomorrow is nearer than you think' and the series presents a plausible future where a person's ability to function as an autonomous individual is dictated by the personal information which is collected and stored by the government in its identity database. The collection and use of that information was initially justified on the basis of law enforcement and public security, but the Total Information Awareness database ('TIA') is now used as a means of control. In effect, the shield has become the sword.

This situation resonates with the concerns of civil libertarians in relation to national identity schemes like the NIS and ACS, but their concerns currently tend to centre on surveillance and

---

[389] Home Secretary, '*The National Identity Scheme-Delivery Plan 2008*' Speech by the Right Honourable Jacqui Smith MP, 6 March 2008.

[390] 'A pawn in a mysterious conspiracy, he discovers to his cost just how far the country will go to protect its people. But, even as time is running out, Stephen becomes determined to find out what really happened to Michael…even at the risk of losing his own identity.' British Broadcasting Commission,'The Last Enemy' <http://www.bbc.co.uk/ drama/lastenemy> at 9 March 2008.

the implications of TIA for privacy. As this thesis shows, the potential threat to an individual's autonomy is much more fundamental. While this thesis, like The Last Enemy, is not about identity in the deep sense of who am I? or what makes me, me, the impact of the concept is significant. A person's identity as recorded in a national identity register, whether it be the NIR, the ACR, or the fictional TIA, determines that person's ability to be accurately recognised and to transact as a unique individual.

7.2. Insight Provided by this Thesis

In the context of a national identity scheme like the NIS, and the proposed ACS, an individual's identity is composed of information. An individual's database identity is a collection of defined information, a subset of which is the individual's token identity.

Database identity is the on-going narrative about an individual for the purposes of the scheme. The use of an individual's token identity as well as access to an individual's entry in the NIR by the individual and government and private sector users of the scheme is continually tracked by the system and that information becomes part of database identity. Database identity determines an individual's reputation under the scheme. Information about how the individual is regarded by the authorities and by the system, including alerts and notes, becomes part of an individual's database identity and database identity affects the way an individual is generally regarded.

The right to privacy protects the broader body of information which makes up an individual's database identity – but incompletely. Under the NIS for example, only information prescribed

by the *Identity Cards Act* can be included in the NIR and once entered, that information can be retained only for so long as it is consistent with the scheme's statutory purposes.[391]Privacy legislation such as the *Data Protection Act* governs the collection, use and disclosure of the information which comprises database identity. The right to privacy, particularly under the privacy legislation, theoretically gives an individual the right to access his or her record in the NIR, and to request corrections. However, as this study shows, the protection provided is limited and it is largely inappropriate considering the key transactional role of token identity, the inherent vulnerabilities of the system, and the consequences for an individual.

Moreover, as discussed in chapter 5, extensive power is given to the State under the *Identity Cards Act* in the interests of national security and crime detection and prevention, to record, use and disclose information without the knowledge or consent of the individual. The right to privacy therefore provides little, if any, effective redress for an individual against the power of the State under a scheme like the NIS. As is typically the case, the purposes of the NIS are broad and are based on 'public interest' which is widely defined to include national security and the prevention and detection of crime.[392] When the right to privacy is balanced against the broader societal interests, the latter often prevails, especially at a time of increased security and crime concerns.

As discussed in chapters 2 and 3, token identity plays a pivotal role under the scheme. Token identity is particularly important in the context of a national identity scheme because it is an individual's transactional identity. However, as discussed in chapter 5, token identity is not clearly protected by the privacy legislation, especially in the United Kingdom. This is largely a consequence of the decision in *Durant* but the public nature of the information which

[391] S 3(1) *Identity Cards Act*.

comprises token identity does not fit well with the notion of privacy, unless the information is considered as private in the sense of its intimate connection with an individual. Even then though, as discussed in chapters 5 and 6, such an intimate and unique connection cannot usually be established until the information which comprises token identity is considered collectively as a set. Consequently, even assuming that *Durant* does not apply,[393] the protection that can possibly be afforded to token identity by privacy legislation like the *Data Protection Act* and the *Privacy Act* and indeed, by the broader right to privacy, is inappropriate and inadequate, considering the nature of token identity.

As examined in this study, token identity has specific functions under the scheme at the time of a transaction. Token identity does not just identify: it enables a transaction with the registered identity. These functions imbue token identity with legal personality. Its legal character makes token identity a particularly important concept which will have a major impact on commercial dealings. As discussed in chapter 3, its legal character has significant ramifications for the government as administrator of the scheme and in its law enforcement role. There are also ramifications for the public and private sector users of the scheme but there are direct consequences for the individual. The argument in this thesis that token identity has legal personality has serious consequences for an individual whose token identity is misused by another person. In enforcing a contract, for example, the transacting entity will look to the individual who is attributed to that token identity in the identity register.

All identity schemes based on digital information must rely heavily on the information which is used to identify the individual. None of the identifying information used in the NIS, including the biometrics, is infallible. All have error rates, including false positives.

---

[392] See, sub-ss 1(3) and (4) *Identity Cards Act.*

Reliability depends on the type of identifying information used, the circumstances in which it is originally collected and recorded in the identity register, whether it is up to date, how it is stored and transmitted, and most importantly, the process used for comparing the information presented at the time of transaction with the information on record in the identity register. As examined in chapter 4, some identifying information such as photo comparison for example, is highly unreliable when the individual is not known to the person making the comparison. Moreover, in a large population even a seemingly low rate of error can result in a large number of mistakes.

These consequences have serious implications for law enforcement[394] and for individuals. If an individual's token identity is inaccurately registered or incorrectly verified at the time of a transaction, or if it is used by another person, the individual's ability to be correctly recognised, and to transact as a unique individual, is fundamentally affected. Most importantly, an individual can face considerable challenges in establishing not only that 'I am who I say I am' but in establishing 'I am not who the identity register says I am.' Even more difficulty can be encountered by the individual in establishing that he or she did not use his or her token identity for a particular transaction. An individual who is a victim of fraud or system error can therefore face considerable difficulty in establishing his or her innocence.

As a result, as this thesis contends, the emergent concept must necessarily give rise to fundamental human rights which encompass more than just the right to privacy. As argued in chapter 5, an individual has a fundamental right to identity. The right to identity is an established human right under international law under the *Convention on the Rights of the*

---

[393] And of course *Durant* does not apply in Australia.
[394] In its broadest sense, that is, in relation to enforcement of the civil and criminal law.

Child and the European Court has stated that it is protected in the United Kingdom under Article 8(1) of the *ECHR.*

The right to identity has special significance in the context of a national identity scheme. An individual's registered token identity is the means by which he or she is recognised and can transact and token identity is the gateway to the other information which makes up database identity. In the context of the scheme, the right to identity takes form as the right of an individual on registration, to an accurate, functional, unique token identity and to its exclusive use.

While the protection afforded to identity, especially to token identity, by the right to privacy is inadequate and inappropriate, this thesis argues that the right to identity clearly protects token identity. The right of an individual to his or her transactional identity is much less likely to be subordinated to the public interest than his or her right to privacy because infringement profoundly affects the individual's ability to be recognised and to function under the scheme. Unilateral removal or alteration of an individual's token identity will effectively disenfranchise the individual, especially in an environment in which transactions routinely require that identity be established. This thesis asserts that the effect is then so profound that it can not be justified or excused on public interest grounds, except in the most extraordinary of circumstances.

A scheme like the NIS and the ACS gives the State considerable power over individuals and their civil liberties. It has serious human rights implications. This thesis demonstrates the importance of establishing a national identity scheme within a regime which recognises and

protects human rights. The common law in the United Kingdom[395] and in Australia[396] may develop so as to provide protection for an individual.[397] However, common law development of a right to identity has not been considered in this thesis because, as discussed in chapter 5, the human rights regime in the United Kingdom has different objectives from a common law cause of action and in many ways, it provides more effective protection.

As discussed in chapter 6, the criminal law assumes particular significance in this context, primarily because of the nature of the emergent concept of digital identity and the inherent vulnerabilities of the scheme, but also because private law currently has limited application. However, in any event, misuse by another person of an individual's registered token identity should be an offence when the misuse is dishonest, or when it is intentional and reckless and causes damage. It is significant therefore that, as argued in this thesis, the offences of theft and criminal damage can apply.

The wrong and the harm caused by misuse of an individual's registered token identity by another person should be recognised as an offence in itself, rather than as a preliminary step to what is regarded as a more serious offence. As examined in chapter 6, on registration, the information which comprises token identity assumes the characteristics of property which is capable of being the subject of theft in the United Kingdom and Australia, and the subject of

---

[395] Note that in *Van Colle v Chief Constable* [2008] 3 All ER 977, 1018 different views were expressed as to whether a common law action should be developed in light of Convention rights. Lord Bingham of Cornhill endorsed the views of Pill LJ and also Rimer LJ in the Court of Appeal that 'where a common law duty covers the same ground as a convention right, it should as far as practicable, develop in harmony with it.' Lord Brown, however, rejected the argument that a parallel common law cause of action should be developed, though this view was clearly influenced by the particular circumstances of this case which concerned a claim that police had failed to protect the life of a prosecution witnesses, and a line of authorities limiting the liability faced by police officers in these circumstances.

[396] As Carolyn Evans and Simon Evans observe that '[i]t may be that , as human rights Acts become widespread across Australia, the common law will begin to change in response as judges become more used to applying rights standards…' Evans and Evans, above n 192, 214.

[397] Given the argument in this thesis that token identity is property, the common law may develop to recognise and protect the individual's proprietary rights, for example.

criminal damage in South Australia. The offences of theft and criminal damage are therefore capable of applying to misuse of token identity and they should apply because they are an important part of the suite of offences needed to protect identity. The general fraud offences and computer misuse offences apply in some circumstances but they have limited application to the type of abuse that can be expected under a national identity scheme. While the new offences enacted in the *Identity Cards Act* address fraud, especially on registration, they do not apply to misuse of an individual's registered token identity by another person. As a result, there is a major gap in the protection currently provided. This gap can be closed by treating misuse by another person of an individual's token identity, as theft or as criminal damage, as appropriate, and labelling the offence accordingly.

7.3. 'Tomorrow is nearer than you think'

In an environment in which transactions are not based on personal relationships and are automated, it is inevitable that identity will assume a crucial role in most, if not all, dealings. Under a national identity scheme, being asked to provide 'ID' will become as commonplace as being asked one's name, and the concept of identity which is the subject of this thesis will become embedded in processes essential to the national economic and social order.

The focus of this thesis is on a national scheme of identity registration using digital information and national schemes are most likely in the near future. However, a regional scheme is certainly feasible, especially for Europe. Indeed, current data sharing and the rights of citizens within the European community make such a scheme likely. A wider scheme is also possible. The token identity of individuals in countries around the world could be

recorded on a network of linked national databases. Such a scheme may seem unlikely now but globalisation is merely the next step. Nations are currently sharing digital passport, visa, work permit and other immigration information as part of border control, and digital information, including biometrics, is shared between international law enforcement and defence authorities. Under these broader schemes, an individual's registered identity becomes his or her officially recognised identity not just on a national basis but as a citizen of the region and eventually of the world. The issues discussed in this thesis then become even more significant.

Consequently, while this is the conclusion of this thesis, it is likely to be just the beginning for this emergent concept of identity, and the impact it will have on all of us. Database identity and token identity in particular, will transform the way individuals are recognised and how transactions are conducted, and will fundamentally change the commercial and legal landscape.

8. Bibliography

8.1. Articles/Books/Reports

Ashbaugh, David, *Quantitative –Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology* (1999)

Ashworth, Andrew, 'The Elasticity of Mens Rea' in C. F. H. Tapper (ed), *Crime, Proof and Punishment: Essays in Memory of Sir Rupert Cross* (1981) 45

Ashworth, Andrew, *Principles of Criminal Law* (5th ed, 2006)

Avery, Lisa, A Return to Life: The Right to Identity and the Right to Identify Argentina's 'Living Disappeared' (2004) 27 *Harvard Women's Law Journal* 235

Baker, C Edwin, 'Property and its Relation to Constitutionally Protected Liberty' (1986) 134(4) *University of Pennsylvania Law Review* 741

Bentham, Jeremy, *An Introduction to the Principles of Morals and Legislation*, W Harrison (ed) (1948)

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

Bruce, Vicki and Young, Andy, 'Understanding Face Recognition' (1986) 77(3) *British Journal of Psychology* 305

Bruce, Vicki et al, 'Verification of Face Identities from Images Captured On Video' (1999) 5(4) *Journal of Experimental Psychology* 339

Bruce, Vicki et al, 'Matching Identities of Familiar and Unfamiliar Faces caught on CCTV Images' (2001) 7(3) *Journal of Experimental Psychology: Applied* 207

Buergenthal, Thomas, 'International Human Rights Law and Institutions: Accomplishments and Prospects' (1988) 63 *Washington Law Review* 1

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

Carter, J W, Peden, Elisabeth and Tolhurst, GJ, *Contract Law in Australia*, (5th ed, 2007)

Chalmers, James and Leverick, Fiona, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 217

Champod, Christopher and Evett, Ian, 'A Probabilistic Approach to Fingerprint Evidence' (2001) 51 *Journal of Forensic Identification* 101

Cohen, Morris, 'Property and Sovereignty,' (1927) 13 *Cornell Law Quarterly* 12

Cole, Simon,'Grandfathering Evidence: Fingerprint Admissibility Rulings from Jennings to Llera Plaza and Back Again' (2004) 41 *American Criminal Law Review* 1226

Cole, Simon, 'More than Zero, Accounting for Error in Latent Fingerprint Identification' (2005) 95 *Journal of Criminal Law and Criminology* 985

Conte, Frances, 'Sink or Swim Together: Citizenship, Sovereignty, and Free Movement in the European Union and the United States' (2007) 61 *University of Miami Law Review* 331

Davies, Graham and Thasen, Sonya, 'Closed Circuit Television: How Effective an Identification Aid?'(2000) 91(3) *British Journal of Psychology* 411

Davies, Margaret and Naffine, Ngaire, *Are Persons Property? Legal Debates About Property and Personality* (2001)

Delbridge, Arthur and Bernard, J R L (eds) *The Concise Macquarie Dictionary* (2nd ed, 1992)

Derham, David, 'Theories of Legal Personality' in Webb, Leicester (ed), *Legal Personality and Political Pluralism* (1958) 1

Detrick, Sharon, *The United Nations Convention on the Rights of the Child. A Guide to the "Travaux Preparatoires*" (1992)

Ducor, P, 'The Legal Status of Human Materials' (1996) 44 *Drake Law Review* 195

Evans, Carolyn and Evans, Simon, *Australian Bills of Rights* (2008)

Fox, Richard, Infringement Notices: Time for Reform, No 50 *Trends and Issues in Crime and Criminal Justice* (1995)

Frowd, Charlie Bruce, Vicki McIntyre Alex and Hancock, Peter, 'The Relative Importance of External and Internal Features of Facial composites' (2007) 98 *British Journal of Psychology* 61

Galton, Francis, *Fingerprints* (1892)

Garfinkel, Simson, Database Nation: *The Death of Privacy in the 21st Century* (2000)

Gray, Kevin, 'Property in Thin Air' (1991) 50 *Cambridge Law Journal* 252

Gavison, R, 'Privacy and the Limits of the Law' (1980) 89 *Yale Law Journal* 421

Goglan, Andy, 'How far should prints be trusted?' 17 September 2005 *New Scientist* 6

Gordon, Robert W.' Paradoxical Property in John Brewer and Susan Staves (eds) *Early Modern Conceptions of Property* (1996) 95

Gray, Thomas C 'The Disintegration of Property' in Pennock, J. Roland and Chapman, John W (eds) *Nomos XX11: Property* (1980)

Greenleaf, Graham, 'Australia's proposed ID Card: Still Quacking like a Duck,' (2007) *University of New South Wales Faculty of Law Research Series* 1

Grieve, David, 'Possession of Truth' (1996) 46 *Journal of Forensic Identification* 521

Hancock, Kirsten and Rhodes, Gillian, 'Contact, Configural Coding and the Other –Race Effect in Face Recognition' (2008) 99 *British Journal of Psychology* 45.

Hancock , Peter , Bruce, Vicki and Burton , A. Mike, 'Recognition of Unfamiliar Faces' (2000) 4 (9) *Trends in Cognitive Science* 330

Harrison, W, (ed) *An Introduction to the Principles of Morals and Legislation* (1948)

Harvey, Colin and Barnidge, Robert 'Human Rights, Free Movement, and the Right to Leave in International Law (2007) 19(1) *International Journal of Refugee Law* 1

Haunch, J, 'Protecting private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris' (1994) 68 *Tulane Law Review* 1238

Hohfeld, Wesley, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) 23(1) *Yale Law Journal* 16

Home Office, *National Identity Scheme Delivery Plan 2008* (2008)

Honoré Anthony, 'Ownership' in AG Guest (ed) *Oxford Essays in Jurisprudence* (1961)

Horder, Jeremy, 'Re-thinking Non Fatal Offences against the Person' (1994) *Oxford Journal of Legal Studies* 335

Information Commissioner, *Entitlement Cards and Identity Fraud. The Information Commissioner's Response to the Government's Consultation Paper*, 30 January 2003

Lawson, F.H, 'The Creative Use of Legal Concepts' (1957) 32 *New York University Law Review* 909

Kaye, David, 'Questioning a Courtroom Proof of Uniqueness of Fingerprints' (2003) 71 *International Statistics Review* 521

Kelsen, Hans, *Pure Theory of Law* (Max Knight trans, 1970 ed)

Kemp, Richard, Towell, Nicola and Pike, Graham, 'When Seeing should not be Believing: Photographs, Credit Cards and Fraud'(1997) 11(3) *Applied Cognitive Psychology* 211

Kersholt, Jose, Raaijmakers, Jeron and Valeton, Mathieu, 'The Effect of Expectation on the Identification of Known and Unknown Persons' (1992) 6 *Applied Cognitive Psychology* 173

Korff, Douwe, *EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws* (2002)

Lee, Henry and Gaensslen, Robert, *Advances in Fingerprint Technology* (2001)

Lopucki, Lynn M, 'Did Privacy Cause Identity Theft?'(2002-2003) 54 *Hastings Law Journal* 1277

LoPucki, Lynn M, 'Human Identification Theory and the Identity Theft Problem' (2001-2002) 80 *Texas Law Review* 89

Mansfield, Tony and Rejman-Green, Marek, *Feasibility Study on the Use of Biometrics in an Entitlement Scheme,* February 2003

McCullagh, Karen, '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 <http//:www.biletapapers/brombyness.html> at 27 April 2005

Minister for Human Services' Consumer and Privacy Taskforce, *Discussion Paper on the Registration Process*, Discussion Paper >http:/www.accesscard.gov.au/various /Registration% 20Paper%FINAL%20 Released %2023%20 March.pdf> at 20 March 2006

Model Criminal Code Officers Committee the Standing Committee of Attorneys- General, *Model Criminal Code Report, Chapter 4, Damage and Computer Offences* (2001)

Model Criminal Law Officers' Committee of the Standing Committee of Attorneys- General, *Final Report Identity* Crime March 2008

Mohr, Richard, 'Identity Crisis: Judgment and the Hollow legal Subject,' 2007 11 *Passages – Law, Aesthetics, Politics* 106

Munzer, Stephen, *A Theory of Property* (1990)

Naffine, Ngaire, 'Who are Law's Persons? From Cheshire Cats to Responsible Subjects' (2003) May *Modern Law Review* 346

Neethling J, Potgeiter J and Visser P, *Neethling's Law of Personality* (2005)

Nekam, Alexander, *The Personality Conception of the Legal Entity* (1938)

Orwell, George, *Nineteen Eighty-Four* (1949)

Palmer, Stephanie, 'Public , Private and the Human Rights Act 1988: An Ideological Divide'(2007) *Cambridge Law Journal* 559

Pankanti, Sarath, Prabhakar, Salil and Jain, Anil, 'Transactions on Pattern Analysis and Machine Intelligence' (2002) 24 (8) *Institute of Electrical and Electronics Engineers Transactions On Pattern Analysis and Machine Intelligence* 1010

Picard, E, 'The Right to Privacy in French Law' in B S Markes (ed) *Protecting Privacy* (1999) 49

Reich, Charles, 'The Individual Sector' (1990-1991) *Yale Law Journal* 1409

Reich, Charles, 'The New Property' in Macpherson, C.B. (ed) *Property Mainstream and Critical Positions* (1978) 177

Risinger, Michael et al, 'The Daubert /Kumho Implications of Observer Effects in forensic Science : Hidden Problems of Expectation and Suggestion' (2002) 90 *California Law Review* 1

Shute, S and Horder, Jeremy, 'Thieving and Deceiving: What is the Difference?' (1993) 56 *Modern Law Review* 548

Singer, Joseph William, Entitlement: The Paradoxes of Property (2000)

Smith, JC, *The Law of Theft* (8th ed, (1997)

Solove, Daniel, 'Identity Theft, Privacy and the Architecture of Vulnerability (Enforcing Privacy Rights Symposium)' (2003) 54 *Hastings Law Journal* 1227

Solove, Daniel, 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure' (2003) 53 *Duke Law Journal* 967

Solove, Daniel, 'Power and Privacy: Computer Data Bases and Metaphors for Information' 2001 53 *Stanford Law Review* 1393

Solove, Daniel, *The Digital Person, Technology and Privacy in the Information Age* (2004)

Stacey, Robert, 'A Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case' (2004) 54 *Journal of Forensic Identification* 706

Steel, Alex, 'Intangible Property as Theft,' (2008) 30 *Sydney Law Review* 575

Stevenage, Sarah and Spreadbury, John, 'Haven't we Met Before? The Effect of Facial Familiarity on Repetition Priming' (2006) 97(1) *British Journal of Psychology* 79

Stigler, Stephen, *Statistics on the Table* (1999)

Stoney, David, 'Critique' in Lee, Henry and Gaensslen, Robert, *Advances in Fingerprint Technology* (2001)

Sullivan, Clare, 'The United Kingdom Identity Cards Act 2006– Proving Identity?' (2006) 3 *Macquarie Journal of Business Law* 259

Sykes, J B (ed), *Concise Oxford Dictionary* (6th ed, 1976)

Tur, Richard, 'The 'Person' in Law' in Arthur Peacocke and Grant. Gillett (Eds), (1987) *Persons and Personality: A Contemporary Inquiry* 116

Underkuffler, Laura S, *The Idea of Property* (2003)

Underkuffler, Laura S, 'On Property'(1990) *Yale Law Journal* 127

United Kingdom Information Commissioner, *The Identity Cards Bill – The Information Commissioner's Concerns* (June 2005) <http://www.ico.gov.uk/eventual.html >at 10 May 2006

Wadham, John Gallagher , Coailfhionn, Chrolavicius, Nicole, *The Identity Cards Act 2006* (2006)

Waldron, Jeremy, *The Right to Private Property* (1986)

Walker, Pamela and Hewstone, Miles, 'A perceptual Discrimination Investigation of the Own-Race Effect and Intergroup Experience' (2006) 20 (4) *Applied Cognitive Psychology* 461

Weber, Max, '"Objectivity" in Social Science' in E. Shils and H. Finch (eds) *The Methodology of the Social Sciences*, (1949) 90 – 1

Vogt, Evon and Hyman, Ray, *Water Witching* (1979)

Zabell, Sandy, 'Fingerprint Evidence' (2005) 13 *Journal of Law and Policy* 143

8.2. Case Law

Amann v Switzerland (2000) 30 EHRR 843

Australian Broadcasting Commission v Lenah Game Meats (2001) 208 CLR 199

Bodil Lindqvist EU Court of Justice Dec C101-01

Campbell v Mirror Group Newspapers Ltd [2004] 2 AC 457

Chan Man-sin v Regina [1988] 1 WLR 196

Copeland v United Kingdom (2007) 45 EHRR 37

Cundy v Lindsay [1878] 3 App Cas 459

Davies v Flackett [1972] Crim L R 708

Doe v ABC [2007] VCC 281

DPP v Lavender [1994] Crim LR 297, CO/2779/92 Unpaginated transcript (John Larking)

Durant v Financial Services Authority [2003] EWCA Civ 1746

Filartiga v Pena-Irala, 630 F.2d 876, 883 (2d cir.1980)

Funke v France, judgment of February 23, 1993, Series A No.256-A; (1992)16 EHRR 297

Gaskin v United Kingdom (1990) 12 EHRR 36

Grosse v Purvis [2003] QDC 151

In re S (a child) [2005] 1 AC 593

Ingram v Little [1961] 1 QB 31

Johnson v Medical Defence Union Ltd [2005] WLR 750

Johnson v The Medical Defense Union [2007] EWCA 262

Kennison v Daire (1985) 38 SASR 404

Kennison v Daire (1986) 160 CLR 129

King's Norton Metal Co v Eldridge, Merrett & Co Ltd (1897) 14 TLR 98

Leander v Sweden (1987) 9 EHRR 433

Lewis v Avery [1972] 1 QB 198

Lindqvist v Sweden [2003] ECR I-12971, 24

Lord Browne of Madingley v Associated Newspapers Limited [2007] EWCA Civ 295

Malone v The United Kingdom (1985) 7 EHRR 14

Mabo No 2 v Queensland [No 2] (1992) 175 CLR 1

Marleasing SA v La Commercial International de Alimentatcion SA (Case C-106/98) (1990 ECR 1-4135

MC v Bulgaria (2005) 40 EHRR 20

National Provincial Bank v Ainsworth [1965] AC 1175

National Trustees Executors & Agency Co of Australasia Ltd v FCT (1954) 91 CLR 540

Österreichischer Rundfunk v Austria [2003] ECR 4989

Oxford v Moss (1978) 68 Criminal Appeal Reports 183

Papas v Bianca Investments Pty Ltd (2002) 82 SASR 581

Peck v United Kingdom [2003] All ER 255, (2003) 36 EHRR 719, [2003] EMLR 287

PG and JH v United Kingdom [2001] HRCD 707, ECHR 2001-IX

Phillips v Brooks Ltd [1919] 2 KB 243

Porter v Latec Finance (Qld) Pty Ltd (1964) 111 CLR 177

Roberson v Wakefield Metropolitan District Council and Another [2002] 2 WLR 889

Rotaru v Romania (28341/95) 8 BHRC 449

Rundfunk v Austria, [2003] ECR 4989

R v Chief Constable of South Yorkshire Police ex parte LS and Marper [2002] 1 WLR 3223

R v Feely [1973] 1 QB 530

R v Ghosh [1982] QB1053

R v Gomez [1993] AC 442

R v Hall [1848-9] Law Times 383

R v Hinks [2001] 2 AC 241

R v Morris [1984] AC 320

R v Rooney [2006] EWCA Crim 1841

R v Secretary of State for Transport ex parte Factorame (No 2) [1991] 1 AC 603

R v Waterfall [1970] 1 QB 148

R v Whiteley (1993) 93 Cr App Rep 25

Samuels v Stubbs (1972) 4 SASR 200

Segerstedt –Wiberg v Sweden (2007) 44 EHRR 2

Shogun Finance Ltd v Hudson [2004] 1 AC 919

Van Colle v Chief Constable [2008] 3 All ER 977

Von Colson and Kamann v Land Nordrhein-Westfalen (Case 14/83) [1984] ECR 1891

Wagner Miret v Fondo de Guarantia Salaria (Case C-334/92) [1993] ECR 1-6911

Yanner v Eaton (1999) 201 CLR 351

YL v Birmingham City Council [2007] UKHL 27

Z v Finland, judgment of February 25, 1997, Reports of judgments and Decisions 1997-I, No 31

8.3. Legislation

Australia

Anti -Money Laundering/ Counter-Terrorism Financing Act 2006 (Cth)
Anti-Money Laundering/ Counter-Terrorism Financing Rules
Australian Constitution
Charter of Human Rights and Responsibilities Act 2006 (Vic)
Crimes Act 1900 (NSW)
Crimes (Theft) Act 1973 (Vic)
Criminal Code Act 1995 (Cth)
Criminal Code Act 1995 (Cth)
Criminal Code (Cth)
Criminal Code 1899 (Qld)
Criminal Code 2002 (ACT)
Criminal Code Act (NT)
Criminal Code Act 1899 (Qld)
Criminal Code Act 1924 (Tas)
Criminal Code Act 1913 (WA)
Criminal Law Consolidation Act 1935 (SA)
Equal Opportunity Act 1995 (Vic)
Fauna Conservation Act 1974 (Qld)
Gambling Regulation Act 2003 (Vic)
Human Rights Act 2004 (ACT)
Law Enforcement and National Security (Assumed Identities) Act 1998 (NSW)
Migration Act 1958 (Cth)
Native Title Act 1993 (Cth)
Privacy Act 1988 (Cth)
Witness Protection Act 1994 (Cth)

United Kingdom

Computer Misuse Act 1990 (UK) c 18
Criminal Justice and Public Order Act 1994 (UK) c 33
Criminal Damage Act 1971 (UK) c 48
Data Protection Act 1998 (UK) c 29
Fraud Act 2006 (UK) c 35
Human Rights Act 1998 (UK) c 42
Identity Cards Act 2006 (UK) c 15
Local Government Act 1972 (UK) c 70
Regulation of Investigatory Powers Act 2000 (UK) c 23
Serious Organised Crime and Police Act 2005 (UK) c 15
Theft Act 1968 (UK) c 60

Other Jurisdictions

Bill of Rights Act 1990 (NZ)

Identity Theft and Assumption Deterrence Act 1998.18 USC 1028(a)

Code Civile (France)

8.4. Treaties

Charter of Fundamental Rights of the European Union (Official Journal of the European Communities 2000/C 364/01) 18 December 2000

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (European Treaty Series No.108, Strasbourg, 1981)

Convention on the Rights of the Child opened for signature 20 November 1989 1558 UNTS 530 (entered in to force in the United Kingdom 16 December 1991) (entered into force in Australia 16 January 1991)

Data Protection Directive 95/46 EU of the European Parliament and of the European Council of 24 October 1995

European Convention for the Protection of Human Rights and Fundamental Freedoms (Opened for signature 4 November 1950) 213 UNTS 221 (entered into force 3 June 1952)

8.5. Other Sources

Australian Broadcasting Commission <http://www.abc.net.au/4corners/achives/2002. html> at 10 May 2006

Australian Government, Submission to the Senate Enquiry on the Human Services (Enhanced Service Delivery) Bill 2007

'Belgium Starts First Phase of Smart Card Rollout', Card Tech Today, May 2003, 3

British Broadcasting Commission, News 'Q&A Identity card plans' <http://www. newsvote.bbc.co.uk.html> at 3 April 2006

British Broadcasting Commission <http//:www.bbc.co.uk.panorama.html> at 29 May 2006

British Broadcasting Commission, 'Rethink on Identity Cards http://www.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_new/politics> at 7 March 2008

British Broadcasting Commission, 'The Last Enemy'<http://www.bbc.co.uk/drama/lastenemy> at 9 March 2008

eID Services, eID <http//:eid.belgium.be/en/navigation/12000/index.html> at 9 May 2007

Explanatory Notes, Identity Cards Act 2006 (UK), 9 <http//:www.opsi.gov.uk.html> at 19 May 2006

Explanatory Memorandum, Human Services (Enhanced Service Delivery) Bill 2007

'*Face Off*', Paramount Pictures (1997)

Geoghegan, Tom, 'I've got a Biometric ID Card', *British Broadcasting News* (London), 12 August 2004 <http://news.bbc.co.uk/go/pr/fr/1/hi/uk/3556720.stm> at 29 March 2007

Heath, David and Bernton, Hal, 'Portland Lawyer Released in Probe of Spain Bombings' *Seattle Times* (Seattle), 21 May 2004, 1

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> at 16 May 2006

Home Secretary, *IPPR Speech* (2004) <http://www.identitycards. gov.uk./publications.html> at 16 May 2005

Home Secretary, '*The National Identity Scheme – Delivery Plan 2008'* Speech by the Right Honourable Jacqui Smith MP, 6 March 2008

Hughes, Gary, 'Passport to Fraud', *The Age* (Melbourne), 6 July 2003 <http://www.theage.com.au /articles/2003/07/06/105 7179212905.htmlpage> at 30 October 2008

Human Services (Enhanced Service Delivery) Bill (Cth) 2007

Identity and Passport Service, *Corporate and Business Plans 2006–2016* <http//:www.identitycards.gov.uk/scheme.html> at 10 May 2006

Identity and Passport Service, *Corporate and Business Plans 2006–2016* <http//:www.ips.gov.uk/identity/publications-corporate.asp> at 1 September 2008

Identity and Passport Service, *Framework Agreement*, 10: <http//:www. identitycards.gov.uk.html> at 16 May 2006

Identity and Passport Service, *Framework Agreement*, 14 <http//:www.ips.gov./idenity/ publications-general.asp.l> at 1 September 2008

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

Identity and Passport Service, *What is the National Identity Scheme*? <http//:www.ips.gov.uk /identity/scheme-what-produced.asp> at 1 September 2008

Identity and Passport Service, *How the National Identity Scheme will get Started* <http//:www. identity cards.gov.uk/scheme.html> at 10 May 2006

Identity and Passport Serivce, *Benefits to* Society <http://www.ips.gov.uk/ identity/how-idcard-daily-providing.asp> at1 September 2008

Identity and Passport Service, *Benefits to the Individual*<http://www.ips.gov. uk/identity/benefits -individual-british. asp> at 1 September 2008

Identity and Passport Service, *Biometrics* <http//: www.identitycards.gov. uk/scheme.html> at 10 May 6

Identity and Passport Service, *What Biometrics will You be Using?* <http//:www.identitycards. gov.uk/scheme.html> at 10 May 2006

Identity and Passport Service, *Using the Scheme in Daily Life* <http://www.identitycards. gov.uk/scheme.html> at 10 May 2006

Identity and Passport Service, *Using the scheme in daily life, Transferring money*, <http//:/www. identity cards.gov.uk/scheme.html> at 10 May 2006

Identity and Passport Service, *Using the Scheme in Daily* Life <http://www.ips.gov.uk /identity/how-idcard-daily-providing.asp.> at1 September 2008

Identity and Passport Service, *What is the Benefit of Using Biometrics* <http//:www.ips. gov.uk/identity/faqs-biometrics-benefits.asp.www.identitycards.gov.uk/scheme.html> at 1 September 2009

Identity and Passport Service, *What Kind of Organizations will use the Scheme?* <http://www.identity cards.gov.uk/scheme.html> at 10 May 2006

Identity and Passport Service, *What Kind of Organizations will use the Scheme?* <http://www.ips.gov.uk/identity/how-organisations.aspl> at 1 September 2008

Identity and Passport Service, *Benefits to Society* <http://www.identitycards.gov.uk/scheme.html> at 10 May 2006

Johnstone, Philip 'Iris Scans Dropped from ID Card Plans', *Telegraph*,(London) 12 January 2007 <http://telegraph.co.uk/ core/Content /displayPrintable.jhtml;jsessionid= DWNA31GV> at 29 March 2007

Kershaw, Sarah, 'Spain and US at Odds on mistaken Terror Arrest' *New York Times* (New York), 5 June 2004, A1

'New Fingerprint Technology' <http//:www.news10now.com/content/top_stories> at 28 May 2006

News10 now <http//:www. news10now.com/content/top_stories> at 28 May 2006

Morris, Nigel, 'Big Brother: What it Really Means in Britain Today,' *The Independent* (London), 15 January 2007 <http//:www.news:theindependent.co.uk/uk/politics/article 2154844.ece> at 29 March 2007

Regulatory Impact Assessment, Identity Cards Bill Introduced to House of Commons on 25 May 2005 (UK) <http//:www.homeoffice.gsi.gov.uk.html> at 16 May 2006

Sherriff, Lucy, 'UK Ditches Single ID Database' *The Register*, (London), 19 December 2006 <http//:www.theregister.co.uk/ 2006/ 12/19/bigbro_cubed/print/html> at 29 March 2007

'*Sleepless in Seattle*,' Tristar Pictures Inc (1993)

'*The Net*,' Columbia Pictures Industries Inc (1995)

Tizon, Tomas Alex, et al, 'Critics Galvanized by Oregon Lawyer's Case' *Los Angeles Times* (Los Angeles) 22 May 2004, 13

United Kingdom, Parliamentary Debates, House of Lords, 30 January 2006, col 79 (Baroness Scotland of Asthal)