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.' [308]

6.1 Introduction

In this chapter I consider the protection afforded by the criminal law to transaction identity. The analysis builds on the examination of the functions and legal nature of transaction 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 of an individual's transaction identity, in the context of a national identity scheme like the NIS, assumes considerable significance.

I argue that dishonest misuse of an individual's registered transaction 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.

308 *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 transaction identity is dishonestly used with intent to make a financial gain or loss.[309] However, although these offences are wide-ranging, in the context of such a scheme transaction 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 transaction 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 transaction identity after registration. Consequently, there is a gap in the protection currently provided by the law that can be filled by the theft offence. Treating misuse of another individual's transaction 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.[310]

I contend that misuse of an individual's registered transaction identity by another person for a transaction is capable of meeting all of the elements required for theft. Central to this argument is the assertion that that transaction 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 ownership of that property. The misuse is a dealing in disregard of the individual's right to exclusive use and control of his or her transaction identity.

I take issue with the view 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

309 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'.

310 The theft offence in the Australian federal *Criminal Code* contains the same elements. See s 131.1(1) which provides that a person is guilty of an offence if 'the person dishonestly appropriates property belonging to another with the intention of permanently depriving the other of the property.'

> taking any physical document or thing, would not deprive the person of the ability to use that information.[311]

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 its appropriation cannot possibly cause permanent deprivation. But an individual's transactional identity under the NIS is more than just information. As discussed in previous chapters, transaction identity has specific functions under the scheme that give it legal character. It is against that background that this chapter argues that registration gives transaction identity the characteristics of property that is capable of being misappropriated.

Transaction identity can also be damaged by misuse. Recognising that transaction 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 that results from misuse of an individual's transaction identity by another person and because, unlike theft, dishonesty is not a requirement for the offence. This chapter argues that misuse of an individual's transaction 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.[312]

The discussion in this chapter is directly relevant to the NIS but it has implications for similar existing schemes and for Australia in relation to any future national identity scheme and its impact on human rights. Following on from chapters 4 and 5, this chapter uses the NIS as the model for the analysis. However, the issues are also applicable to other similar schemes, particularly the ACS 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, transaction identity would be established by Commonwealth legislation. As property established by Common-

311 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.

312 S 85(3) *Criminal Law Consolidation Act.*

wealth legislation, transaction identity would be covered by Commonwealth theft law,[313] 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,[314] is considered to apply to an individual's transaction 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.

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 transaction 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 I examine later in this chapter.

In examining theft, I distinguish 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. I then consider the elements of the theft offence in relation to misuse of an individual's transaction 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. I consider the South Australian offence, which applies to intangible property, in relation to the damage caused by misuse of transaction 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 Transaction Identity

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

313 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.*

314 See s 131.1(1) (b). S 131.1 is a slightly modified version of the United Kingdom theft offence in the *Theft Act.*

time of a transaction singles out a registered identity from those recorded on the register and authorises the system to deal with that identity. Transaction identity acts as the metaphorical key which enables the system to transact.

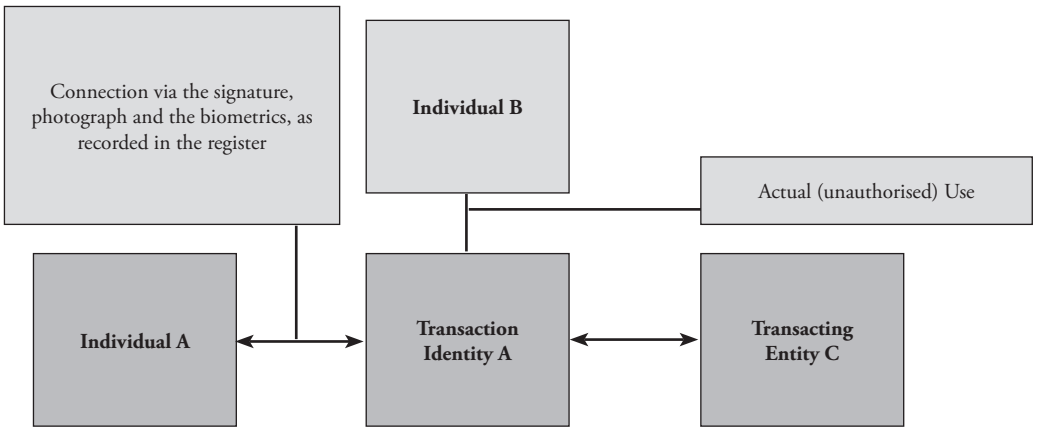
Misuse of an individual's transaction identity by another person for a transaction is made possible by the verification process under the scheme. Identity is verified when the required transaction identity information, as presented, matches the record in the register. Recall from the discussion in chapters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

As mentioned in chapter 3, 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 photograph, comparison of the handwritten signature, and/or comparison of biometrics. Routine transactions conducted in-person usually require a match with the photograph or a signature. Use of biometrics makes misuse more difficult (although not impossible) but biometrics are only used for significant financial transactions under the NIS[315] and were not planned for the ACS. 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 2, their purpose is really to check that the transaction identity is in the right hands. This additional information is not part of transaction identity.

Use of the transaction identity of individual A by another person B, for example, exploits the presumption that the transaction identity is presented by A, but as argued in chapter 3, the transaction is between the transacting entity and identity A. Transaction 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:

315 Identity and Passport Service, *Using the Scheme in Daily Life* <ips.gov.uk> at 1 September 2008. and Directgov, *'Identity cards: an introduction'* <direct.gov.uk> at 19 January 2010.

Figure 12



Assuming absence of conspiracy between B and A (and C), if B presents A's transaction identity as his or her own, A is the primary victim. In this situation, B has presented A's transaction identity and the transacting entity C will seek to enforce the transaction against individual A as the obvious, presumed administrator of transaction 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 or that the record will be retained for future comparison. Without such a record, the biometric presented cannot subsequently be compared to the biometric in the register, nor to the individual suspected of using the transaction identity for the transaction.

The wrong is the use of A's transaction identity by another person and the wrong occurs at the time of the misuse. The wrong is primarily to the individual whose transaction 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 transaction identity is used by another person for a transaction but the nature of transaction identity and its functions under the scheme mask the true effects of the misuse. While harm it not necessary for theft, the harm caused by the misuse nevertheless reveals the impact on the individual as the primary victim, and the harm caused to transaction identity is directly relevant to the offence of criminal damage which I argue should apply to intentional or reckless misuse.

The intangible nature of transaction 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. However, the enduring nature of the information that comprises transaction

identity and its unique association with an individual under the scheme[316] means that misuse of an individual's transaction identity by another person impairs that unique and exclusive association.

The misuse does not necessarily render the transaction identity useless to the individual either during or after misuse. Use by another person will not prevent the individual from using his or her transaction 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 transaction 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 register while details of the transaction are also recorded in the database of the transacting entity. This is the case for all transactions under the NIS, irrespective of whether they are with a government or a private sector entity. Consequently, the use of the individual's transaction identity for a transaction becomes part of the individual's database identity under the scheme[317] while 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. In the meantime, however, 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.

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' [318] (emphases added). Under a national identity scheme like the NIS and ACS, the set of information that is an individual's identity for the particular transaction is indicia of identity.

316 Even if a victim can use a new transaction 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.

317 Recall that public sector databases are to be generally accessible under the scheme.

318 *Neethling*, above n 207, 36.

I argue that identity theft is the dishonest use of an individual's transaction identity for the particular transaction. Theft therefore only applies to a transaction with a transacting entity under the scheme for which the individual is required to provide his or her transaction identity. 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. Under such a scheme, most commercial transactions entered into by an individual with public and private sector businesses are envisaged to be transaction identity dealings.

As discussed, the transaction identity information required depends on the particular transaction but always comprises name, date and place of birth, gender and identifying information such as comparison of photograph, signature, or biometrics which under the NIS are initially limited to fingerprints. For example, a transaction may require name, date and place of birth, gender and 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 register) for the transaction, I argue that use of that set of information constitutes theft of the individual's transaction identity. That use is identity theft as defined in this book.

By contrast, identity fraud is essentially deception as to any database identity information including transaction 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 book. 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 that 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 scheme.

While adding a current address to the set of information narrows the field significantly, the *Identity Cards Act* separates 'identity' from residential address/es,[319] 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 that constitutes transaction 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

319 See s 1(5) *Identity Cards Act.*

information cannot be considered to be the indicia of identity, unless it is the set required to establish identity for a transaction under the scheme.

Use of just the identifying information of another individual such as photograph and/or fingerprints is also insufficient to constitute theft. Consider the situation depicted in *The Net,* where Angela Bennett's fingerprints and photo are recorded with the name, address and social security number[320] of another person, Ruth Marx, to create a false identity. If this situation arises because of data manipulation as occurred in *The Net,* the activity is usually caught by specific computer crime offences which include hacking,[321] unauthorised modification of computer material[322] and, depending on the circumstances, unauthorised access with intent to commit or facilitate the commission of further offences.[323] However, the more likely scenario in the context of a scheme like the NIS is that a person will register using biographical information that relates to another person but will provide his or her own identifying information such as photograph and fingerprints.

On registration, that biographical information is 'sealed to or permanently paired'[324] 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 transaction 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 the fraudster of that registered transaction identity is fraudulent but it is not identity theft as defined in this book.

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

320 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 transaction identity, under the NIS.

321 *Computer Misuse Act 1990* (UK) c 18 (*'Computer Misuse Act*'). See also, s 478.1 Australian federal *Criminal Code.*

322 *Computer Misuse Act.* See also s 477.2 and s 478 Australian federal *Criminal Code.*

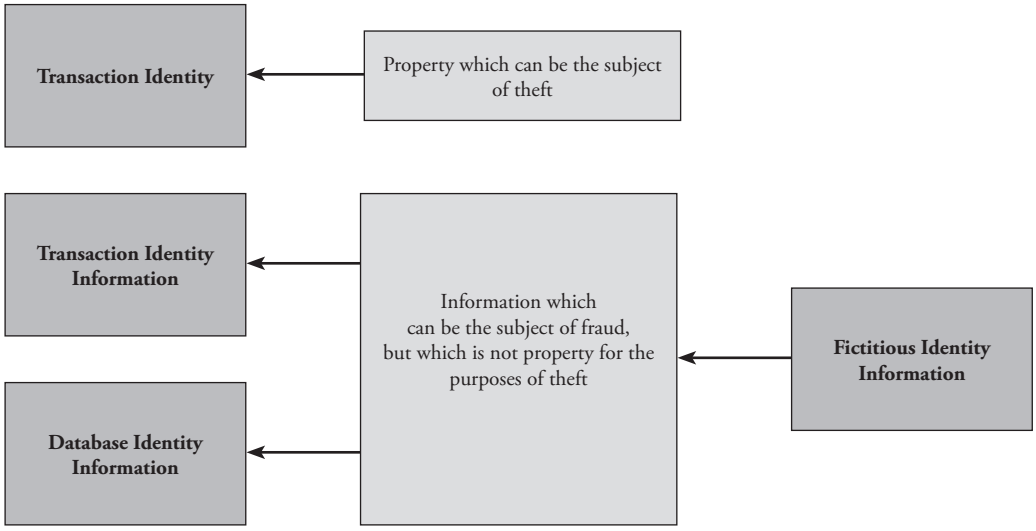
323 Computer Misuse Act. See also s 477.1 Australian federal *Criminal Code.*

324 Identity and Passport Service, *Biometrics* <identitycards.gov.uk> at 10 May 2006.For recent version of this statement, see Identity and Passport Service, *'What is the National Identity Scheme?'* <ips.gov.uk> at 1 September 2008.

although that person does not still have to be alive, as long as the identity is registered under the scheme.[325]

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

Figure 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 sui generis offences.'[326] However, I argue that dishonest use of an individual's transaction 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 transaction 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 transaction identity, which I argue 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

325 Recall that transaction identity includes date of death. See s 1(7) *Identity Cards Act.*

326 Alex Steel, 'Intangible Property as Theft' (2008) 30 *Sydney Law Review* 575. A sui generis offence is a offence which specifically addresses a particular crime. Computer offences such as those in the *Computer Misuse Act,* and the new offences in the *Identity Cards Act,* are examples of sui generis offences.

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', [327] 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,*[328] which are examples of the sui generis offences to which Steel refers, have limited application to the types of misuse that can be expected in the context of a scheme like the NIS. Use of an individual's transaction identity by another person does not necessarily involve modification of data[329] nor modification or impairment of electronic communication[330] and, arguably, access is not unauthorised as required by section 1(1) of the *Computer Misuse Act*.[331]

327 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 transaction 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 transaction identity. In Australia, see 6.4also s 134.2 *Criminal Code* which refers to 'financial advantage'.

328 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*.

329 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 transaction 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.

330 In Australia, see for example, ss 476.4 and 474.6 *Criminal Code*.

331 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 transaction identity. Nevertheless, in specific circumstances, the offence under s 1 can apply to misuse of an individual's registered transaction 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, however, that although these offences may be invoked in some circumstances, they do not fit misuse of transaction identity like theft or, indeed, criminal damage.

Even the 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 transaction 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. For example, 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 either identity theft nor identity fraud, as defined in this book, an offence per se. Instead, the offence is the use of another person's 'personal identification information',[332] 'intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence'.[333] 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.[334] It is a common approach, the rationale being that identity crime is often a preliminary step to a (more) serious crime.[335] 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 section 144 of the South Australian *Criminal Law Consolidation Act*, for example, defines as an indictable

332 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.

333 See, for example, s 144A *Criminal Law Consolidation Act* which defines 'serious criminal offence' to mean 'an indictable offence' or '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 311, 25.

334 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'.

335 This approach 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.

offence or a prescribed offence. Labelling these offences 'identity theft'[336] and 'identity crime'[337] can therefore be misleading.

Section 144 of the *Criminal Law Consolidation Act* 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;
(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 that comprise transaction identity under the United Kingdom scheme and under the ACS. However, a defined concept of identity for transactional purposes is not evident in the provision.[338]

Moreover, as noted above, dishonest misuse of an individual's transaction 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 is theft, specifically identity theft and should be labelled accordingly. As Andrew Ashworth observes, the concern lying behind fair labelling or representative labelling, as it was originally termed,[339] 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-

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

337 The title of the model offences recommended by the MCLOC is 'Recommended model identity crime offences'. See MCLOC, above 311, 25.

338 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 transaction identity into the additional information which comprises database identity.

339 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.

breaking'.[340] As Ashworth notes, labelling is important for reasons of 'proportionality' to provide 'maximum certainty' and he touches on the importance of legal definitions reflecting 'common patterns of thought in society'.[341] This reasoning has been supported by recent research that shows that description and differentiation are the two most important considerations in the accurate labelling of offences.[342] A description that accurately describes the offence is the most important consideration for the general public. A label which clearly differentiates the nature of the offence is the most important consideration for people working within the criminal justice system because the label influences sentencing, parole and rehabilitation orders and victim compensation.[343]

The label 'identity theft', correctly applied, readily differentiates this offence from fraud. It is important to make this distinction because fraud can apply to a much wider range of criminal behaviour with many different victims and different consequences. Consequently, contrary to Steel's assertion, there is a significant gap in the protection currently provided to an individual's registered transaction identity. This gap can be addressed by regarding the dishonest use of an individual's transaction identity by another person for a transaction as theft of the individual's identity, and by labelling it as identity theft. That label acknowledges the true nature of the offence as a dishonest misappropriation of the individual's rights in his or her transaction 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.[344]

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

340 Andrew Ashworth, *Principles of Criminal Law* (5th ed, 2006), 88.

341 Ibid 88-89.

342 James Chalmers and Fiona Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) *Modern Law Review* 217, 246.

343 Ibid.

344 The theft offence in s 131.1(1) of the Australian federal *Criminal Code* contains the same elements. See n 310 above.

harm to the individual occurs at the time his or her transaction identity is used by another person for a transaction. That misuse, per se, is capable of meeting all of the elements required for theft.

6.5.1 Transaction 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)'(emphases added).[345]

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

When considered separately, the components of transaction 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 that 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.[346] 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, I maintain that on registration under a scheme like the NIS, the information that makes up transaction 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 transaction identity then belongs, as defined in section 5(1), to the individual to whom it is attributed in the register.

345 The Australian equivalent contains very similar definitions. See s 130.1 and s 130.2(1) *Criminal Code*.

346 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.

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,'[347] is well established in international legal scholarship and jurisprudence.[348] The 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,*[349] which cites the influential work of Kevin Gray: [350]

> 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 i.e. 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

347 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'.

348 See C Edwin Baker, 'Property and its Relation to Constitutionally Protected Liberty' (1986) 134 (4) *University of Pennsylvania Law Review*, 741, 742-75. Baker 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'. Similarly, 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).

349 (1999) 201 CLR 351.

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

> from the residual perception that "property" is itself a thing or resource rather than a legally endorsed concentration of power over things and resources.[351]
>
> 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.[352]

Although these views of the High Court are obiter dicta,[353] they provide, as Gray states, a frame of reference. Most importantly in the context of this book, they present a realistic conceptualisation that takes into account modern forms of intangible property such as transaction identity.[354] They recognise that property is a relationship and that it can be a relationship based on an abstraction or a thing.

Under a scheme like the NIS, there is a relationship between the individual and his or her registered transaction identity that necessarily requires the individual's control or power over access. Under the scheme, the individual controls the use of his or her transaction identity for transactions and hence access to his or her record in the register 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 digital 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 transaction identity is recognised and respected. Central to this relationship is the individual's control over his or her registered identity for transactional purposes.

---

351 (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 and that 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.'

352 (1999) 201 CLR 351, paras 17-20.

353 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'. Ibid paras 30 and 40.

354 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.

Under the scheme, there is necessarily a general duty on other members of society not to interfere with an individual's transaction 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 behaviour 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 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.[355]

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'.[356]

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.[357]

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.

355 Hans Kelsen, *Pure Theory of Law* (Max Knight trans, 1970), 131.

356 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.

357 Stephen Munzer, *A Theory of Property* (1990), 23.

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, the right 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.[358] As discussed below, I assert that in relation to his or her registered transaction identity, the individual has most of the eleven rights and duties listed by Honoré.[359]

Although the *Identity Cards Act* provides that if an ID card is issued, it 'remains the property of the person issuing it,'[360] the Act is silent as to the ownership of the information which comprises transaction identity. Nevertheless, just as the card can be stolen from the individual cardholder, information that collectively constitutes transaction identity can be stolen. On registration, the power to possess and control the collection of information that constitutes his or her transaction 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.[361] Both aspects are present in relation to an individual and his or her transaction identity. Registration puts the individual in control of the registered transaction identity and gives the individual the right to remain in control of that property, within the constraints of the scheme.[362] Embedded in this right to control is the right that others cannot unilaterally and unlawfully interfere with it.[363] Honoré states that '[i]t is of the essence of the right to possess that it is in the sense of availing against persons generally' and that,

358 Anthony Honoré, 'Ownership' in A.G. 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).

359 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 transaction 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 transaction 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 transaction identity primarily because of its intangible nature and because it is an emergent form of property.

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

361 Honoré, above n 358, 113.

362 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.

363 Honoré, above n 358, 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'.[364]

As argued in chapter 5, an individual has the exclusive right to his or her unique identity under the scheme and therefore in that sense the individual has exclusive 'dominion' over his or her registered transaction 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 transaction 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 transaction 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 transaction identity.

As to duties, the individual must not use the transaction 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 transaction identity vest in someone else. In the context of transaction identity, that 'someone else' may be an executor or it may be the State.

Transaction identity is therefore fundamentally different from the confidential information in the exam paper dishonestly read by a student in *Oxford v Moss,* which was held not to be intangible property capable of being stolen.[365]Transaction identity is also fundamentally different from the other more detailed information that 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 that can be the subject of theft.

364 Ibid.

365 (1978) 68 Criminal Appeal Reports 183.

6.5.2 Appropriation of an Individual's Registered Transaction 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.[366]

Honoré's incidents of ownership map out the specific ownership rights (and duties) which I maintain arise under the scheme and which are appropriated when the transaction identity is used by another person for a transaction. Specifically, in using an individual's transaction identity for a transaction, an offender assumes the individual's right to possess and use the transaction identity, as discussed above. The offender also assumes the individual's right to manage the registered transaction 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 Transaction Identity

To amount to theft the appropriation must done with intent to permanently deprive the individual of his or her transaction identity. Section 6 (1) of the *Theft Act* states that:

> A person appropriating property belonging to another without meaning the other 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,

366 *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 326, 579.

> 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.'[367]

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

Smith states that section 6(1) was intended to cover the situation in *R v Hall* ('*Hall*') in which the defendant was convicted of theft.[368] 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.

Like a person who dishonestly uses another person's transaction 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. Yet, as Parker B found in *Hall,* '[i]n this case there is the intent to deprive the owner of dominion over his property'.[369]

Similarly, in *DPP v Lavender*[370] ('*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,*[371]which considered that a disposal under section 6 includes dealing.

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

367J C Smith 'The Law of Theft' (8th ed, 1977), 80.

368 Ibid 76.

369 [1848-49] Law Times 383.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'.

370 [1994] Crim LR 297.

371 [1988] 1 WLR 196.

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.[372]

Both *Hall* and *Lavender* concern tangible property but the basic principles apply to intangible property like transaction 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 transaction identity for a transaction exerts control over the transaction identity and thereby encroaches on, and usurps, the owner's rights[373] even though the transaction identity is not disposed of in the sense used by Smith.

372 CO/2779/92 Unpaginated transcript (Tuckey J) See also [1994] Crim LR 297, s8, 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.'

373 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 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.'

6.5.4 Dishonestly Appropriating Transaction 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'[374] 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'.[375] 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.[376]

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.[377] In the context of a scheme like the NIS, use of an individual's registered transaction identity by another person will usually clearly be dishonest.

---

374 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 thestandards 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.'

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

376 [1982] QB 1053, 1064.

377 *R v Waterfall* [1970] 1 QB 148.

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.[378] 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. 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'.[379] 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 transaction identity for a transaction.

A misappropriation must be dishonest for it to be theft. However, under the scheme, even honest use by another person of an individual's transaction identity undermines the underlying assumptions of the scheme and compromises the scheme's integrity. Consequently, special arrangements will be required in cases of incapacity, for example. The system can be designed so that the transaction 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 (by presenting the individual's transaction identity) that he or she is the incapacitated individual.

6.6 Criminal Damage

Where the use is reckless but not dishonest, the offence of criminal damage, which is closely related to theft, can and should, apply. Much of the argument for the application of the offence of criminal damage draws on the same associations as theft.

Considering the damage that can be caused by the misuse by another person of an individual's transaction identity as examined earlier in this chapter, the offence of criminal damage should extend to transaction identity. The offence applies to deliberate acts and

378 The Australian federal *Criminal Code* contains a similar provision. See s 131.2.

379 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.'

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.

The *Criminal Damage Act* in the United Kingdom currently only applies to tangible property[380] but there is no reason in principle why criminal damage and theft cannot apply to the same forms of property. In South Australia, for instance, the criminal damage offence extends to damage to intangible property.[381] The offence closely follows the United Kingdom provision but is capable of applying to new forms of property like transaction 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'.[382]

As discussed earlier in this chapter, when an individual's transaction identity is misused by another person, the use does not necessarily render the transaction identity useless. The individual can still use it, albeit with additional steps such as provision of a PIN or answers to additional designated questions. However, although it does not appear to be affected, primarily because of its intangible nature, the transaction identity has nevertheless been damaged. Its

380 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 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.

381 S 5(1) *Criminal Law Consolidation Act*. defines 'property' to mean 'real or personal property whether tangible or intangible'.

382 S 84(1).

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 caused. In a statement which is particularly relevant to the special nature of the damage resulting from the use of an individual's transaction identity by another person, Walters J in *Samuels v Stubbs*[383] 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.[384]

This statement has direct relevance to an individual's transaction 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',[385] misuse of an individual's transaction identity by another person also causes functional derangement. Unlike the policeman's cap, however, transaction 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 transaction identity as recorded in the register so additional security procedures are required to verify identity for a transaction. As mentioned, these procedures will 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 transaction 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 transaction identity for a transaction under the scheme. So, while the core transaction identity information is unchanged, the misuse changes its usual function at the time of a transaction. Presentation of only the required transaction identity information without complying with the additional system security requirements will no longer be sufficient to enable a transaction under the scheme.

383 (1972) 4 SASR 200, 203.

384 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.

385 Above n 383. 203 .

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'.[386] 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.

In the context of a scheme like the NIS, an individual's transactional identity is the means by which an individual is known by the system and can function under the scheme. Under a scheme which is fully operational and universal, transactional identity is 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 that comprises transaction identity but the connection is cemented by registration under the scheme. The nature of the information that constitutes transaction 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 transaction 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*,[387] 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 transaction identity. Like the policeman's cap, transaction 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 transaction 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 transaction identity.

386 Model Criminal Code Officers Committee the Standing Committee of Attorneys- General, *Model Criminal Code Report, Chapter 4, Damage and Computer Offences* (2001), 17.

387 See above n 384.

6.7 Conclusion

While Steel maintains that nothing of practical value is gained by extending theft to include intangible property,[388] in the case of transaction identity such an extension addresses a critical gap in the protection provided to transaction identity under the criminal law in the United Kingdom, and in Australia.

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 transaction identity after registration. The offences under the United Kingdom *Fraud Act* apply if another person's registered transaction identity is used with intent to make a financial gain or cause a loss. However, the basic wrong, that is, the misuse of another person's transaction 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 book.

Other offences such as the computer offences in the *Computer Misuse Act* and the telecommunications offences 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 transaction 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 transaction identity should be a criminal offence. An individual's transaction identity is more than just information. The scheme transforms the components of transaction identity from information into a set that, 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 transaction identity by another person is not just fraud. Its use by another person is an appropriation of property. In using the transaction 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 transaction identity and to control its use. Dishonest use of an individual's transaction 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,*[389] 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 more widespread, the individual is the primary victim in terms of damage to his

388 Steel, above n 326.

389 Although, as discussed, s 2(1)(b) *Theft Act* requires amendment, and s 6 could be amended to specifically include intent to seriously encroach on the owner's proprietary rights as has been done in South Australia.

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 transaction identity. When misuse of an individual's transaction 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 transaction 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 that in the context of a national identity scheme like the NIS or 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. Transaction identity is, therefore, especially deserving of protection and, as discussed in chapter 5, under the United Kingdom's national human rights regime, transaction 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 by the court. Considering the nature and objectives of the NIS and the transactional role of transaction identity, the protection provided by the criminal law to transaction identity is particularly important. Moreover, while fraud offences 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 transaction identity for a transaction.

Of course, the argument advanced in this chapter that transaction identity is property can also be applied to give an individual private law proprietary rights in his or her registered transaction 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'.[390]

390 Jeremy Horder, 'Re-thinking Non Fatal Offences against the Person' (1994) *Oxford Journal of Legal Studies* 335.